

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.

FILED UNDER SEAL

CV 12-1335

U.S. DISTRICT COURT
EASTERN DISTRICT
OF NEW YORK

2012 MAR 9 AM 8:51

FILED
CLERK

KORMAN, J.

MANN, M.J.

**DECLARATION OF MARK DEBENHAM IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER,
SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Mark Debenham, declare as follows:

1. I am a Senior Manager of Investigations in the Digital Crimes Unit of Plaintiff Microsoft Corp.’s (“Microsoft”) Legal and Corporate Affairs group. I make this declaration in support of Plaintiffs’ Application For An Emergency Temporary Restraining Order, Seizure 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 Microsoft, I assess technology security threats to Microsoft and the impact of such threats on Microsoft’s business. Prior to my current role, I worked as a security engineer in Microsoft’s Trustworthy Computing group, dealing with the discovery, remediation and mitigation of Internet and software security vulnerabilities. Among my responsibilities were investigating targeted attacks and driving the establishment of Microsoft Security Response Center’s response to online service vulnerabilities. Before joining Microsoft, I worked for Verizon Business as a Senior Network Security Specialist performing security assessments as part of its network security professional services team for clients ranging from healthcare and educational establishments to aerospace companies.

3. I have conducted an investigation of the structure and functions of three interrelated botnet architectures called “Zeus,” “Ice-IX,” and “SpyEye,” as well as the activities carried out through these botnets, and an assessment of the impact on Microsoft’s business and on users of the Internet. For simplicity, throughout this declaration, these interrelated architectures, each of which incorporates the “Zeus” code, are collectively referred to as the “Zeus Botnets.” The Zeus Botnets have caused, and continue to cause, extreme damage to Microsoft and other parties which, if allowed to continue, will be compounded as the case proceeds.

BOTNETS IN GENERAL

4. A botnet is a network made up of end-user computers connected to the Internet that have been infected with a certain type of malicious software (“malware” or a “Trojan”) that

places them under the control of the individuals or organizations who utilize the infected end-user computers to conduct illegal activity. A botnet network may be comprised of as few as hundreds or as many as tens of thousands or millions of infected end-user computers. Once a large-scale botnet has been created, its massive infrastructure can be used by the botnet operators to engage in malicious activity—such as stealing financial credentials, stealing personal identification information, stealing confidential data, sending spam email or anonymously carrying out other technical activities or attacks.

THE STRUCTURE OF THE ZEUS BOTNETS

5. The botnets at issue in this case—the “Zeus Botnets”—are credential stealing botnets. The primary aim of these botnets is to infect end-user computers in order to (1) steal credentials for online accounts, such as account login information for Microsoft or other websites, or financial and banking credentials, from the owners or users of those computers, (2) access the victims’ online accounts with the stolen credentials, and (3) transfer information or funds from the victims’ accounts to accounts or computers controlled by the Defendants. Defendants and the Zeus Botnets cause extreme injury to individuals, companies, and governments alike. For example, attached as Exhibit 1 is a true and correct copy of a letter to Microsoft from the Minister for the Cabinet Office and Paymaster General of the government of the United Kingdom, detailing the injury caused by the Zeus Botnets to UK government institutions.

6. I have carried out an examination of the “Zeus,” “Ice-IX,” and “SpyEye” code found on infected end-user computers that are part of these botnets. I have researched the command and control infrastructure of the “Zeus,” “Ice-IX,” and “SpyEye” botnets. I have researched the infrastructure used to propagate the “Zeus,” “Ice-IX” and “SpyEye” botnets. I have also reviewed literature by other Internet security researchers regarding the code, architecture and features of these botnets, including the command and control servers, infected end-user computers that are part of the botnet and infrastructure used to disseminate botnet code. Based on this analysis, I reach the following conclusions regarding the origins of and

relationships between the “Zeus,” “Ice-IX,” and “SpyEye” code and the technical architecture of this infrastructure.

A. The Defendants Who Created The Malicious “Zeus,” “Ice-IX” And “SpyEye” Software Have Leveraged Each Others Work To Create, Distribute And Operate The Zeus Botnets

7. The Zeus, Ice-IX and SpyEye code is offered by Defendants as “builder kits” that allow other would-be cyber criminals to easily setup, operate, maintain, and propagate botnets to infect end-user computers, carry out theft of online credentials for Microsoft or financial institution websites, engage in financial theft, engage in identity theft, send spam email or engage in other malicious activities. The Defendants offer the kits for sale on “underground” cybercrime forums on the Internet. The simplest versions of the malicious software described below are readily available for purchase in underground forums for \$700 or more. Sophisticated versions with more robust features, support and sometimes source code access, are typically offered only to smaller, trusted group of clients and can cost approximately \$15,000 or more. The kits typically contain a builder that can generate a botnet “executable,” configuration files, and web server files (e.g., script files that enable the website to be more interactive with the user, images, or templates to provide data management functionality) for use as the command and control server.

8. As set forth below, the Defendant creators and sellers of the interrelated “Zeus,” “Ice-IX” and “SpyEye” malicious code, which form the basis of the Zeus Botnets, are individuals known on the Internet as “Slavik,” “Monstr,” “Harderman,” “Gribodemon” and “nvidiag.” Over a period, beginning in approximately 2007, from the evidence I have reviewed, I conclude that these individuals have engaged in multiple acts to create, distribute, encourage and operate the Zeus Botnets in a continuous manner, leveraging each others’ work and often cooperating significantly to improve that code in the newer Zeus, Ice-IX and SpyEye software.

9. From the interrelated nature of the code and the operation of the code directed at intruding into computers of Microsoft’s customers, stealing their account credentials for online accounts, such as account login information for Microsoft services or other websites, or financial

and banking credentials, and by sending spam email propagating the code both from these victim computers and to users of Microsoft's email services, I conclude that the purpose of the botnet code, the Zeus Botnets and the Defendants' operation is to steal account credentials, personal identification information, steal funds and to further propagate the botnet infrastructure to do so. I conclude from these same facts, upon information and belief, that the Defendants must have known and intended that the botnet code, the Zeus Botnets and Defendants' operation was to defraud end-user and corporate victims of the Zeus Botnets, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. As further described below, Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts.

10. From the pricing of the code sold by these Defendants who have created the Zeus Botnets, and the scale of infected computers in the Zeus Botnets, as further discussed below, I conclude that these Defendant creators of the botnet code have obtained payment in a given year of \$1,000 or more for such botnet code.

11. The sale and operation of the botnet code and the Zeus Botnets by these Defendants takes place on the Internet, including acts carried out in interstate and international communications and transmissions on and through the Internet.

Zeus Botnet Code

12. The creator of the "Zeus" botnet code is a currently unidentified individual defendant, **John Doe 1**, who goes by the online nickname/handles "Slavik" or "Monstr." John Doe 1 has also gone by the nicknames "IOO" and "Nu11." Attached as Exhibit 5 is a true and correct copy of a report identifying the individual known as "Slavik" and "Monstr" as the author of the malicious Zeus botnet code. Attached as Exhibit 6 is a true and correct copy of an Internet forum discussing the Zeus botnet code, and identifying individuals known as "Slavik" and "Monstr" as the author. My investigation uncovered evidence that John Doe 1 may be contacted at messaging address bashorg@talking.cc.

13. The "Zeus" botnet code was first identified by security researchers in 2007 when

reports surfaced that it was used to steal information from various organizations. From 2009 forward, instances of computers infected by the malicious Zeus software became more widespread.

14. In approximately November 2010, researchers began detecting a new version of Zeus called Zeus Version 2.1. This version of Zeus contained much of the same code as Version 2.0.8.9, but included further features designed to counter attempts to analyze or disable the botnet. For example, Version 2.1 includes a mechanism that verifies the digital signature on all of the botnet files and the data that it downloads, and further stores most of the botnet code's strings in encoded form. The purpose of these features is likely to prevent competitors or security professionals from introducing configuration files into the botnet infrastructure in order to disable it. By spring 2011, a Zeus version 2.1.0.10 was being detected with more frequency and in June 2011 there was a notable peak in attacks carried out through Zeus 2.1.0.10 computers. While there were a number of variants of Zeus 2.1.0.10, each had an identical list of triggers, indicating a single operations team. Attached as Exhibits 7 and 8 are true and correct copies of reports by security firm RSA regarding Zeus 2.1.0.10.

15. In approximately September 2011, a new version 3 of the Zeus code appeared. This version of Zeus contained much of the same code as Version 2.0.8.9, but further incorporates a “peer to peer” communication system in which some computers serve to “proxy” communications through other infected computers, in order to obfuscate the ultimate source and destination of the communications and to make identification of the perpetrators more difficult. In Zeus version 3 changes were also made to limit the way in which the HTTP protocol is used, in an attempt to impede the tracking of the botnet. Attached as Exhibits 9 and 10 are true and correct copies of reports by security researchers regarding Zeus version 3.

Ice-IX Botnet Code

16. The creator of the “Ice-IX” botnet code is a currently unidentified individual defendant, **John Doe 2**, who goes by the online nickname/handle “nvidiag.” John Doe 2 has also gone by the nicknames “zebra7753,” “lexa_mef,” “gss,” and “iceIX.” Attached as Exhibit 11 is

a true and correct copy of an Internet forum posting identifying the individual known as “nvidiag” as the author of the malicious Ice-IX botnet code. My investigation uncovered evidence that John Doe 2 may be contacted at Jabber messaging address iceix@secure-jabber.biz and ICQ messaging address “610875708.”

17. In the fall of 2011, security researchers discovered a variant of the Zeus botnet code built using the source code of Zeus 2.0.8.9. This variant of Zeus was called “Ice IX.” This version includes enhancements to the original Zeus code that permit bypassing of firewalls, bypassing of virus scanning software, and protecting the code from detection by researchers monitoring the botnet. Attached as Exhibit 12 is a true and correct copy of a report by security researchers regarding Ice-IX.

SpyEye Botnet Code

18. The creator of the “SpyEye” botnet code is a currently unidentified individual defendant, **John Doe 3**, who goes by the online nickname/handles “Harderman” or “Gribodemon.” Attached as Exhibit 5 is a true and correct copy of a report identifying the individual known as “Harderman” and “Gribodemon” as the author of the malicious SpyEye botnet code. Attached as Exhibit 13 is a true and correct copy of a report including an interview with “Gribodemon” indicating that this person is the author of the SpyEye code. Attached as Exhibit 6 is a true and correct copy of an Internet forum discussing the Zeus botnet code, and identifying an individual known as “Gribo” as the author of a variant of the Zeus code. My investigation uncovered evidence that John Doe 3 may be contacted at email and messaging addresses shwark.power.andrew@gmail.com, johnlecun@gmail.com, gribodemon@pochta.ru, glazgo-update-notifier@gajim.org, and gribo-demon@jabber.ru.

19. In October 2010, it was announced on “underground” Internet forums where botnet code is sold that the code for the original Zeus botnet was to be merged with the SpyEye botnet code. The SpyEye code began to incorporate code and functionality that was originally only seen in Zeus. For example, a Zeus feature that targeted anti-malware software developed by a particular antivirus vendor became part of SpyEye.

20. Attached as Exhibits 14, 15, 16, 17 and 18 are true and correct copies of reports discussing the merger of the Zeus and SpyEye code.

B. The Creators And Purchasers Of The Malicious “Zeus,” “Ice-IX” And “SpyEye” Software Leverage Each Others’ Work In Developing And Operating he Zeus Botnets

21. The creators of the malicious Zeus, Ice-IX and SpyEye botnet code, discussed above, work together with other sellers, developers and purchasers of that code to operate the Zeus Botnets. After October 2010, currently unidentified individuals, who go by the online nicknames/handles listed below have sold, developed and/or purchased such code, and are currently operating or have contributed to the operation of the Zeus Botnets:

a. **John Doe 4:** Goes by the nicknames “Aqua,” “aquaSecond,” “it,” “percent,” “cp01,” “hct,” “xman,” and “Pepsi.” My investigation uncovered evidence that John Doe 4 may be contacted at messaging addresses aqua@incomeet.com and “637760688.” Evidence indicates that John Doe 4 recruits money mules and uses them to cash out stolen credentials, and operates multiple Zeus botnets to compromise credentials. John Doe 4 and other defendants herein refer to themselves as the “JabberZeus Crew.”

b. **John Doe 5:** Goes by the nicknames “miami” and “miamibc.” My investigation uncovered evidence that John Doe 5 may be contacted at messaging addresses miami@jabbluisa.com, um@jabbim.com, and hof@headcounter.org. Evidence indicates that John Doe 5 is a developer of “web inject” logic for the Zeus Botnets. For example, he has been called on by other John Doe defendants in this case to develop simple web inject code for Zeus configuration files (e.g. injecting additional form fields like for atm card number, pin, etc, as described further below).

c. **John Doe 6** goes by the nickname “petr0vich.” My investigation uncovered evidence that John Doe 6 may be contacted at email and messaging addresses theklutch@gmail.com, niko@grad.com, Johnny@guru.bearin.donetsk.ua, petr0vich@incomeet.com and 802122. Evidence indicates that John Doe 6 is a primary network administrator for other John Doe defendants in this case, handling most of the tasks relating to

Zeus hosting and operations.

d. **John Doe 7** goes by the nickname “Mr ICQ.” My investigation uncovered evidence that John Doe 7 may be contacted at messaging address mricq@incomeet.com. Evidence indicates that John Doe 7 is one of the actors in Defendants’ organization who handles incoming notifications of newly compromised victim information. John Doe 7 is also connected to underground electronic currency exchange services.

e. **John Doe 8** goes by the nickname “Tank” and “tankist.” My investigation uncovered evidence that John Doe 8 may be contacted at email and messaging addresses T4ank@ua.fm, tank@incomeet.com and 366666. Evidence indicates that John Doe 8 works closely with petr0vich and is involved in cashing out stolen credentials.

f. **John Doe 9** goes by the nickname “Kusunagi.” Evidence indicates that John Doe 9 is involved in writing and obtaining web inject code. He is associated with “Tank” and thus can likely be contacted at email and messaging addresses T4ank@ua.fm, tank@incomeet.com and 366666.

g. **John Doe 10** goes by the nickname “Noname.” Evidence indicates that John Doe 10 is associated with “Aqua,” operates the Zeus Botnets and can likely be contacted at aqua@incomeet.com and “637760688.”

h. **John Doe 11** goes by the nicknames “Lucky” and “Bashorg.” My investigation uncovered evidence that John Doe 11 may be contacted at messaging address “647709019.” Evidence indicates that John Doe 11 is a Zeus code vendor and has provided cashiering functions (e.g. initiator of ACH/wire transaction) to other Defendants.

i. **John Doe 12** goes by the nickname “Indep.” John Doe 12 is associated with “Monstr,” “Tank” and “Lucky” and thus can likely be contacted at T4ank@ua.fm, tank@incomeet.com and “366666,” “647709019.” Evidence indicates that John Doe 12 has used the latest versions of the Zeus code.

j. **John Doe 13** goes by the nickname “Mask.” Evidence indicates that John Doe 13 is involved in Defendants’ money mule operations.

k. **John Doe 14** goes by the nickname “Enx.” Evidence indicates that John Doe 14 is involved in Defendants’ money mule operations.

l. **John Doe 15** goes by the nicknames “Benny,” “Bentley,” “Denis Lubimov,” “MaDaGaSkA,” and “Vkontakte.” My investigation uncovered evidence that John Doe 15 may be contacted at email and messaging addresses getready@safebox.ru, john.mikle@ymail.com, alexeysafin@yahoo.com, moscow.berlin@yahoo.com, cruelintention@email.ru, bind@email.ru, firstmen17@rambler.ru, benny@jabber.cz, “77677776,” “76777776,” “173094207,” and “45677777.” Evidence indicates that John Doe 15 specializes in money mule recruitment of young people going to the U.S. (or already there) on a J1 student visa. John Doe 15 advertizes a cash out service known as Hot Spot in the underground and is believed to work with the petr0vich associates on a regular basis.

m. **John Doe 16** goes by the nickname “rfcid.” Evidence indicates that John Doe 16 has purchased and used Zeus code.

n. **John Doe 17** goes by the nickname “parik.” Evidence indicates that John Doe 17 has purchased and used Zeus code.

o. **John Doe 18** goes by the nickname “reronic.” Evidence indicates that John Doe 18 was involved in testing and using the merged “Zeus-SpyEye” code.

p. **John Doe 19** goes by the nickname “Daniel.” My investigation uncovered evidence that John Doe 19 may be contacted at messaging address “565359703.” Evidence indicates that John Doe 19 was involved in developing Zeus/SpyEye code.

q. **John Doe 20** goes by the nicknames “bx1,” “Daniel Hamza” and “Danielbx1.” My investigation uncovered evidence that John Doe 20 may be contacted at email and messaging addresses airlord1988@gmail.com, bx1@hotmail.com, i_amhere@hotmail.fr, Deja-vu@jabber.org, bx_1@hotmail.fr, daniel.h.b@universityof sutton.com, princedelune@hotmail.fr, bx1_@msn.com, danibx1@hotmail.fr, and danieldelcore@hotmail.com. Evidence indicates that John Doe 20 has purchased and used the Zeus/SpyEye code.

r. **John Doe 21** goes by the nickname “jah.” John Doe 21 is associated with “Daniel.” Evidence indicates that John Doe 21 was involved with the development of the Zeus/SpyEye code.

s. **John Doe 22** goes by the nickname “Jonn.” John Doe 22 is associated with “Aqua” and thus can likely be contacted at aqua@incomeet.com and “637760688.” Evidence indicates that John Doe 22 specializes in money mule recruitment in the UK.

t. **John Doe 23** goes by the nickname “jtk.” John Doe 23 is associated with “Aqua” and thus can likely be contacted at aqua@incomeet.com and “637760688.” Evidence indicates that John Doe 23 specializes in money mule recruitment in the UK.

u. **John Doe 24** goes by the nickname “Veggi Roma.” John Doe 24 is associated with “Aqua” and thus can likely be contacted at aqua@incomeet.com and “637760688.” Evidence indicates that John Doe 24 specializes in money mule recruitment in the UK.

v. **John Doe 25** goes by the nickname “D frank.” My investigation uncovered evidence that John Doe 25 may be contacted at messaging addresses d.frank@jabber.jp and d.frank@0n1ne.at. Evidence indicates that John Doe 25 is involved in hosting Zeus code.

w. **John Doe 26** goes by the nickname “duo.” My investigation uncovered evidence that John Doe 26 may be contacted at messaging address duo@jabber.cn. Evidence indicates that John Doe 26 is involved in hosting Zeus code.

x. **John Doe 27** goes by the nickname “Admin2010.” My investigation uncovered evidence that John Doe 27 may be contacted at email addresses fering99@yahoo.com and secustar@mail.ru. Evidence indicates that John Doe 27 is involved in purchasing and using the Zeus code.

y. **John Doe 28** goes by the nickname h4x0rdz@hotmail.com. My investigation uncovered evidence that John Doe 28 may be contacted at email addresses h4x0rdz@hotmail.com. Evidence indicates that John Doe 28 is involved in purchasing and using

the Zeus/SpyEye code.

z. **John Doe 29** goes by the nickname Donsft@hotmail.com. My investigation uncovered evidence that John Doe 29 may be contacted at email addresses Donsft@hotmail.com. Evidence indicates that John Doe 29 is involved in purchasing and using the Zeus/SpyEye code.

aa. **John Doe 30** goes by the nickname mary.j555@hotmail.com. My investigation uncovered evidence that John Doe 30 may be contacted at email addresses mary.j555@hotmail.com. Evidence indicates that John Doe 30 is involved in purchasing and using the Zeus/SpyEye code.

bb. **John Doe 31** goes by the nickname susanneon@googlemail.com. My investigation uncovered evidence that John Doe 31 may be contacted at email addresses susanneon@googlemail.com. Evidence indicates that John Doe 31 is involved in selling PDF exploits to deliver the Zeus/SpyEye code.

cc. **John Doe 32** goes by the nickname kainehabe@hotmail.com. My investigation uncovered evidence that John Doe 32 may be contacted at email addresses kainehabe@hotmail.com. Evidence indicates that John Doe 32 is involved in purchasing and using the Zeus/SpyEye code.

dd. **John Doe 33** goes by the nickname virus_e_2003@hotmail.com. My investigation uncovered evidence that John Doe 33 may be contacted at email addresses virus_e_2003@hotmail.com. Evidence indicates that John Doe 33 is involved in purchasing and using the Zeus/SpyEye code.

ee. **John Doe 34** goes by the nickname spanishp@hotmail.com. My investigation uncovered evidence that John Doe 34 may be contacted at email addresses spanishp@hotmail.com. Evidence indicates that John Doe 34 is involved in purchasing and using the Zeus/SpyEye code.

ff. **John Doe 35** goes by the nickname sere.bro@hotmail.com. My investigation uncovered evidence that John Doe 35 may be contacted at email addresses

sere.bro@hotmail.com. Evidence indicates that John Doe 35 is involved in purchasing and using the Zeus/SpyEye code.

gg. **John Doe 36** goes by the nicknames “muddem” and “mechan1zm.” My investigation uncovered evidence that John Doe 36 may be contacted at email addresses lostbuffer@hotmail.com and lostbuffer@gmail.com. Evidence indicates that John Doe 36 is involved in purchasing and using the Zeus/SpyEye code.

hh. **John Doe 37** goes by the nickname vlad.dimitrov@hotmail.com. My investigation uncovered evidence that John Doe 37 may be contacted at email address vlad.dimitrov@hotmail.com. Evidence indicates that John Doe 37 is involved in purchasing and using the Zeus/SpyEye code.

ii. **John Doe 38** goes by the nickname jheto2002@gmail.com. My investigation uncovered evidence that John Doe 38 may be contacted at email address jheto2002@gmail.com. Evidence indicates that John Doe 38 is involved in creating injection code to deliver the Zeus/SpyEye code.

jj. **John Doe 39** goes by the nickname sector.exploits@gmail.com. My investigation uncovered evidence that John Doe 39 may be contacted at email address sector.exploits@gmail.com. Evidence indicates that John Doe 39 is involved in selling Adobe Flash exploit code to deliver the Zeus/SpyEye code.

22. In addition, **John Does 1-39** may be contacted at the email addresses that they used to register the malicious internet domains that control the Zeus Botnets. Those email addresses are listed at Exhibits 2 and 3 to this declaration.

23. The evidence I have reviewed strongly indicates that John Doe 1 wrote the code for the original Zeus Botnet, that John Doe 2 and John Doe 3 leveraged that work to create Ice IX and SpyEye respectively, and that John Doe 1 and John Doe 3 later combined their respective branches of the Zeus codebase. The same evidence strongly indicates that the remaining John Does listed above have purchased Zeus botnet kits from John Does 1-3, operate those Zeus botnets, or provide technical or logistical services to the botnet operators furthering their criminal

operations. After October 2010, based on the evidence I have reviewed, I conclude that these individuals have engaged in multiple acts to receive, distribute, encourage and operate the Zeus Botnets, in a continuous manner, with interlinking relationships among them.

24. From the operation of the code directed at intruding into computers of Microsoft's customers, stealing their account credentials for online accounts, such as account login information for Microsoft or other websites, or financial and banking credentials, and by sending spam email propagating the code both from these victim computers and to users of Microsoft's email services, I conclude that the purpose of these individuals' purchase of botnet code, running of Zeus Botnets and often coordinated operation is to steal account credentials and personal identification information, steal funds and further propagate the infrastructure to do so. I conclude from these same facts, upon information and belief, that these Defendants knew and intended that the botnet code, the Zeus Botnets and Defendants' operation would defraud end-user and corporate victims of the Zeus Botnets, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. As further described below, Microsoft has been directly injured in its business and property by these Defendants' acts and the pattern of acts.

25. From known activities of these Defendants who have operated the Zeus Botnets or contributed to the operation of the Zeus Botnets, and the scale of theft attributed to the Zeus Botnets, as further discussed below, I conclude that these Defendants have obtained payment in a given year of \$1,000 or more based on sale, purchase or use of the botnet code.

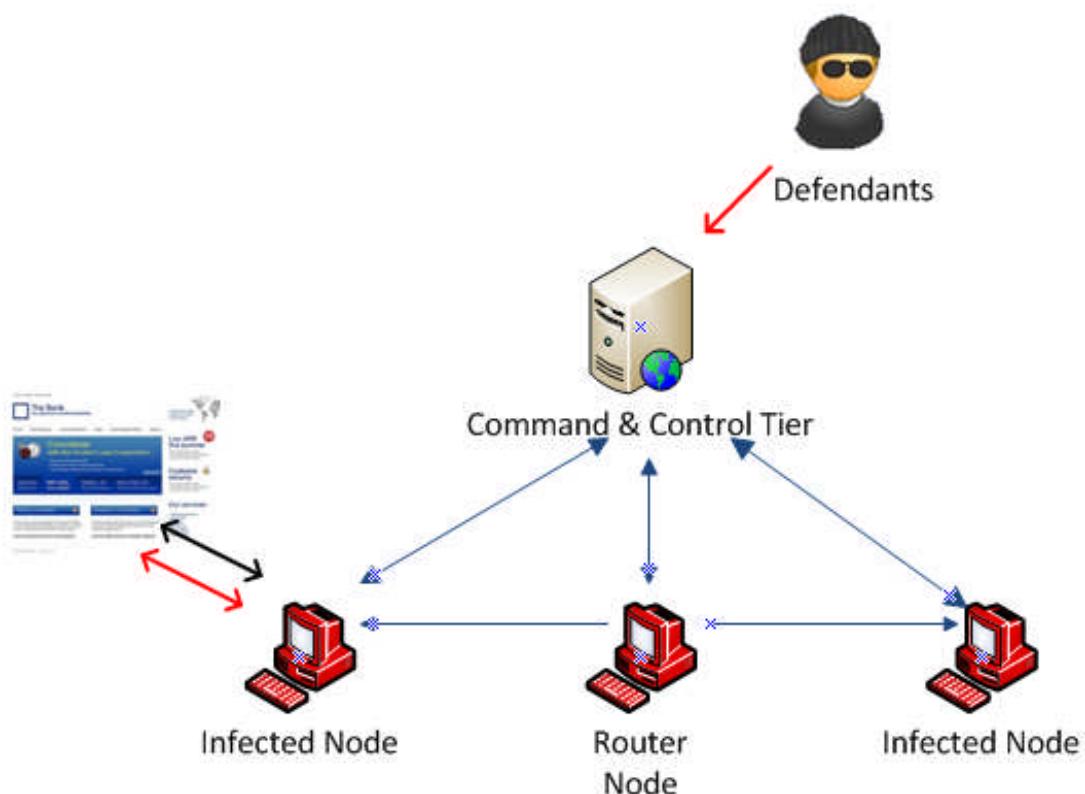
26. Upon information and belief, in light of the continuous nature and persistence of the Zeus Botnets, and the substantial amounts of money generated from procurement, trading and operation of the Zeus Botnets, I conclude that these Defendants, use such revenue both to operate and conduct the affairs of the Zeus Botnets through the procurement, trading and operation of the botnet code and the fraudulent acts discussed further below.

27. The sale and operation of the botnet code and the Zeus Botnets by these Defendants takes place on the Internet, including acts carried out in interstate and international

communications and transmissions on and through the Internet.

C. The Zeus Botnets Have A Multi-Tiered Architecture

28. The Zeus Botnets have a multi-tiered architecture. Different types of components are employed for very specific purposes in the operation of its infrastructure. The Zeus Botnets are made up of two tiers of computers: an “Infected Tier,” made up of computers infected with Zeus (“Infected Nodes”), some of which have been chosen by the botnet operators to perform additional tasks in managing the botnet (“Router Nodes”); and a “Command and Control Tier.” The tiered architecture of the Zeus Botnets can be represented as follows:



1. Infected Tier

29. The lowest tier, the “Infected Tier” consists of millions of infected end-user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world.

30. In general, the Defendant operators of the Zeus Botnets are constantly engaged in infecting additional end-user computers. To counter them, numerous software providers and software security firms are constantly engaged in trying to disinfect those computers. Security firms that conduct research on botnets estimated, as of spring 2010, that the Infected Tier of computers infected by the “Zeus” code alone were comprised of approximately 3.6 million infected computers. Attached as Exhibit 19 is a true and correct copy of a report by security researchers, estimating that there were 3.6 million computers in the Zeus Botnets at that time.

31. I have conducted independent investigation into the number of computers infected by the malicious Zeus, Ice-IX and SpyEye software. Between September 2011 and December 2011, through cooperation from a third-party internet service provider, I was able to observe the behavior of 106 discrete domains that were being used in the command and control infrastructure for these botnets. During that period, I observed connections to those 106 command and control domains from 51,832 unique IP addresses, each representing a victim computer. Thus, each command and control domain reasonably corresponds to approximately 489 infected end user computers. There is a total of 3750 known, active command and control domains at issue in this case. Assuming 489 infected end user computers for each such domain, the total number of infected end user computers active in merely a three month period may reasonably be estimated as approximately 1.8 million.

32. The total number of infected computers in the Zeus Botnets, over time, has been massive. Since 2007, Microsoft’s malware detection software and systems have detected suspected Zeus Botnet infections on 13,730,116 end-user computers. Attached as Exhibit 20 is a true and correct copy of a document summarizing these detected, infected computers by specific variant of the code.

33. The Infected Tier is responsible for performing the daily work of the botnet.

Further, owners of computers in this tier are targets of the Defendants, as the Defendants can steal account credentials and other personal information from the owners of the infected computers, and ultimately steal money from these individuals' bank accounts.

34. Computers that Defendants have targeted for infection by the "Zeus," "Ice-IX" and "SpyEye" software can be found in every state in the United States and in almost every corner of the world. For example, Figure 2 below shows the locations of a small number of the Zeus infected computers, detected in a particular recent investigation, believed to be located in the Eastern District of New York which sent spam email propagating the Zeus Botnets.

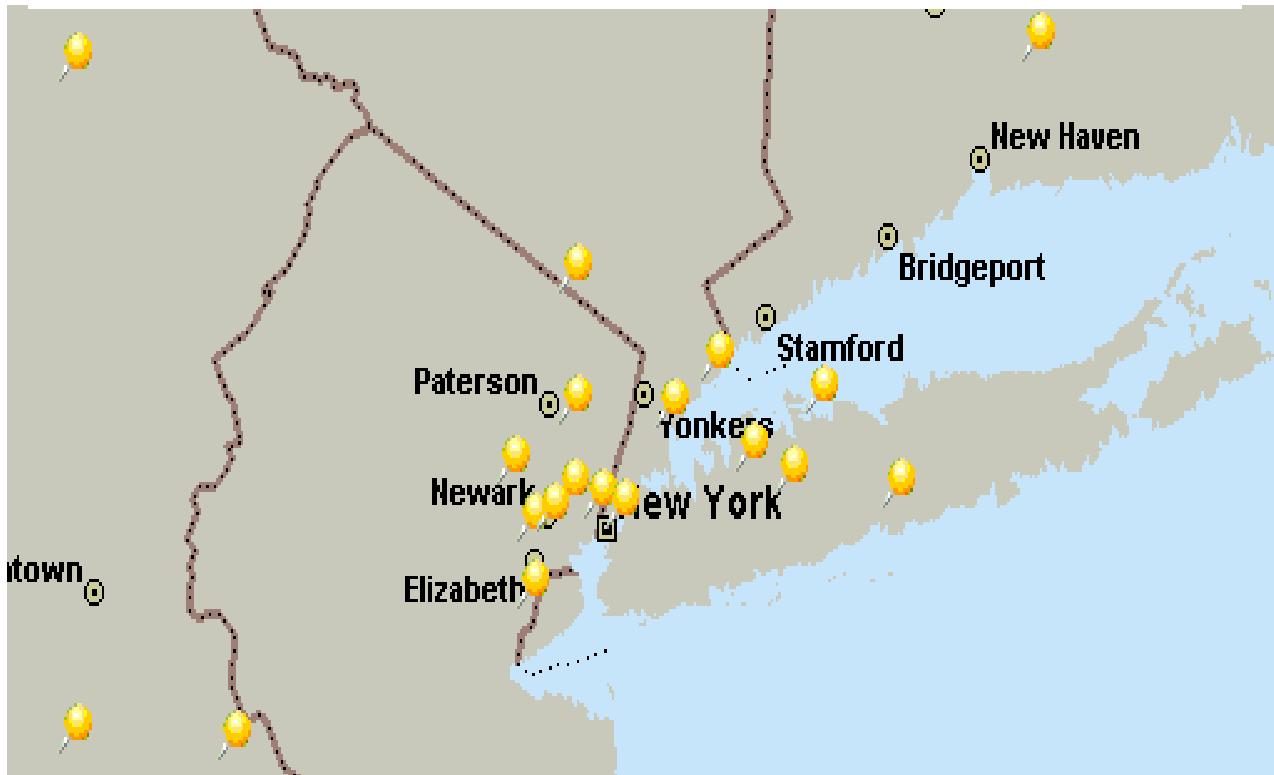
Figure 2 - Computers In The Eastern District Of New York Propagating Zeus Botnet



35. As another example, Figure 3 shows the locations of a small number of the Zeus infected computers, detected in a recent investigation, believed to be located in the Eastern District of New York that requested instructions from known Zeus Botnet command and control

servers.

Figure 3 - Zeus Botnet Computers In The Eastern District Of New York



2. The Router Nodes

36. A subset of infected computers in the Infected Tier may be chosen to perform addition communication tasks on behalf of the botnet. These are referred to as “Router Nodes.” Router Nodes may serve several different purposes, depending on the instructions set by the botnet’s command and control computers. First, they may act as proxies relaying communications among different botnet computers, both to distribute the processing burden and to obfuscate the true source of the communications. Second, these computers may act as HTTP, SOCKS 4 or SOCKS 5 servers capable of delivering commands and responses, when receiving requests from other botnet computers.

3. The Command And Control Tier

37. The third level of the architecture, the Command and Control Tier, consists of specialized computers and/or software (“servers”). Defendants purchased or leased these servers and use them to send commands to control the Zeus Botnets’ Infected Nodes and Router Nodes of the Infected Tier. These computers send the most fundamental instructions, updates and commands, and overall control of the botnets is carried out from these computers. Servers in the Command and Control Tier include the servers at the domain names and IP addresses at Exhibits 2, 3 and 4, which are described more fully below.

THE ZEUS BOTNETS ARE CONTROLLED AND PROPAGATED BY A NETWORK OF MALICIOUS DOMAINS AND IP ADDRESSES

38. The Zeus Botnets are controlled and propagated from computer servers, each of which has an associated domain name and IP address. A “domain name” (commonly thought of as a website name) is an alphanumeric string separated by periods, such as “getbussinesinfo.com,” serving as an address for a computer network connection. An “IP address” is a unique string of numbers separated by periods, such as “149.154.152.161” that identifies each computer attached to the Internet. Each active domain name on the Internet has a corresponding IP address at which the website content is located.

39. The Defendants control the domain names and IP addresses that are used to distribute and propagate the botnet code, to receive communications from the botnets and to control the botnets. True and correct lists of these malicious Zeus, Ice-IX and SpyEye botnet domain names and IP addresses are attached as Exhibit 2, 3 and 4 to this declaration. The relief sought in this case is directed at disabling these malicious domain names and IP addresses.

40. Exhibit 2 to this declaration contains a list of the command and control domains—such as “fastspy.info,” “nacha-reports.org,” “ijqrqinyhmjsvr.net” and many others. Defendants have registered these domains, directly and solely control them, and use them to operate the Zeus Botnets. In these cases, to disable the Zeus Botnets and preserve evidence, the Internet domain registries must redirect traffic to the entire domain to secure computers.

41. Exhibit 3 to this declaration contains a list of the command and control IP

addresses. Defendants have registered these IP addresses, directly and solely control them, and use them to operate the Zeus Botnets. In these cases, to disable the Zeus Botnets and preserve evidence, the Internet hosting companies must redirect the IP addresses to secure computers.

42. Exhibit 4 to this declaration contains a list of file paths—such as <http://qybo-hubybewu.freewebsitethosting.com/nonplatalentiluu21.html>. Here, Defendants have used free website hosting services (in this case the service is called “freewebsitethosting.com”) to create a particular subdomain (“hubybew.freewebsitethosting.com”) and/or file path (“/nonplatalentiluu21.html”) that they use to operate the Zeus Botnets. In these cases, to disable the Zeus Botnets, the free website hosting services must delete or otherwise disable access to the full file path. The general domain of the website hosting service (freewebsitethosting.com or other examples) may remain in operation, as Defendants’ malicious activity is only taking place at the specific file path.

43. The number and locations of the servers represented by these domain names and IP addresses may change over time. Microsoft and other security researchers monitor communications of infected end-user computers and network traffic on a regular basis to detect these changes over time.

44. The functions of the Command & Control domain names and IP addresses are set in additional detail below.

A. Command And Control Domain Names And IP Addresses Are Used To Infect End-User Computers

45. The domain names and IP addresses at Exhibits 2, 3 and 4 to this declaration are used to infect end-user computers and cause them to become part of the Zeus Botnets. The entries at Exhibits 2, 3 and 4 labeled “Embedded_js,” “Infector” and “Source” are such domain names and IP addresses used by the Defendants to infect end-user computers.

46. The Defendants use several methods to infect end-user computers. Typically, the infection of end-user computers involves using software called a “Trojan downloader” that installs the malicious software. The botnet operators store this malicious software on computer servers at the domain names and IP addresses at Exhibits 2, 3 and 4. The Defendants then

mislead Internet users to visit these servers, where the users unknowingly download the malicious software.

47. In one method, the Defendants send Internet users “spam” emails containing links to the domain names or IP addresses of the servers containing the malicious software. The content of the spam email misleads Internet users to click on the links, causing the malicious software to be installed on their computers without their knowledge or consent. In particular, the spam emails falsely claims to be from Microsoft, NACHA, American Bankers Association, major financial institutions or other government agencies, such as the IRS, or companies. The spam emails contain those entities’ trademarks and contain misleading messages, to induce the user to click on malicious links.

48. The Defendants send spam email purporting to be from Microsoft. For example, reproduced below at Figures 4 and 5 are true and correct excerpts of spam emails offering a fake Microsoft “Critical Security Update” and a fake Microsoft “Update for Microsoft Outlook / Outlook Express.” These emails include links that, when clicked, direct the user to one of the Command and Control domains or IP addresses, and results in the infection of the user’s computer with the malicious software:

Figure 4 - Email Falsely Claiming To Be From Microsoft

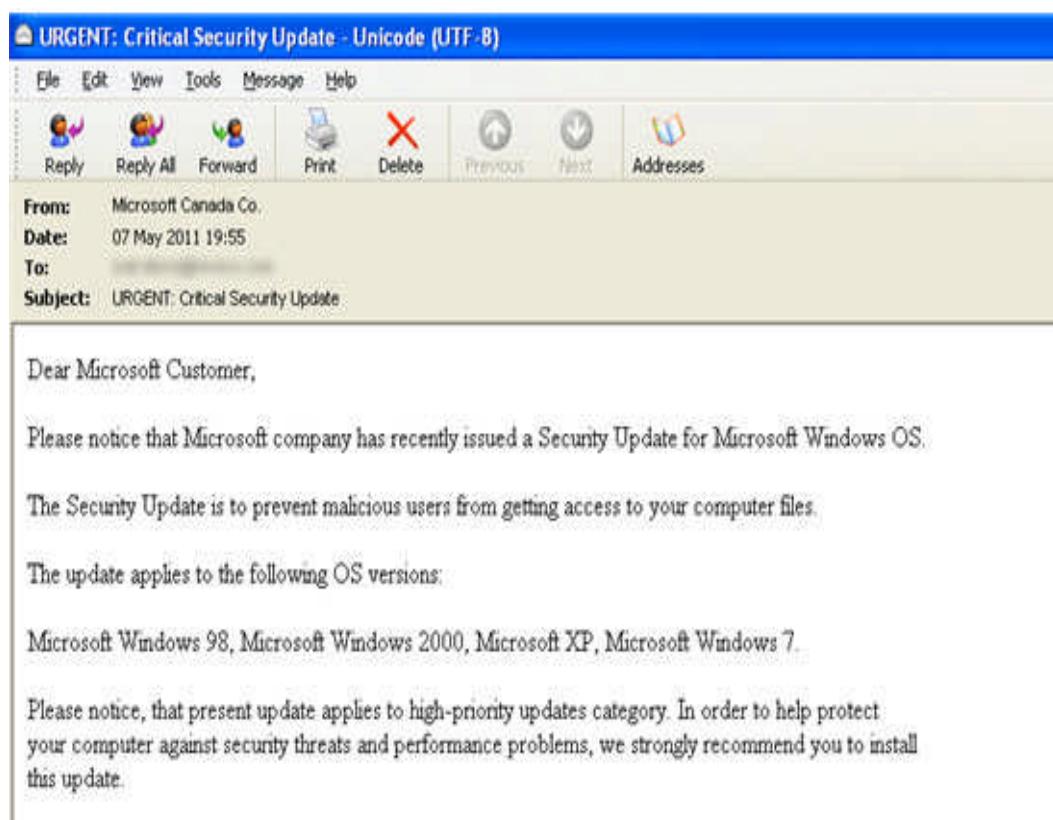
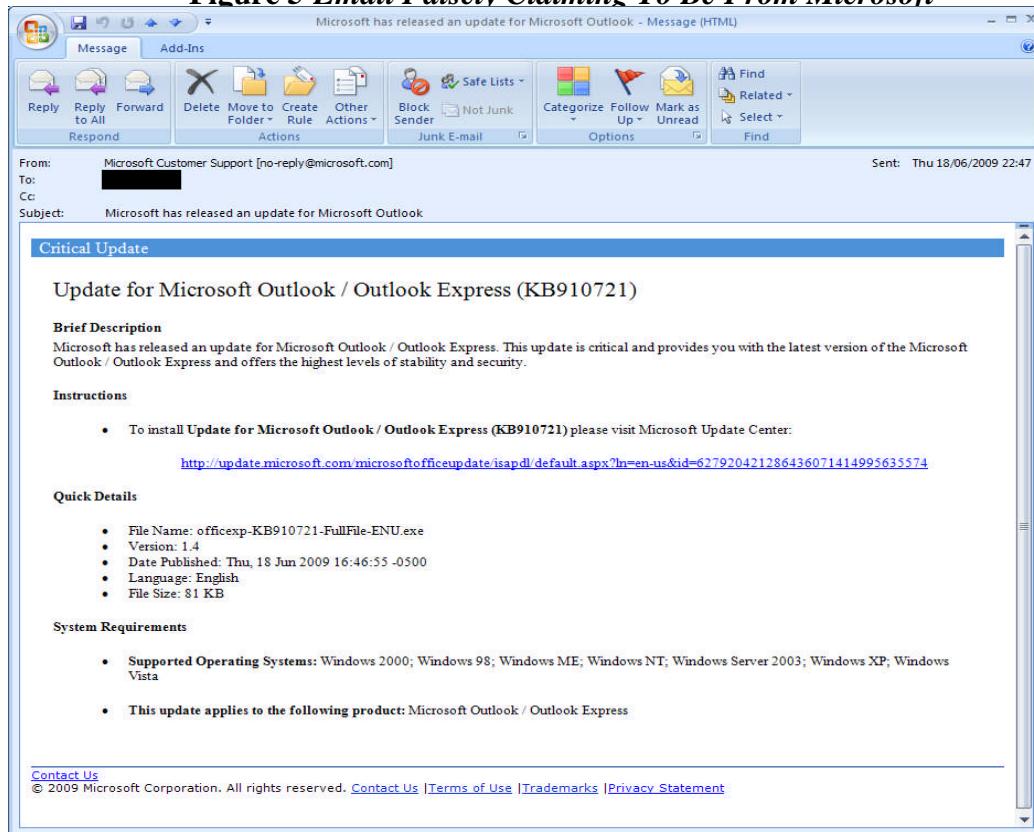


Figure 5-Email Falsely Claiming To Be From Microsoft



49. Similarly, Defendants send such spam email purporting to be from major financial institutions, NACHA, American Bankers Association or other government entities or companies, along with messages. In my investigation, I have seen such spam email containing the following fraudulent messages: (1) email purporting to be from NACHA and requesting that user click on a link to manage a rejected ACH transaction, (2) email purporting to be from banks and requesting that user click on a link to update their banking information, (3) email purporting to be from American Bankers Association and requesting that user click on a link to view an account statement, (4) email purporting to be from the IRS and requesting that user click on a link to download a tax statement, (5) email purporting to be from DHL or Federal Express and requesting that user click on a link to confirm a delivery, (6) email purporting to be an electronic greeting card, inviting users to click on a link to view the card, (7) email purporting to be from Google and other websites asking the user to click on a link to review a submitted job application

or shipping documents, and (8) email purporting to be from social media sites such as Facebook, LinkedIn or others, requesting that users click on a link to accept invitations from “friends.”

50. For example, attached as Exhibit 21 are true and correct copies of spam email propagating the Zeus Botnets, that purport to be from “NACHA,” and directed to customers of Microsoft’s Hotmail email service. In a period of only eight days, between February 16 and 23, 2012, there were at least 3,806 such emails directed by Defendants at Microsoft’s customers, in order to deceive them and take control of their computers.

51. Attached as Exhibit 22 are true and correct copies of reports discussing such spam email purporting to be from NACHA. Attached as Exhibit 23 are true and correct copies of reports discussing such spam email purporting to be from the American Bankers Association.

52. Such spam email is further discussed in the declarations of Pamela Moore, William Nelson and William Johnson, submitted with this declaration.

B. Command And Control Domain Names And IP Addresses Receive Stolen Financial Credentials And Other Information From End-User Computers

53. Many of the domain names and IP addresses at Exhibits 2, 3 and 4 are used to collect stolen financial account credentials and other confidential information from infected end-user computers. The entries at Exhibits 2, 3 and 4 labeled “Dropzone” are such domain names and IP addresses used by the Defendants to receive stolen information from infected user computers. The Defendants subsequently use this information to steal funds from the victims’ financial accounts.

C. Command And Control Domain Names And IP Addresses Control Infected End-User Computers And Control The Botnet As A Whole

54. The domain names and IP addresses at Exhibits 2, 3 and 4 labeled “Updater” are domain names and IP addresses that Defendants use to deliver new configurations and target lists to end-user computers. These domain names and IP addresses enable the Defendants to control infected end user computers after they have already been infected by the malicious software.

55. The foregoing command and control servers house the Zeus Botnets’ configuration files. These servers and the configuration files put the infected end-user computers

under the control of the Defendants, instruct those computers to steal end-user financial account credentials and force those computers to send out spam messages without the knowledge or approval of the end-users.

56. The configuration files stored on the Zeus Botnets' command and control servers contain templates that mimic the websites of virtually all major financial institutions. These website templates contain not only the trademarks of major financial institutions, but also identical copies of those financial institutions' website content. These website templates are sent from the command and control servers to infected end-user computers, and when the end-users attempt to access and use their online banking websites, the website templates are presented instead of the real websites, in order to intercept and steal the end-users' account credentials. The configuration files also contain the domain names of the command and control servers, to which stolen data is to be sent. The operation of these aspects of the botnet on infected end-user computers are described more fully below.

57. The configuration files stored on the Zeus Botnets' command and control servers or related software may contain "spam-templates" or resource files that the infected end-user computers receive from the command and control servers. The malicious software on the end-user computers uses these templates to generate spam email that is sent from the end-user computers and used to infect other computers. The spam templates and resource files contain Microsoft's trademarks, NACHA's trademarks, American Bankers Association's trademarks and the trademarks of major financial institutions. The spam templates and resource files also contain other content and messages designed to create the impression that the email is from Microsoft, NACHA, American Bankers Association or major financial institutions, in order to mislead email recipients into clicking links in the email, as described more fully below.

58. The website templates and spam templates contain counterfeit copies of the trademarks of Microsoft, NACHA, American Bankers Association and financial institutions, and such templates and counterfeit trademarks are stored on the Zeus Botnets' command and control servers.

THE ZEUS BOTNETS' COMMAND AND CONTROL INFRASTRUCTURE IS DESIGNED TO EVADE TECHNICAL COUNTER-MEASURES

59. The most vulnerable point in the botnet architectures used in the Zeus Botnets are the domain names and IP addresses of the command and control servers, as they can be identified and, if disconnected from the Internet, the botnets' communications with infected end-user computers will be severed (i.e., communications between computers in the Infection Tier and Command and Control Tier will be broken) and propagation of the botnet disabled. As discussed above, I have observed that certain features of the command and control infrastructure enable the botnets to better withstand technical counter-measures. For example, over time, the set of domains and IP addresses associated with the command and control servers changes. Certain domains and IP addresses fall out of use by the infected end-user computers and the Defendants. New domains and IP addresses are added to those that the infected end-user computers used to communicate with. In essence, the set of domains and IP addresses used in the command and control infrastructure is dynamic, making attempts to disable the botnet more challenging.

60. Also, I have observed that if infected computers are unable to contact command and control servers, some versions of the Zeus Botnet code will attempt to reestablish contact with the botnet through a fallback mechanism of dynamically generated fallback domains. For this reason, preservation of evidence regarding Defendants' botnet infrastructure is critical to detecting and future remediation of potential fallback infrastructure.

61. Additionally, as described, in most versions of the botnets, communications between the infected end-user computers and the command and control servers are encrypted, and the malicious software is designed to evade anti-virus software and common analysis tools used to gain information about the functioning of the botnet.

THE ZEUS BOTNETS CAUSE SEVERE INJURY TO MICROSOFT'S CUSTOMERS

A. The Defendants And The Zeus Botnets Cause Unauthorized Intrusion

62. The first harm to Microsoft's customers is the installation of the malicious Zeus, Ice-IX and SpyEye software on their computers without their authorization or

knowledge. While the malicious software can infect a number of operating systems, the versions of the software targeted in this case are specifically designed to infect and run on computers equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to end-users. Attached hereto as Exhibit 24 is a true and correct copy of the Windows 7 end-user license agreement. Attached hereto as Exhibit 25 is a true and correct copy of the Windows Vista end-user license agreement. Attached hereto as Exhibit 26 is a true and correct copy of the Windows XP end-user license agreement. End-users' computers can become infected with the malicious software through clicking on a link in an e-mail or visiting an infected website where a Trojan downloader designed to download the malicious software is staged.

63. The installation of malicious software in and of itself damages the user's computer and the Windows operating system on the user's computer. During the infection of an end-user's computer, the malicious software makes changes at the deepest and most sensitive levels of the computer's operating system including the kernel, registry, and systems files. It installs its own kernel mode-driver and intercepts and processes various Windows driver-requests. It alters the behavior of various Windows routines by manipulating various registry key settings. It replaces Windows files with files of the same name that contain the malicious software. It installs software that it needs to steal financial account credentials and generate spam email, and to communicate with the command and control servers.

64. When the Zeus or Ice-IX executable is launched on a targeted computer, it copies itself to the `%system%` or `%appdata%` directory, depending on the operating system version, the version of the malicious software, and the privilege level of the account that the software is running under. It then proceeds to inject itself into various processes in the system, typically `winlogon.exe` and `explorer.exe`, and run primarily from within those processes' contexts. For example, with respect to Zeus, the value of a Windows registry key such as `HKLM/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/ Winlogon` is appended

with the path of an executable, such as: *C:/WINDOWS/system32/sdra64.exe*. This causes the malicious software to execute when the computer restarts. At this stage, the malware initiates system-wide API hooks to obtain sensitive information, hide files, and to protect itself from removal. Zeus and Ice-IX then contact their command and control servers to receive further instructions. Further, Zeus and Ice-IX software can modify system settings in order to disable the Windows firewall, disable antivirus software or to render the end-user's system unbootable, to conceal that misconduct has occurred. The Zeus and Ice-IX software can also download and execute other malicious software.

65. Other security researchers have observed the foregoing behavior of Zeus and Ice-IX as well: (1) Attached as Exhibit 27 is a true and correct copy of a report entitled "On the Analysis of the Zeus Botnet Crimeware Toolkit by H. Binsalleeh et al., discussing intrusion by the Zeus code. (2) Attached as Exhibit 28 is a true and correct copy of a report entitled "What is Zeus?" by a researcher at security firm SophosLabs, discussing intrusion by the Zeus code. (3) Attached as Exhibit 29 is a true and correct copy of a report entitled "Zeus: God of DIY Botnets" by a researcher at security firm Fortiguard, discussing intrusion by the Zeus code. (4) Attached as Exhibit 30 is a true and correct copy of a report entitled "ZeuS: A Persistent Criminal Enterprise" by a researcher at security firm Trend Micro, discussing intrusion by the Zeus code (5) Attached as Exhibit 12 is a true and correct copy of a report entitled "Ice IX: not cool at all" by a researcher at security firm Kaspersky Lab discussing intrusion by the Zeus/Ice-IX code.

66. The SpyEye malicious software makes use of user mode rootkit techniques to hide both, its registry key located inside the Windows registry key *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run* and the folder that contains the executable file and the configuration file *config.bin*. As with Zeus and Ice-IX, the SpyEye code initiates system-wide API hooks from within *winlogon.exe*. The code will first call a function that will hook several APIs in the file *ntdll.dll* and other DLL files like *wininet.dll*, *ws2_32.dll*, *advapi32.dll* and *crypt32.dll*. The code will then

create registry keys and threads in these processes. With the hooked APIs in running processes, the SpyEye software can obtain sensitive information, hide files, and to protect itself from removal and contact its command and control server to receive further instructions. SpyEye can modify system settings in order to disable the Windows firewall, disable antivirus software or to render the end-user's system unbootable, to conceal misconduct. The SpyEye software can also download and execute other malicious software.

67. Other security researchers have observed the foregoing behavior of SpyEye as well. Attached as Exhibit 31 is a true and correct copy of a report entitled "TR/Spy.SpyEye Analysis" by a researcher at the security firm Avira, discussing intrusion by the SpyEye code. Attached as Exhibit 18 is a true and correct copy of a report entitled "The New Frontier For Zeus & SpyEye," discussing intrusion by the SpyEye code.

68. Microsoft's customers whose computers are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and forcibly draft the customers' computers into the botnet.

69. Customers are usually unaware of the fact that their computers are infected and have become part of the Zeus Botnets. Even if aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. For example, attached as Exhibit 37 are true and correct copies of a small sample of customers' communications on Microsoft-run Internet forums related to their attempts to identify and eradicate infections by the Zeus Botnets. These communications demonstrate the extreme problems that this infection creates for Microsoft's customers.

70. The Zeus Botnets turns the infected computer into the worker of the botnet, capable of performing the day-to-day illegal activity. Among other things, an "executable file" is installed on a victim's computer. The executable file is computer code that instructs the

infected end-user computer to, among other things:

- a. hide the executable file from detection;
- b. lower the Internet browser security settings to make the infected computer more susceptible to the botnet controller's control, malware, and instructions;
- c. contact the command and control servers to retrieve a "configuration file" that contains another set of instructions, including website templates that mimic the websites of financial institutions or other instructions;
- d. steals usernames, passwords, and other credentials found on the infected end-user's computer;
- e. communicate the stolen data back to the botnet command and control servers;
- f. intercept or carry out transactions without the user's knowledge or consent, and
- g. alone or in connection with other software, access "spam" email templates and send spam email from or through the infected computer or the victim's email account(s).

71. When the executable file is first installed, it instructs the infected end-user computer to contact the command and control server and download a "configuration file." The configuration file specifies what role the infected end-user computer is to perform and what task it will undertake as part of the botnet. The system is very flexible and Defendants can send a wide variety of commands from a command and control server to an infected computer. Set forth at Figure 6 is a true and correct excerpt of a "control panel" at a command and control server, showing commands that are available to be sent to infected computers:

Figure 6 - Botnet Control Panel Showing Commands That Can Be Sent To Infected Computer

Available commands	
reboot	Reboot computer.
kos	Kill OS.
shutdown	Shutdown computer.
bc_add [service] [ip] [port]	Add backconnect for [service] using server with address [ip]:[port].
bc_del [service] [ip] [port]	Remove backconnect for [service] (mask is allowed) that use connection to [ip]:[port] (mask is allowed).
block_url [url]	Disable access to [url] (mask is allowed).
unblock_url [url]	Enable access to [url] (mask is allowed).
block_fake [url]	Disable executing of HTTP-fake/inject with mask [url] (mask is allowed).
unblock_fake [url]	Enable executing of HTTP-fake/inject with mask [url] (mask is allowed).
rexec [url] [args]	Download and execute the file [url] with the arguments [args] (optional).
rexeci [url] [args]	Download and execute the file [url] with the arguments [args] (optional) using interactive user.
lexec [file] [args]	Execute the local file [file] with the arguments [args] (optional).
lexeci [file] [args]	Execute the local file [file] with the arguments [args] (optional) using interactive user.
adddf [file_mask...]	Add file masks [file_mask] for local search.
delfsf [file_mask...]	Remove file masks [file_mask] from local search.
getfile [path]	Upload file or folder [path] to server.
getcerts	Upload certificates from all stores to server.
resetgrab	Upload to server the information from the protected storage, cookies, etc.
upcfg [url]	Update configuration file from url [url] (optional, by default used standard url)
rename_bot [name]	Rename bot to [name].
getmff	Upload Macromedia Flash files to server.
delmff	Remove Macromedia Flash files.
sethomepage [url]	Set homepage [url] for Internet Explorer.

B. The Defendants And The Zeus Botnets Steal Financial Credentials And Personal Information

72. The primary aim of the Zeus Botnets is to steal the end-user's banking credentials and other personal identifying information in order to access the end-user's bank accounts and siphon funds to the Defendants or other criminal organizations. The Zeus Botnets steal account credentials as follows.

73. The configuration files downloaded to the infected computer may contain templates that contain the website addresses for online banking sites of major financial institutions, as well as other websites and web services. The configuration files contain instructions designed to modify the appearance of the genuine banking websites. The configuration files may contain templates that mimic the websites of major financial institutions and other websites and web services. Such templates contain trademarks of major financial institutions.

74. Once installed on an end-user computer, the malicious software detects when the user of that computer navigates to an online banking website (or any other website

specified in the configuration files). When a user visits their online banking website, the malicious software may do one of the following:

- a. Access the real banking website, but unknown to the user, execute instructions that modify or extend the website. In particular, the Zeus Botnets may cause the website to contain extra fields into which users are instructed to type additional sensitive information that is not requested at the legitimate website. For example, the fake versions of the websites may seek information such as ATM “PIN,” social security number, mother’s maiden name, addresses, birthdates and similar information.
- b. Intercept the request from the user’s web browser and presents the user with a fake website, based on the template, which appears to be the legitimate website, or
- c. Intercept the request and redirect the user to a different fake website that appears to be the legitimate website.

75. In each of these cases, the website presented to the user is a fake or modified version, which appears very similar to the legitimate website and misuses the trademarks and website content of financial institutions and of Microsoft. The following examples, at Figures 7, 8, 9, 10 and 11 are true and correct excerpts from such fake or modified websites, generated by the Zeus Botnets:

Figure 7 - Fraudulent Website Content Misusing Names Of Microsoft And Financial Institutions



Figure 8 - Website Mimicking Banking Website And Fraudulently Adding An Extra Field

Legitimate Online Banking Website:

Sign On to View Your Accounts

We do not recognize your username and/or password. Please try again.
Enter your username and password to securely view and manage your Wells Fargo accounts online.

Sign on to: Account Summary

Username:

Password:

[Username/Password Help](#)

Don't have a username and password? [Sign Up Now](#)

The Botnet Inserts An Extra Field To Collect The User's PIN:

Sign On to View Your Accounts

We do not recognize your username and/or password. Please try again.
Enter your username and password to securely view and manage your Wells Fargo accounts online.

Sign on to: Account Summary

Username:

Password:

[Username/Password Help](#)

ATM PIN:

Fraudulent "ATM PIN" Field



Figure 9 - Fraudulent Website Mimicking Banking Websites

HSBC The world's local bank

Personal Business HSBC United Kingdom Search

Financial Planning HSBC Premier HSBC Plus Current accounts Settings Investments Credit Cards Loans Mortgages Insurance International

Internet Banking Personal Log on Register Security Information

Welcome Log in

Forgot ID? Contact HSBC Help Register

New Customers Find out more about Internet Banking Find out more about Online Security

Business Internet Banking Log on

Important

Symons are PCs can ask very user securely. You can do this on your PC. You have payment. You can get advice from the place go to. [getonline.org](#) and follow their guidance.

Find out more

Interactive demo

To see how Internet Banking can help you manage your money better, take a look at our interactive video demo.

Get Safe Online

To combat the threat of internet fraud and hacking, the Government and businesses like HSBC have combined to create Get Safe Online.

View demo Get Safe

Legal Information Accessibility About HSBC Careers Site Map Branch Locator Contact Us based on UK currency | © HSBC Bank plc 2009

Figure 11 - Fraudulent Website Mimicking Banking Websites

The screenshot shows a Mozilla Firefox browser window with the title "Bank of America | Customer Form - Mozilla Firefox". The address bar displays the URL: <http://www.bankofamerica.com.sv-50981497.118.com.mx/customerservice/secure-directory/direct/documents>. The page content is a仿冒网站 (spoofed website) for Bank of America's online banking enrollment. It features the Bank of America logo and "Online Banking" header. The form includes fields for ATM/Check Card Number (16 digits), Expiration Date (mm/yyyy), Card Identification Number (3 digits), ATM/Check Card PIN (4-12 digits), First & Last Name, and Email Address. A note at the top right says: "In order to use our Text Chat features, please ensure that Java Script is enabled in your browser." Below this are sections for "Online Banking Enrollment" (with radio buttons for "Email Alert" and "Customer Form") and "Online Security Check" (with a message: "Your Internet browser meets our security standards"). A "Submit" button is located at the bottom left of the form.

76. During my investigation, I have observed that the Zeus Botnets create fraudulent, extended versions of websites, redirect users to fake websites or generate fake websites of an array of financial institutions and payment services including:

Citibank	Wells Fargo Bank
Bank of America	Silicon Valley Bank
HSBC	JP Morgan Chase
U.S. Bancorp	Citizens Bank
Capital One	TD Bank
East West Bancorp	Comerica Bank
PNC Financial Services Group	Suntrust Bank
Regions Bank	Chemical Bank
People's Bank	Sterling National Bank
Hargreaves Lansdown	Royal Bank of Scotland
BNY Mellon	First Federal Savings Bank
Deutsche Bank	Halifax Bank
Scottrade	PayPal

Bank of Ireland	Caixabank
Deutsche Postbank	DNB Bank
Posteitaliane	Banca Reale
Presidio Bank	Banco Comercial Portugues
Procredit Bank Bulgaria	Queensland Teachers Credit Union
Railways Credit Union	Rasbank
San Francisco Fire Credit Union	RBK Money
National Bank of Bahrain	Riyad Bank
Royal Bank of Canada	Standard Chartered Bank
Saudi British Bank	The Saudi Investment Bank
National Bank of Oman	Samba Financial Group
Banco Santander	Savings & Loan Credit Union
Sudostoitelny Bank	Space Coast Credit Union
Siam City Bank	Bank of Nova Scotia
Lloyds TSB Bank	Australian Central Credit Union
Ally Bank	AMP Bank
BNP Paribas	Banque Saudi Fransi
Svenska Handelsbanken	ING Bank of Canada
The Toronto-Dominion Bank	Hellenic Bank Public Company
Zions Bancorporation	Capital One
Australia and New Zealand Banking Group	Saudi Hollandi Bank
Shell Federal Credit Union	Suncoast Schools Federal Credit Union
U.S. Bank	ABN AMRO Bank
Branch Banking and Trust Company	Seattle Metropolitan Credit Union
Co-operative Bank	South Valley Bank and Trust
ING Bank Slaski	ClickBank
Malayan Banking Berhad	Union Bank

77. When the user types in their account credentials, including username, password and other additional personal data, the malicious software collects this data and transmits it over the Internet to command and control servers (the “dropzones”), where it is received by the Defendants. Similarly, the malicious software can take screenshots of online banking websites where the user has typed in account credentials or other information. Again, these screenshots of the user’s data is collected and transmitted over the Internet to the command and control servers.

78. The Zeus Botnets’ code is also able to (1) inject the Defendants’ own transactions into a victim’s online banking session, (2) divert the funds from a victim’s banking or ACH transaction to an account controlled by Defendants, (3) manipulate the screen display presented to a victim to falsify account balances, thus hiding the theft, and (4)

re-generate “.pdf” versions of account statements delivered to a victim, removing fraudulent transactions, thus hiding the theft.

79. The Defendants use the data sent from victim computers to the command and control servers to access victims’ online financial accounts and steal money from those accounts. Set forth at Figure 12 is a true and correct excerpt from the “control panel” of a botnet command and control server, showing a list of captured screen images of victims logging into their accounts, which would include their login credentials (here the files are stored in a folder called “screens”):

Figure 12 - List Of Files Containing Stolen Account Credentials On Command And Control Server

Result:		
	Name	Size (bytes)
	/	
	[files]	<DIR> 25.09.2009 00:20:40
	/files	
	[plag]	<DIR> 01.10.2009 21:49:00
	/files/plag	
	[vb4_00276d75]	<DIR> 30.09.2009 21:40:47
	[bot_10000001]	<DIR> 30.09.2009 21:53:13
	[vb4_001593af]	<DIR> 29.09.2009 20:55:38
	[vb4_000f7e54]	<DIR> 01.10.2009 21:49:00
	/files/plag/bot_10000001	
	[d:]	<DIR> 30.09.2009 21:38:12
	[screens]	<DIR> 30.09.2009 21:53:13
	/files/plag/bot_10000001/d:	
	Autorun.inf	116 30.09.2009 21:38:12
	/files/plag/bot_10000001/screens	
	[www.bank.com]	<DIR> 05.10.2009 23:16:30
	/files/plag/bot_10000001/screens/www.bank.com	
	0220_000CB260.jpg	16 761 30.09.2009 22:00:20
	0220_00261659.jpg	16 412 30.09.2009 22:27:19
	0220_000D65A8.jpg	26 828 30.09.2009 22:01:11
	0220_000D3BD7.jpg	29 422 30.09.2009 22:01:06
	0220_001A7A1B.jpg	22 520 30.09.2009 22:14:48
	/files/plag/vb4_001593af	
	[d:]	<DIR> 05.10.2009 23:26:22
	[certs]	<DIR> 29.09.2009 20:55:40
	/files/plag/vb4_001593af/certs	
	Root_29_09_2009.pfx	103 752 29.09.2009 20:54:37
	CA_29_09_2009.pfx	11 958 29.09.2009 20:54:38
	AuthRoot_29_09_2009.pfx	98 280 29.09.2009 20:55:40
	Disallowed_29_09_2009.pfx	4 886 29.09.2009 20:55:38

80. The Defendants may set parameters controlling precisely when and how the botnet steals credentials or victim funds. For example, based on my investigation, I am aware of instances where, after stealing account credentials, the botnet operators waited until victim account balances reached some amount over \$1,000 and then would initiate transfers to steal funds in amounts between \$500 and \$2,500.

81. Often, the Defendants hire “money mules.” These are individuals who travel to or are located in different countries, including the United States, in order to set up bank accounts to receive transfers of stolen funds from the victims’ accounts. The money mule withdraws the funds from the account they have set up, keeps a percentage for their own payment and transmits the remainder to the Defendants. Sometimes the money mules use the stolen funds to purchase high-value items, which are easier to transport than cash and can easily be resold later for cash. Attached as Exhibit 32 is a true and correct copy of an article issued by the Federal Bureau of Investigation describing the structure of such account theft and money transfers.

82. The same code and methods can be used to steal credentials to access other online services as well. The Defendants fine tune copies of the malicious software to only steal information from websites that they are interested in. For example, in addition to online banking and financial services, the botnets have been tailored to steal login credentials for protected storage accounts, files uploaded from the victim’s computers, online social networks or e-mail accounts and other websites. In particular, I have observed configuration files of the malicious software which are set up to detect when a user accesses: (a) any website which ends in “.microsoft.com/” and (b) Microsoft’s “hotmail.com” or “live.com” email websites. For example, the “Ice-IX” variant of the code access the victims Windows Mail email account, Microsoft Live email account, Outlook emails, contacts, calendar and notes. The Defendants use the Zeus Botnets to steal account credentials from these Microsoft users, in order to access their accounts, steal the personal information contained in

the accounts and send spam email from the email accounts.

83. Similarly, the botnets have targeted many other online accounts and services, including Google Gmail, YouTube, Blogger, Facebook, eBay, Yahoo, LiveJournal, MySpace, Amazon, Flickr, Hi5, Metroflog, Sonico, Netlog and others.

84. The malicious software is specifically designed to allow Defendants to perpetrate this malicious activity without revealing any evidence of the fraud to the end-user, Microsoft, the financial institutions or other victim websites until it is too late for the user or owners of these websites to regain control over funds or stolen information. For example, the software can re-write on-screen account balances and hide transactions from the user's view, and can hide itself from antivirus software.

C. The Defendants And The Zeus Botnets Send Spam Email

85. The Defendants, through the Zeus Botnets and often in connection with other software, also send, without the user's knowledge or permission, unsolicited bulk email (often known as "spam"). The spam email usually contains links to malicious code that infects further computers adding them to the botnets or may serve other purposes, such as inviting users to enter financial or other valuable personal information. The Defendants are capable of sending spam email to perpetuate fraud; to collect financial and personal data; to distribute harmful and fraudulent software; to promote scams; and to carry out other illicit activities. Examples of such spam email are described above, describing the spread of the Zeus Botnets through spam email.

86. The Defendants accomplish the sending of spam email in several ways. First, by stealing account credentials to victim's email accounts, the Defendants send spam email from such email accounts, which are accessed without knowledge or authorization of their owners. Second, the Defendants send spam email directly from infected end-user computers. In this second situation, part of the software downloaded to infected computers has the capability to turn the infected computers into spam email generators sending email to other computers. In this way the malicious code instructs the infected end-user computer to send

such spam email, without the user's knowledge or permission.

87. In either situation, configuration files containing spam templates are retrieved from the command and control servers and downloaded to infected computers, or other computers used to access victim email accounts without authorization. These spam-templates work with the email server software in order to structure the appearance and content of the outgoing spam email messages. The spam templates and resource files contain Microsoft's trademarks, the trademarks of NACHA, the American Bankers Association, major financial institutions and other content designed to mislead the recipients of the spam email into clicking on links in the spam email. Examples of such email are discussed above.

D. The Defendants And The Zeus Botnets Use Microsoft Customers' Computers In Criminal Activity

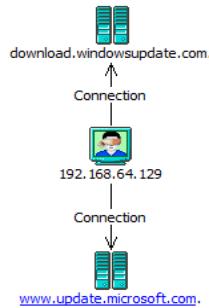
88. Once infected with malicious software, the end-user's computer is under the control of the Defendants operating the Zeus Botnets. As discussed above, based on my observations and the observations of other security researchers, the primary functions of a Zeus Botnets is to infect end-user computers, to steal end-users banking credentials and to send out a very large quantity of illegal spam e-mail each day of its operation. As discussed, I have observed that the fake financial websites and spam emails generated by and through infected computers use the trademarks of Microsoft, NACHA, American Bankers Association, major financial institutions and many other government institutions and companies.

E. The Defendants And The Zeus Botnets Use Microsoft's Customers' Computer-Resources For Illicit Purposes

89. An infected end-user computer's processing power, memory, communications bandwidth, and other resources will be used for the high volume of processing, data transfer and connections to the Internet that the infected end-user computer engages in. I recently investigated the impact that infection has on the activities of an infected computer. I first recorded the Internet activity of a Windows computer that was not infected with any

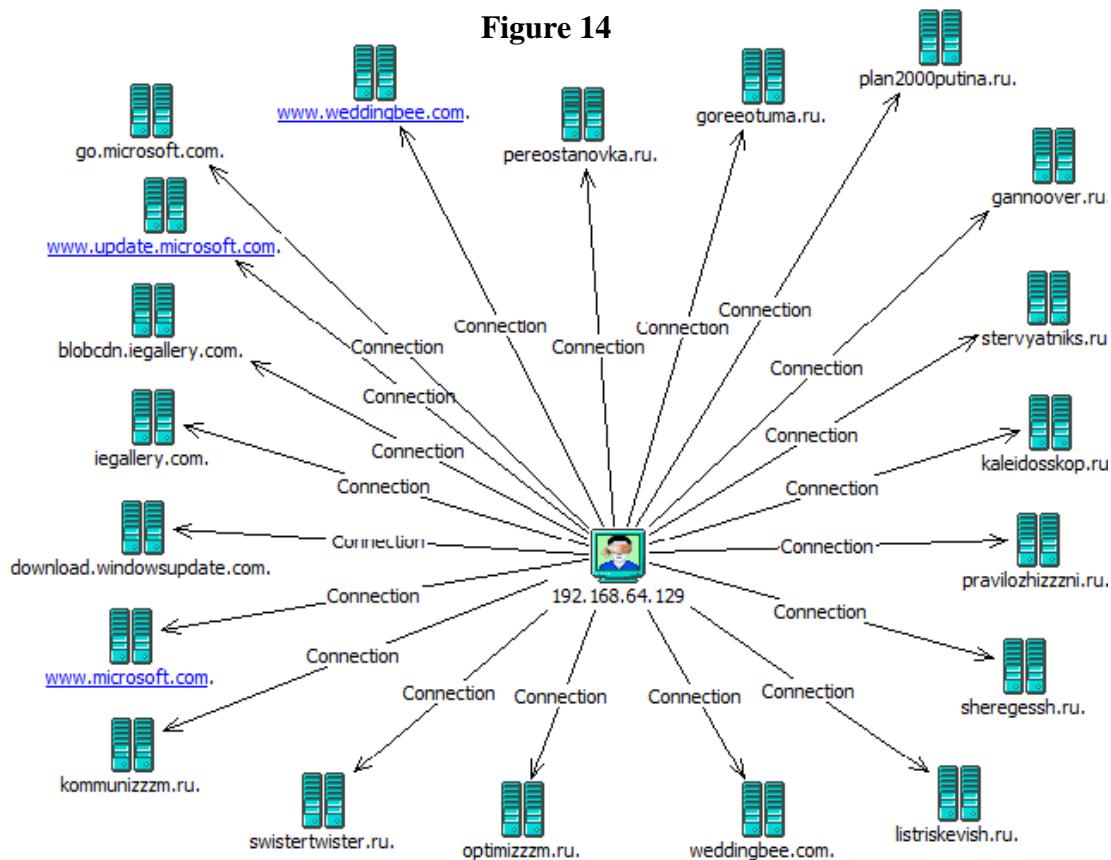
malware. I observed two, all of which I found to be normal in the operation of the computer over the course of approximately two hours. This provided me with the baseline level of activity of an uninfected computer. This activity is depicted in Figure 13, below:

Figure 13



90. I then intentionally infected the computer with the code that would be part of the Zeus Botnets and ran the sample for approximately two hours, using the baseline system. I observed the infected end-user computer made the normal connections of the baseline computer, but in addition, it performed additional connections to command and control servers as part of the botnet's operation. This activity is shown in Figure 14, below, in which the infected computer is shown in the center.

Figure 14



F. The Defendants And The Zeus Botnets Directly Targeted Microsoft Customers With Its Spam Campaigns

91. Microsoft's email customers are targeted by the Defendants' and the Zeus Botnets' spam campaigns. During the period between February 16 and February 23, 2012, approximately 3,806 e-mails were received at Microsoft's Hotmail email service, purporting to be from NACHA and attempting to infect user computers and make them part of the Zeus Botnets. That totals 173,000 such malicious, spam emails per year directed to Hotmail customers. However, the actual number is certainly much higher, given that this figure only accounts for malicious emails purporting to be from NACHA and does not account for the vast array of spam email schemes designed to infect users' computers.

THE ZEUS BOTNETS CAUSE SEVERE INJURY TO MICROSOFT

A. High Cost of Dealing with Credential Theft

92. Microsoft, as a provider of the Windows operating system and Internet

Explorer web browser, must incorporate security features in an attempt to stop account credential theft by the Zeus Botnets from occurring to customers using Microsoft's software.

B. High Cost of Dealing with Spam

93. Microsoft, as a provider of online e-mail services such as Hotmail, must maintain spam filters to stop spam originating from or otherwise promoting the Zeus Botnets from reaching Microsoft's customers.

94. As discussed, Microsoft's Hotmail systems are the target of a substantial volume of spam from and promoting the Zeus Botnets. The sending of vast amounts of spam email to Microsoft's Hotmail email services imposes a burden on Microsoft's servers, and requires Microsoft to expend substantial resources in an attempt to defend against and mitigate the effects of this vast amount of spam email.

95. I have reviewed spam-related complaints posted by Microsoft Hotmail account customers on Microsoft's customer forums, and based on these questions and comments, I believe that the very large amount of spam directed at Microsoft's Hotmail customers frustrates them and unfairly diminishes their regard for Hotmail and Microsoft. For example, attached as Exhibits 33 are true and correct copies of customers' complaints regarding significant volumes of spam, bombarding their Hotmail accounts and seeking solutions, up to and including disabling their Hotmail accounts, to escape from the spam.

C. High Cost of Assisting Customers to Disinfect Computers

96. Additionally, Microsoft devotes significant computing and human resources to combating infections by the Zeus Botnets and helping customers determine whether or not their computers are infected, and if so, cleaning them. For example, since 2007, Microsoft has detected suspected infections on 13,730,116 end-user computers. *See Exhibit 20.* Given the scale of this threat, Microsoft has had to invest significant resources attempting to clean these machines and counter this ever-evolving threat. Microsoft has had to constantly update its telemetry to counter the threat as Defendants means of evasion evolve.

97. I believe that customers' frustration with having to deal with Zeus Botnet

infections on their computers, discussed above, unfairly diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill.

98. The cost to Microsoft specifically attributable to blocking spam email promoting the Zeus Botnets, assisting customers to remove the malicious code of the Zeus botnets and to investigate and take steps to remediate the Zeus Botnets is conservatively approximated to be \$1.7 million.

THE ZEUS BOTNETS CAUSE SEVERE INJURY TO THIRD PARTIES AND THE PUBLIC

99. As set forth more fully in the Declaration of William Nelson, the Declaration of Pamela Moore and the Declaration of William Johnson, the Zeus Botnets cause injury to numerous financial institutions, the trade groups that represent them, including FS-ISAC, NACHA and the American Bankers Association, and individual accountholder victims whose information and funds are stolen.

100. I am informed and believe that numerous third-party companies have been and continue to be injured by the Zeus Botnets. The following are examples of such abuse:

- a. In 2010 it was reported that several instances of the Zeus botnet had resulted in theft of \$70M. Attached as Exhibit 32 is a true and correct copy of a report by the FBI, entitled "Cyber Banking Fraud: Global Partnerships Lead to Major Arrests," describing this account compromise.
- b. In 2010 it was reported that one instance of the Zeus botnet had compromised at least 3,000 computers and stolen £675,000 in a single month. Attached as Exhibit 34 is a true and correct copy of a report, entitled "Thousands of online banking customers have accounts emptied by 'most dangerous Trojan virus ever created,'" describing this account compromise.
- c. In 2009 it was reported that the Zeus botnet had compromised over 74,000 FTP accounts on websites of such companies as the Bank of

America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and Business Week. Attached as Exhibit 35 is a true and correct copy of a report, entitled “ZBot data dump discovered with over 74,000 FTP credentials,” in a computer security publication describing this account compromise.

- d. In 2009 it was reported that over 1.5 million phishing messages were sent on Facebook with the purpose of spreading the Zeus trojan.

Attached as Exhibit 19 is a true and correct copy of a white paper by the company Unisys, entitled “Zeus Malware: Threat Banking Industry,” describing the Facebook campaign and impact on the banking industry.

REDIRECTING THE COMMAND AND CONTROL DOMAINS AND IP ADDRESSES TO SECURE COMPUTERS, WITHOUT FIRST INFORMING THE DEFENDANTS, IS THE ONLY WAY TO PREVENT INJURY AND PRESERVE EVIDENCE

101. The Zeus Botnets are designed to resist technical mitigation efforts, eliminating viable technical means to curb the injury being caused and are designed to destroy evidence of and conceal the misconduct.

102. Given the specific architecture of the Zeus Botnets, I believe that if provided advance notice that the command and control domains and IP addresses were to be redirected to secure computers, thus disabling them, the Defendants would take measures to keep the Zeus Botnets alive by migrating the command and control infrastructure to new IP addresses and domains. As discussed above, the botnets are designed to withstand technical counter-measures:

- a. They have an extensive Command and Control Tier, giving each infected end-user computer multiple points of contact with the botnets;
- b. They change the domains and IP address of the command and control servers over time;
- c. The infected end-user computers and Defendants are able to generate an alternate list of fallback rendezvous domains should the infected end-user

computers be unable to communicate with the command and control servers.

103. Therefore, a piecemeal approach to disconnecting the Zeus Botnets' command and control servers will fail. Unless all of the domains and IP addresses of the current command and control infrastructure are redirected to secure computers immediately and simultaneously, there is a chance that the Defendants will be able to migrate the command and control infrastructure to new servers.

104. Further, unless all of the domains and IP addresses of the command and control infrastructure are redirected to secure computers, the Defendants may be able to access those computers, thus destroying evidence of their misconduct and their identities, and destroying evidence of the infected computers that connect to the command and control servers, thus preventing mitigation and cleaning of those victim computers at a future point in time.

105. I am specifically aware of a previous instance in which the botnet controllers changed the location of a botnet's command and control servers after services to the hosting company supporting those servers were interrupted by enforcement efforts. In that instance, the command and control server was allowed back on line for a brief interval of time, during which the command and control servers were moved to new locations in Russia and the infected end-user computers were directed to the new locations.

106. I am aware of other prior instances where security experts or the United States government attempted to curb injury caused by botnets, but inadvertently allowed the bot-herders to receive notice. In these cases, the bot-herders immediately moved the botnet command and control servers to new, unidentified locations causing the botnet to continue its operations while also destroying and/or concealing evidence of the botnet's operations.

107. I am specifically aware of the prosecution of individual participants in activities related to Zeus Botnets, yet despite such enforcement efforts, the operators of the Zeus Botnets have continued their illegal activities. For example, on November 3, 2009 a British couple was arrested for allegedly using Zeus code to steal personal data. A true and

correct copy of this report is set forth at Exhibit 36. On October 1, 2010, the FBI announced the arrest in the U.S. of suspected members of the ring who had served as conduits for moving approximately \$70M stolen by the Zeus botnet. Arrests were also made in the UK and Ukraine. A true and correct copy of this report is set forth at Exhibit 32. Because of these enforcement efforts, the Defendants operating the Zeus Botnets are likely to be expecting and prepared for further enforcement efforts and will move the command and control infrastructure and destroy evidence if notified in advance.

108. I have personally participated in informal efforts to eliminate Zeus botnet command and control servers, by working with third party internet service providers to which I have reported such domains and requested that the domains be disabled. While I have received cooperation in this regard and disabled some such domains, the Zeus Botnet command and control structure continues to operate and grow. Such informal efforts are insufficient to disable the bulk of the botnet infrastructure, given the scale of the infrastructure and the fact that disabling such infrastructure is piecemeal and not coordinated, allowing the botnets to continue. There is a need for coordinated, simultaneous action to disable the broader infrastructure, which is only possible through a Court order directing such relief.

109. Based on my experience involving Internet security matters and disabling of botnets, I believe that the most effective way to suspend the injury caused by Zeus Botnets is to follow the protocol set forth in the [Proposed] *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction (“Proposed TRO”). An explanation of the protocol in the Proposed TRO is set forth below. There are three goals: 1) to preserve evidence of criminal activity; 2) to provide for the identification of the Internet service providers (“ISPs”) through which Zeus victims connect to the Internet so that the ISP’s can help in the process of identifying the Zeus victims and assist in removing the Zeus code from their computers; and 3) to halt the operation and spread, to the extent possible, of the most significant portion of the Zeus Botnets infrastructure that we have been able to

identify.

110. The first necessary step is to preserve evidence related to communications to and from the most active Zeus Botnet command and control servers that we have been able to identify. Appendix B to the proposed order identifies the specific IP addresses of these command and control servers and identifies the specific data centers and hosting companies in which those servers are believed to be located. Data center and web hosting companies are companies that typically provide space, technical support, and connection to the Internet for hundreds or thousands of computers leased or owned by third-parties for various purposes, usually to host or support legitimate websites. Evidence preservation can be accomplished by preserving traffic to and from the specifically identified command and control servers for a short period of up to four hours. Preserving this evidence will preserve the ability to identify the Internet addresses of servers functioning at deeper levels of the command and control infrastructure that we currently cannot see, as well as the ISPs through which victim computers are connecting to the Internet, which again may allow, at some future point, for the identification of and rendering of assistance to those victims. Because the evidence preserved may include highly sensitive information, such as financial account information stolen by the botnet operators from Zeus victims, it should be collected and preserved under seal by the Court-appointed forensic specialist. The information preserved by monitoring traffic to and from the command and control servers should be preserved in-full, as it very likely comprises evidence of criminal conduct.

111. The second necessary step is to disconnect and seize the physical command and control servers and/or the command and control software located on the servers. This will halt the operation and spread of a significant portion of the Zeus Botnets. This step can be accomplished in part with the assistance of the data-center and webhosting companies in whose facilities the command and control servers are located. Because the servers also likely contain evidence of criminal conduct, they, or the relevant content on them, should be preserved under seal by the Court-appointed forensic specialist.

112. The third necessary step is to disconnect communication between parts of the Zeus Botnets and certain identified domains (i.e., websites). Appendix A to the proposed order identifies Defendants' specific harmful domains (domains such as "fastspy.info," "nacha-reports.org," "ijqrqinymhjsvr.net" and others) and identifies the specific domain registries through which Defendants registered the domains. The domain registries should be directed to redirect Defendants' Harmful Domains to specific IP addresses of secure computers, in order to disable those domains and preserve evidence available through them, a step discussed further in the following paragraph.

113. The fourth necessary step is to redirect the Internet traffic going to the domains identified in Appendix A the proposed order to computers controlled by Microsoft. The Microsoft computers are configured to capture only the IP addresses of computers that are attempting to establish contact. They are deliberately configured to break-off the communication before any content is received. This again will allow Microsoft to identify the IP addresses of the ISPs of Zeus victims, who can assist in the process of identifying the Zeus victims so that they can be assisted in removing Zeus code from their computers. Such IP address information is publicly visible information anytime a computer connects to the Internet. This redirection of Internet traffic can be accomplished with the assistance of the relevant domain registries that can redirect traffic seeking particular domains (i.e., websites or numbered Internet addresses) to IP addresses of the secure computers designated by Microsoft.

114. The fifth necessary step is to direct certain other website hosting services, identified in Appendix C to the proposed order, to delete or otherwise disable access to other resources being used by the Zeus botnet operators. These hosting services provide their customers, including operators of the Zeus Botnets, with space on computers connected the Internet. Our evidence indicates that the Zeus Botnet operators have staged resources at specific locations on specific computers provided by these companies. Appendix C to the proposed order identifies specific file paths—such as <http://qybo->

hubybewu.freewebsitehosting.com/nonplatentiluu21.html —that Defendants have created through free website hosting services (in this case the service is called “freewebsitehosting.com”), and where Defendants have placed harmful resources used in the operation of the Zeus Botnets. In these cases, the free website hosting services should delete or otherwise disable access to the full file path. The general domain of the website hosting service (freewebsitehosting.com or other examples) may remain in operation, as Defendants’ malicious activity is only taking place at the very specific listed file paths and files.

115. It is important that the requested actions be closely coordinated, such that the malicious command and control domains and IP addresses, in various locations, are directed by the Court to be redirected to secure computers immediately upon receipt of any order issued by the Court and/or at a specified time, such that the command and control infrastructure is disabled simultaneously, and the evidence available through the domains and IP addresses is preserved. Delay between execution of the requested actions at various locations may enable the botnet operators to become aware of this action, access the servers in the location that is delayed, move the botnet command and control tier to new, unidentified servers/locations and destroy evidence of their misconduct, their identities and information needed to assist victims in the future. It is also important that the command and control IP addresses be redirected to secure computers placed at the hosting companies, in order to identify connections to any “fallback” infrastructure that Defendants may use in an attempt to resurrect the botnets, which can be disabled at a later date.

116. I have recently investigated the command and control domains and IP addresses in the context of the Zeus Botnets. Based on observing the command and control domains and IP addresses, I conclude that their purpose is solely to support and propagate the Zeus Botnets, as described above and that they further malicious activity through the botnet. If there is content not associated with the Zeus Botnets that is incidentally contained on the servers at the command and control IP addresses, based on my experience as a technologist generally, my work involving Internet security matters and implementation of

prior Court Orders disabling botnet command and control infrastructure, I believe that such content can be moved to new IP addresses, with only negligible impact.

117. It is my opinion that unless the steps described above are taken, the injury caused by the Zeus Botnets will continue and will be compounded, and evidence of Defendants' misconduct and the botnets' operation will be moved or destroyed.

I declare under penalty of perjury under the laws of the United States of America that
the foregoing is true and correct to the best of my knowledge.

Executed this 18th day of March, 2012, in New York, New York.



Mark Debenham

EXHIBIT 1

The Rt Hon Francis Maude MP

Minister for the Cabinet Office and Paymaster General

70 Whitehall

London

SW1A 2AS

Telephone 020 7276 0835

Fax 020 7276 0841

Email psfrancismaude@cabinet-office.gsi.gov.uk

Web www.cabinetoffice.gov.uk

Our Ref: NMP322285

Richard Domingues Boscovich
Microsoft Corporation
One Microsoft Way
Redmond
WA 98052- 6399

8 March 2012

Dear Richard,

Thank you for your letter to James Quinault on behalf of Microsoft Corporation, which requested information on the damage inflicted to the UK Government by malicious software and in particular the Zeus Botnet. I am responding as the Minister responsible for Cyber Security and Information Assurance.

In a strategic context, the UK Government views cyber criminal threats as a key component of a 'tier one' threat to UK national security. In 2010, we allocated an additional £650 million of new investment across Government to enhance our response to such threats, with £63 million specifically allocated to combating cyber crime.

Zeus is one of the most widely used and promiscuous strains of malware in the UK and we have seen compromises (and many attempted compromises) of UK Government and wider public sector systems by Zeus. Instances of Zeus being sent to Government domains are seen on a regular basis and are becoming more common.

In one example from late 2011, Zeus malware attempted to propagate and infect computers on over 50 Government networks, ranging from central Government departments to non-departmental public bodies and local councils. In another attack, an email purporting to be from the White House was sent to a large number of international recipients who were directed to click on a link that then downloaded a variant of Zeus to their computers; the UK Government was also targeted in this attack. In the last 12 months, at least 20 incidents of successful Zeus infections have been seen on UK public sector networks. In the above examples, experts were required to purge the systems of the infections and advice was issued to departments highlighting the ongoing risks of Zeus infection. The remediation of such infections and the continuing protection against them come with significant associated costs, including maintaining specialised staff, response and support capabilities, and keeping systems' security updated. Malware infections also



disrupt services delivered online or via a network connection, as these services are likely to be suspended while a compromise is investigated.

We know that the problem extends beyond central Government networks. One infection by a piece of malware similar to Zeus on the network of a local council is reported to have cost £1.2 million. One UK regional police force's network reportedly became infected with malware similar to Zeus, which resulted in their disconnection from a business critical database for around 3 days. A similar infection was blamed for preventing an NHS hospital trust from booking online appointments for a short period, causing delays in serving patients.

It is difficult to assess accurately the total cost of protecting Government systems against malware infections in general, and Zeus specifically. However, maintaining effective defences against the whole range of current and future threats is essential. A capability to respond to new threats effectively, at pace, and cleanse systems after infection, are a significant and necessary part of business operating and planning costs. It is likely that the total cost to Government of defending our networks against malware runs into many millions of pounds. As the UK Government moves to deliver more public services online, the cost required to defend them will increase further.

I welcome your efforts and hope this note adequately supports your action.

A handwritten signature in black ink, appearing to read "Francis Maude".

FRANCIS MAUDE

EXHIBIT 2

Appendix A

INTERNET COORDINATING BODY

Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601
United States

Entity responsible for coordination of the Internet's systems of unique identifiers, particularly domain names.

DOMAIN NAME REGISTRIES

Verisign Naming Services
21345 Ridgetop Circle
4th Floor
Dulles, Virginia 20166
United States

VeriSign Global Registry Services
12061 Bluemont Way
Reston Virginia 20190
United States

	Harmful Botnet Domain Name	Type	Whois Email Address
1.	uniterace.com	embedded_js	ivernagalindo@uniterace.com
2.	update-kb18628311.com	dropzone, source	atrabaja@peru.com
3.	vacantitechip.com	updater	c/o Verisign
4.	varioldinnics.com	updater	c/o Verisign
5.	vcsturnediana.com	updater	vcsturnediana.com@privacy.above.com
6.	vegatorkspeps.com	updater	c/o Verisign
7.	vemaxxlionna.com	updater	c/o Verisign
8.	vendettamenolkreamste.com	updater	c/o Verisign
9.	vensart.net	dropzone, infector	jonuklm4f2798221092b@w86bna54f21bffa2ff d1.privatewhois.net
10.	vesryop.com	dropzone	perolsp@yahoo.com
11.	soucker.com	dropzone, infector	contact@myprivateregistration.com
12.	strbrst.net	dropzone, infector	meromax@online.ua
13.	xaz6g1bc-server.com	infector	dimalines@yahoo.com
14.	xldavinchireverce.com	infector	xldavinch@gmail.com
15.	xlreservation.com	infector	revstabl77@gmail.com
16.	xtrace-upgrade.com	dropzone	c/o Verisign
17.	xxmagicreservation.com	infector	yarik33@gmail.com
18.	xxxmagicreservation.com	infector	xmagicrv@gmail.com
19.	yettaillarfic.com	updater	repossesseddomain@godaddy.com
20.	youthinktoolovenotneco.com	updater	lauraboschetti@aol.com

21.	ytjsxkupugwfppp.com	infector	ikinybyvetudufy@yahoo.com
22.	ytpfnnmgyjinxrhe.com	infector	drawnmccoy@yahoo.com
23.	zlegalsource.com	infector	zlegal@hotmail.com
24.	zsearchweb.com	infector	zsearch@yahoo.com
25.	answertels.com	dropzone	admin@answertels.com
26.	borrownetpowerlimited.com	updater	c/o Verisign
27.	camesd.com	dropzone, source	perolsp@yahoo.com
28.	cdnsecurehost.com	embedded_js	cadet@fastermail.ru
29.	everyyouneverymecomm.com	dropzone, source, infector	nsrm@register.com
30.	gedpoil.com	dropzone	perolsp@yahoo.com
31.	globalwebz.net	dropzone	admin@macro-store.com
32.	grz942.com	updater	c/o Verisign
33.	grz971.com	updater	admin@macro-store.com
34.	headtickets.com	source	gogo@mailti.com
35.	keevegolyn.com	dropzone	c/o Verisign
36.	marsplus.com	updater	marsplus@mail13.com
37.	nobodyjiomertomcomnet.com	updater	stingomauro@yahoo.com
38.	taemaidoo.com	dropzone, infector	flip@mailae.com
39.	talettedible.com	updater	c/o Verisign
40.	thernextoneter.com	updater	c/o Verisign
41.	thescarts.name	dropzone, infector	livemetal88@hotmail.com
42.	tokiocitus.com	dropzone, infector	atrabaja@peru.com
43.	tongomario.com	dropzone, infector	meromax@online.ua
44.	topsecurityplace.com	dropzone, infector	contact@myprivateregistration.com
45.	totalexcel.net	dropzone	lavionamarkus@yahoo.com
46.	wwwapps-ups.net	infector	sdfdsfdf@126.com
47.	tradingcenter.cc	dropzone, infector	abuse@cinipac.com
48.	trigaproholds.com	dropzone, infector	j.sanchez00000@gmail.com
49.	triplexguard.com	dropzone	triplexg77@ymail.com
50.	tscounter.com	dropzone, infector	nikola@tscounter.com
51.	tuk-tuk.com	infector	chatchai@twoplussoft.com
52.	tventinypoloret.com	dropzone, infector	simonich@inbox.ru
53.	tywinderdamaku.com	updater	c/o Verisign
54.	ufkirankmega.net	dropzone, infector	cxkmg164f2b6d4097e4c@w86bna54f21bffa2ff d1.privatewhois.net
55.	uilveropoly.com	infector	jaunt@free-id.ru
56.	ukrainewskill.com	updater	c/o Verisign
57.	ultragatewealth.com	infector	ultragatew@gmail.com
58.	ultrareservation.com	infector	ultrart5@gmail.com
59.	ultrawirereservation.com	infector	sergiva43@hotmail.com
60.	sepower.net	embedded_js	perolsp@yahoo.com
61.	systrmp.com	infector	west@cutemail.org
62.	sfimnakedgirls.com	infector	percy@mailti.com
63.	shikalmuna.com	dropzone, infector	admin@shanmana.net
64.	shipportlise.com	updater	c/o Verisign
65.	silvarnetinn.com	updater	c/o Verisign
66.	simontfica.com	updater	c/o Verisign
67.	simplychasinasis.com	dropzone, infector	xdr2ea04f2329f1b475e@w86bna54f21bffa2ffd 1.privatewhois.net
68.	skiangpa.net	dropzone, infector	afsmedcla@gmail.com
69.	sludential.com	embedded_js	admin@sludential.com
70.	smartsecurityadvizor.com	dropzone, infector	contact@myprivateregistration.com
71.	smartsecuritybox.com	dropzone, infector	smartbox0001@yahoo.com
72.	sneckstrumo.com	updater	c/o Verisign

73.	softsecuritylab.com	dropzone, infector	ambassador@yahoo.com
74.	somanyontion.com	updater	gmvjcxkxhs@whoisservices.cn
75.	sonyvaio77.com	dropzone, infector, source	gmvjcxkxhs@whoisservices.cn
76.	sqwed.net	dropzone	perolsp@yahoo.com
77.	ssl-autoris.com	embedded_js	voffchih@yandex.ua
78.	stacyeiblerki.com	infector	ease@fxmail.net
79.	sterijncompan.com	updater	c/o Verisign
80.	strongtopguard.com	infector	c/o Verisign
81.	suitionsaway.com	updater	c/o Verisign
82.	sunageoshighvi.com	updater	c/o Verisign
83.	svistoklex.com	dropzone	contact@privacyprotect.org
84.	prlwppsunenofsx.com	infector	apexdomains@hotmail.com
85.	ptsoncmrusnjoew.com	infector	c/o Verisign
86.	quantraxactor.com	updater	c/o Verisign
87.	quardsecurity.com	infector	contact@myprivateregistration.com
88.	quiverharbor.com	infector	quivertip@rocketmail.com
89.	quizclub.net	dropzone	zealot@mail13.com
90.	qwertyghost122245678.com	infector	mordehaigur@yahoo.com
91.	recavatech.com	updater	c/o Verisign
92.	recellhelsen.com	updater	c/o Verisign
93.	reetexista.com	updater	c/o Verisign
94.	repetitirovnet.net	dropzone	ch5m6hg4f2be56c3d025@w86bna54f21bffa2ff d1.privatewhois.net
95.	retuloplopes.net	infector	d0g0r0n@gmail.com
96.	revercestable.com	infector	c/o Verisign
97.	rewriterform.com	dropzone	rewriterform.com@whoisprotectservice.net
98.	rollingthemydicenetbe.com	dropzone, infector, source	nsrm@register.com
99.	runtroadeatb.com	updater	c/o Verisign
100.	saldchwetheach.com	updater	c/o Verisign
101.	sampinv.name	dropzone	k8ie_e86@yahoo.com
102.	sardballierman.com	updater	admin@sardballierman.com
103.	sausandergere.com	updater	marlenehobbsawm@live.co.uk
104.	scarts.name	dropzone, infector	livemetal88@hotmail.com
105.	schoolboygetout.com	infector	gxwx9ur4f2be5929d2e4@w86bna54f21bffa2ff d1.privatewhois.net
106.	sciteleganal.com	updater	c/o Verisign
107.	sdfokoiasedewq.com	updater	admin@sdfokoiasedewq.com
108.	secariadna.com	embedded_js	admin@overseedomainmanagement.com
109.	secstat.com	embedded_js	contact@privacyprotect.org
110.	securitydaemon.com	dropzone, infector	domain.tech@yahoo-inc.com
111.	seeikom.name	dropzone, infector	livemetal88@hotmail.com
112.	seg-opales1.net	dropzone, source, infector	c/o Verisign
113.	sellertop.cn.com	dropzone, infector	livemetal88@hotmail.com
114.	senstonymy.com	updater	c/o Verisign
115.	photalegraza.com	updater	photalegraza.com@privacy.above.com
116.	pintamierback.com	updater	c/o Verisign
117.	planeostsquavep.com	updater	c/o Verisign
118.	polovinkajfie.com	infector	simonich@inbox.ru
119.	poogatodf.com	infector	wind@cutemail.org
120.	portmeadowcapital.com	dropzone	portmeadowcapital.com@domainsbyproxy.co m
121.	pospayinstruzione.com	dropzone	domain.tech@yahoo-inc.com
122.	posta-myposta.com	dropzone	vilonichpotap@yahoo.com
123.	poste-secyre.com	infector, dropzone	gmvjcxkxhs@whoisservices.cn

124.	vibeapnesbu.com	updater	c/o Verisign
125.	viewediesolver.com	updater	c/o Verisign
126.	vigetectrockset.com	updater	c/o Verisign
127.	viimans.com	dropzone, infector	fundomlong@yandex.ru
128.	vipworldhost.com	infector	admin@vipworldhost.com
129.	vzrnrb4o4.com	infector	martin.dudley@live.com
130.	westansgualiti.com	updater	c/o Verisign
131.	westernillusion.com	infector	westill50@gmail.com
132.	whatixemieldin.com	updater	c/o Verisign
133.	whyvavilon.com	infector	admin@whyvavilon.com
134.	wickissievele.com	updater	c/o Verisign
135.	widowadvertising.net	dropzone, infector	va19zm44f2aa71e08338@w86bna54f21bffa2ff d1.privatewhois.net
136.	wopedjhfntzfgh.com	dropzone, infector	wopedjhfntzfgh.com@contactprivacy.com
137.	minollumentlynx.com	updater	c/o Verisign
138.	moderheittrack.com	updater	c/o Verisign
139.	moigerta.cn.com	dropzone, infector	livemetals88@hotmail.com
140.	mspselling.com	infector	csimons@raingroup.com
141.	mutanisopendsie.com	updater	c/o Verisign
142.	muticeptad.com	updater	c/o Verisign
143.	myscarts.name	dropzone, infector	livemetals88@hotmail.com
144.	mywatchresource.com	dropzone, source, infector	admin@mywatchresource.com
145.	nachauserinfo.com	infector	christopherharms17@yahoo.com
146.	nachauser-storeinfo.com	infector	jerrylynnhinnantjr@yahoo.com
147.	nakostelidze.net	source	jlhiluz4f4fb888e24f@w86bna54f21bffa2ffd1. privatewhois.net
148.	national-security-agency.com	infector	lionelmerrdok@yahoo.com
149.	neironhounder.com	infector	tycoon@mail13.com
150.	neoprenolen.com	dropzone	bitbitbord@rocketmail.com
151.	newturbobrowser.com	dropzone	pending-delete@registerapi.com
152.	nobodyjiomertomcomnet.com	updater	stingomauro@yahoo.com
153.	nookbizkitsad.com	infector	hula@mail13.com
	norwitols.com	dropzone	c/o Verisign
154.	nsdnsrv.com	dropzone, infector	dfghrter@hotmail.com
155.	nsonchecks2.com	infector	ghbvsd@msn.com
156.	objectsphereuf.com	infector	grasp@yourisp.ru
157.	oblomidze.net	updater	tf4xsmg4f4bfda8ac864@w86bna54f21bffa2ffd 1.privatewhois.net
158.	onespointheadia.com	updater	c/o Verisign
159.	oposumschoone.com	infector	cool@fxmail.net
160.	oqplss.com	dropzone	phone@wir3s.com
161.	padesionittatu.com	updater	c/o Verisign
162.	panamachnlms.com	embedded_js	admin@panamachnlms.com
163.	patroqualarva.com	updater	c/o Verisign
164.	perisoneterts.com	updater	c/o Verisign
165.	justbigtoys.net	dropzone	doughertyj32@yahoo.com
166.	kenamersoftvu.com	updater	repossesseddomain@godaddy.com
167.	kickthefuture.com	dropzone, infector	domain.tech@yahoo-inc.com
168.	killdfymerraque.com	updater	c/o Verisign
169.	klrtm.com	dropzone, infector	admin@klrtm.com
170.	kristradentro.com	updater	kristradentro.com@privacy.above.com
171.	krivoglazeg.net	updater	pe0id4z4f2b6ace21c71@w86bna54f21bffa2ffd 1.privatewhois.net
172.	layeradv.com	dropzone	ebauacn4f2475b893ed5@w86bna54f21bffa2ff

			d1.privatewhois.net
173.	lekhausurex.com	updater	c/o Verisign
174.	leopodentargit.com	updater	c/o Verisign
175.	level-upgrage.com	dropzone	levelup7@mail.com
176.	lilaussieprems.com	updater	admin@lilaussieprems.com
177.	liverylink.com	updater	c/o Verisign
178.	localdarcenss.com	infector	thorn@mail13.com
179.	locaresplicutl.com	updater	c/o Verisign
180.	lorevingbranta.com	updater	c/o Verisign
181.	lprshcsmijfovp.com	infector	30a2d2f58c3fc4e525e0d212ad23e5c5-1337853@contact.gandi.net
182.	lucascattientop.com	updater	c/o Verisign
183.	lucassfield.com	updater	c/o Verisign
184.	m5ta2bq-server.net	dropzone, infector	m5ta2bq-server.net@contactprivacy.com
185.	managenetwor.com	updater	c/o Verisign
186.	manageopoly.com	infector	boogievoogiescar@ymail.com
187.	marsplus.com	updater	marsplus@mail13.com
188.	maymacngocphuong.com	infector	chodoi1988@gmail.com
189.	mcgoth.com	dropzone, infector	levelupohio@yahoo.com
190.	meazeridashloc.com	updater	c/o Verisign
191.	https04.com	dropzone, infector	contact@myprivateregistration.com
192.	mediacoif.com	source, infector	lulu@cutemail.org
193.	mentripete.com	updater	c/o Verisign
194.	michigan4movies.com	dropzone, infector	newdomains@siteground.com
195.	microbase-update.com	dropzone, infector	chris.deakle82@ymail.com
196.	microsoft-update.name	dropzone, infector	maxpet1212@gmail.com
197.	hoffmarketraph.com	updater	c/o Verisign
198.	holmancybeac.com	updater	c/o Verisign
199.	hosthqk.net	dropzone	admin@hosthqk.net
200.	hunterdriveez.com	infector	expel@cutemail.org
201.	hv673hv573hv53h7khv57.com	dropzone, infector	chris.deakle82@ymail.com
202.	icredoname10012.com	infector	mr.andreev84@bk.ru
203.	ignarysama.com	updater	c/o Verisign
204.	inboxacc.com	dropzone, infector	contact@privacyprotect.org
205.	incode.name	dropzone, infector	contact@privacyprotect.org
206.	indigocrickets.com	infector	watt@bz3.ru
207.	inforksonseia.com	updater	c/o Verisign
208.	intelinellouse.com	updater	c/o Verisign
209.	interponsseella.com	updater	c/o Verisign
210.	investriotinto.com	infector	gmvjcxkxhs@whoisservices.cn
211.	invetechinte.com	updater	c/o Verisign
212.	iserverupdates.com	infector	iserver@gmail.com
213.	jamsulumency.com	updater	c/o Verisign
214.	jdjsaf34.com	infector	admin@jdjsaf34.com
215.	jellabillat.com	updater	c/o Verisign
216.	jinanpharmaceutical.com	dropzone, infector	registry@oderland.se
217.	jobinedianingfo.com	updater	c/o Verisign
218.	jockesnotliked.com	updater	jockesnotliked.com@privacy.above.com
219.	johngottybest.com	dropzone, infector	dale590@aol.com
220.	josunrwpyghvtr.com	infector	ti-samfar@mail.ru
221.	juniordoops.name	dropzone	livemetal88@hotmail.com
222.	gedpoil.com	dropzone	perolsp@yahoo.com
223.	gertyphacqueier.com	updater	c/o Verisign
224.	giftcanbuy.com	dropzone, infector	j_jorge13@yahoo.com

225.	globalwebz.net	dropzone, infector	admin@macro-store.com
226.	globridolumet.com	updater	c/o Verisign
227.	gramablessattro.com	updater	c/o Verisign
228.	grascowallmastmyway.com	dropzone, source, infector	jones@cutemail.org
229.	greatrotewallen.com	embedded_js	v.saluja@aol.com
230.	grounaxyxin.com	updater	grounaxyxin.com@privacy.above.com
231.	grz942.com	updater	c/o Verisign
232.	grz971.com	source, updater	c/o Verisign
233.	gsssoftware5.com	updater	admin@macro-store.com
234.	guppobod.net	dropzone, infector	andpushon@hotmail.com
235.	headtickets.com	updater	gogo@mailit.com
236.	hfcpdaonlines6324.com	updater	c/o Verisign
237.	hhtres.com	dropzone, infector	admin@hhtres.com
238.	highnetlifelentrax.com	updater	highnetlifelentrax.com@domainsbyproxy.com
239.	highnetlifenet.com	dropzone, infector	pearl@mail13.com
240.	high-privacy.com	dropzone	highpriva0@hotmail.com
241.	high-update.com	infector	highlelev7@gmail.com
242.	high-upgrade.com	infector	c/o Verisign
243.	domritu.com	updater	Zhongguancun@yahoo.com
244.	doubbox01.com	updater	c/o Verisign
245.	doutektronumni.com	updater	doutektronumni.com@privacy.above.com
246.	driveplex.net	updater	viola@mail13.com
247.	drontapesoff.com	infector	drontapesoff.com@whoisprotectservice.net
248.	dst-finance.com	dropzone, infector	rw5njrx4f2adcae721b3@w86bna54f21bffa2ffd1.privatewhois.net
249.	dualglobalwave.com	dropzone	dualwave@gmail.com
250.	ebuityketfinus.com	updater	c/o Verisign
251.	eguildaycock.com	updater	c/o Verisign
252.	eponamindranthe.com	updater	c/o Verisign
253.	eunitynewgbc.com	updater	c/o Verisign
254.	europeconsults.com	dropzone	smithers3@yahoo.com
255.	eurostats2012.net	infector	jsl14@live.it
256.	everyyouneverymecomm.com	source	nsrm@register.com
257.	evraffeyplings.com	updater	c/o Verisign
258.	exedrininsteadna.com	updater	c/o Verisign
259.	famontare80.net	dropzone	admin@famontare80.net
260.	favoritopilodjd.com	dropzone, infector	simonich@inbox.ru
261.	federalreserve-online.com	infector	rttresswalo@yahoo.com
262.	federetoktyt.net	dropzone, infector	simonich@inbox.ru
263.	federalwire-report.com	infector	rttresswalo@yahoo.com
264.	fiboxencercha.com	updater	carriefraser@live.co.uk
265.	finewcreautomp.com	updater	finewcreautomp.com@privacy.above.com
266.	flashbangsecurity.com	dropzone, infector	upperhouseblack@yahoo.com
267.	foolieracceiv.com	updater	c/o Verisign
268.	forppp.net	dropzone, infector	plmmvvql@whoisprivacyprotect.com
269.	forviclemo.com	updater	repossesseddomain@godaddy.com
270.	fpzbox.com	dropzone, infector	aeca08c15ce745498efdcef3c7020d4d.protect@whoisguard.com)
271.	frtualpornclub.com	infector	four@mail13.com
272.	conwortonnent.com	updater	conwortonnent.com
273.	copepixell.com	updater	c/o Verisign
274.	cornermarketmedia.com	infector, dropzone	domain.tech@yahoo-inc.com
275.	creamottonovati.com	updater	creamottonovati.com
276.	cronjelaw.com	dropzone, infector	cronjelaw.com

277.	cryogiwogater.com	updater	cryogiwogater.com@privacy.above.com
278.	cuficellimaad.com	updater	marlenehobbsbawm@live.co.uk
279.	cumberiangle.com	updater	c/o Verisign
280.	cyberistrolax.com	updater	cyberistrolax.com@privacy.above.com
281.	daosf3doapo.com	dropzone, infector	firicosl@live.com
282.	dasyucorbit.com	updater	c/o Verisign
283.	dazerfest.com	dropzone	nvpfydgrs@whoisprivacyprotect.com
284.	dbi-static.com	infector	oke2@mail.ru
285.	demanajelo.com	dropzone, source	admin@demanajelo.com
286.	dempeighternya.com	updater	dempeighternya.com@privacy.above.com
287.	deratirelcomni.com	updater	repossesseddomain@godaddy.com
288.	deressenwarpol.com	updater	deressenwarpol.com@privacy.above.com
289.	dnsongchecks3.com	infector	domains@microsoft.com
290.	dogovoridze.net	dropzone	c/o Verisign
291.	brandc.name	dropzone, infector	brandc.name@domainsproxy.name
292.	brigatexgluc.com	updater	c/o Verisign
293.	bringithomedude.com	dropzone, updater	steven.sorn@yahoo.com
294.	brnsounds.cc	dropzone, infector	rastainfo@gmail.com
295.	bryandsighter.com	updater	repossesseddomain@godaddy.com
296.	bxkkuskgdjskdn.com	dropzone	bxkkuskgdjskdn.com@contactprivacy.com
297.	camesd.com	dropzone, source	perolsp@yahoo.com
298.	careolnetcompowerfew.com	dropzone, source, infector	nsrm@register.com
299.	cartapps.com	source, updater	waved@mailti.com
300.	cdkd.net	infector	exsile777@gmail.com
301.	cdnsecurehost.com	embedded_js	cadet@fastermail.ru
302.	cedeophys.com	dropzone	admin@cedeophys.com
303.	celequidictor.com	updater	celequidictor.com@privacy.above.com
304.	chacecipte.com	dropzone	xkcrdqfg@whoisprivacyprotect.com
305.	chbytechipemen.com	updater	chbytechipemen.com@privacy.above.com
306.	chetteaditas.com	updater	c/o Verisign
307.	clingcornem.com	dropzone	admin@clingcornem.com
308.	closedsource.cc	dropzone	c/o Verisign
309.	codecurveopusi.com	dropzone	hut@bz3.ru
310.	036px.com	embedded_js	contact@myprivateregistration.com
311.	108cms.com	source	i.cannot.do.it@gmail.com
312.	1b86a9c7.com	embedded_js	domain.tech@yahoo-inc.com
313.	1nbank.info	source	noqcha@mail.ru
314.	2020films.net	updater	admin@exticie.com.au
315.	24onlinedrug.com	source	24onlinedrug.com@domainnameproxyservice.com
316.	2report-nacha-org.com	source	mzn5z4sihe64xyuvvdsjfncnkylnncxhhxsgqet0vhqndwlc@2report-nacha-org.com.whoisproxy.org
317.	4to4kit.com	dropzone	repossesseddomain@godaddy.com
318.	56pa7bo.com	dropzone	c/o Verisign
319.	73a372rtp.com	dropzone	c/o Verisign
320.	7435424vs.com	dropzone	c/o Verisign
321.	7435474vs.com	dropzone	c/o Verisign
322.	7435924vs.com	dropzone	c/o Verisign
323.	7437424vs.com	dropzone	c/o Verisign
324.	7438424vs.com	dropzone	c/o Verisign
325.	83a372rtp.com	dropzone	c/o Verisign
326.	888778889900.net	updater	c/o Verisign
327.	930nbsdaiodsa.com	dropzone	admin@930nbsdaiodsa.com

328.	aaal-news.net	dropzone	craig@trexmarketing.co.za
329.	aaakiudsnavyq.com	updater	aaakiudsnavyq.com@domainsbyproxy.com
330.	aboutinsurcar.com	dropzone	contact@PrivacyProtect.org
331.	accesslist.net	embedded_js	admin@accesslist.net
332.	ach-files-alert.com	source	contact@myprivateregistration.com
333.	ach-nacha.com	source	info@premiumregistrations.com
334.	accoukierlism.com	updater	c/o Verisign
335.	ach-reports.com	source	Randisnyder33@yahoo.com
336.	ach-transffers-us.com	source	derewsater@yahoo.com
337.	achyoransib.com	updater	c/o Verisign
338.	acrefied.com	dropzone	c/o Verisign
339.	ad1cflg2.com	embedded_js	contact@myprivateregistration.com
340.	administrationistsdug.com	dropzone	admin@ikeainyourmindgiraf.com
341.	advdomain.com	updater	info@advdomains.com
342.	adventurehorde.com	Source	steve@bingotalk.com
343.	adventureineer.com	infector	howellinsuperable@yahoo.com
344.	adventureitect.com	source	howellinsuperable@yahoo.com
345.	adventuremechanic.com	infector	support@neturf.com
346.	adventureriver.net	source	support@neturf.com
347.	adventurerocks.net	source	rowenachauvin@ymail.com
348.	adventureshoal.com	source	accounting@moniker.com
349.	adventureswarm.com	source	rowenachauvin@ymail.com
350.	aephyone.com	dropzone	c/o Verisign
351.	aeractaspac.com	updater	c/o Verisign
352.	afiating.com	dropzone	c/o Verisign
353.	aitgrqfhvmewsys.com	dropzone, infector	g856y7f88nz@nameprivacy.com
354.	ajax-com.net	embedded_js	Domain.tech@yahoo-inc.com
355.	akcakocadetayinsaat.com	source	akcakocadetayinsaat.com@domainsbyproxy.com
356.	alconichill.com	updater	c/o Verisign
357.	aldrorist.com	dropzone	andpushon@hotmail.com
358.	adv-protection.cc	embedded_js	admin@adv-protection.cc
359.	aleorew.com	dropzone	perolsp@yahoo.com
360.	alertedzones.com	dropzone, source, infector	admin@alertedzones.com
361.	alerts-federalresrve.com	source	contact@myprivateregistration.com
362.	alleopneandertal.com	embedded_js	lancasterchemisorb@yahoo.com
363.	allmemoryram.com	source	Anshpat2826@gmail.com
364.	all-nachadatainfo.com	source	christineselva@yahoo.com
365.	all-nacha-datainfo.com	source	crystolwiedeman@yahoo.com
366.	allnacha-users-bank.com	source	allnacha-users-bank.com@contactprivacy.com
367.	americauta.net	updater	contact@webdomainsbyproxy.com
368.	amersterin.com	updater	alanmcwilliams@live.co.uk
369.	angebrethetcombiznet.com	updater	c/o Verisign
370.	anthonydeloso.com	dropzone	anthonydeloso.com@proxy.dreamhost.com
371.	antifraud-check.com	embedded_js	info@antifraud-check.com
372.	antiglobalgg.com	updater	zhongguancun@yahoo.com
373.	anualiverk.com	updater	anualiverk.com@domainsbyproxy.com
374.	applefincorp.net	dropzone, source, infector	gmvjcxkxhs@whoisservices.cn
375.	appscoast.com	dropzone	video@fxmail.net
376.	aquadigita.com	infector	support@hostgator.com
377.	aquaedition.com	source	domains@netfirms.com
378.	aquaJaunt.com	source	barmintual@ymail.com
379.	aquaschooner.com	infector	barmintual@ymail.com
380.	aquaskiff.com	infector	barmintual@ymail.com

381.	aquasloop.com	infector	domains@hugedomains.com
382.	aquasrc.com	source	barmintual@ymail.com
383.	arabeeffect.com	dropzone	c/o Verisign
384.	arctosinbrasilia.com	dropzone	zhongguancun@yahoo.com
385.	armyfloridagames.com	embedded_js	doorkeepernava@yahoo.com
386.	arrested-taxes.com	source	jukioleroa@yahoo.com
387.	artechellirat.com	source	repossesseddomain@godaddy.com
388.	articityxpaqua.com	updater	alanmcwilliams@live.co.uk
389.	aryirs.com	infector	stopgap@ymail.com
390.	asanveni.com	dropzone	the.malware.cabal@gmail.com
391.	askeduptier.com	dropzone	c/o Verisign
392.	assmitizeree.com	updater	assmitizeree.com@privacy.above.com
393.	astinazmen.com	dropzone	c/o Verisign
394.	atbandau.com	dropzone	c/o Verisign
395.	athmainfosolutions.com	source	idreamzsolutions@gmail.com
396.	atlancentuage.com	updater	c/o Verisign
397.	audubideonety.com	updater	c/o Verisign
398.	australia-verse.com	infector	cheryltreinen@yahoo.com
399.	autoparo.com	embedded_js	contact@privacyprotect.org
400.	avaintellegeron.com	updater	susanboyce@live.co.uk
401.	avectintemottis.com	updater	c/o Verisign
402.	azuremator.com	source	accounting@moniker.com
403.	babybertha.com	infector	traffic@intrustdomains.com
404.	backupdomainmuie1245.com	dropzone	admin@backupdomainmuie1245.com
405.	badlike.com	source	texasboy00@rocketmail.com
406.	badthen.com	source	texasboy00@rocketmail.com
407.	badthese.com	source	texasboy00@rocketmail.com
408.	bakboro.com	dropzone, source, infector	chris.deakle82@ymail.com
409.	balticsevicestrust.com	dropzone	admin@weknewthatallthetime.com
410.	bankencryption.net	embedded_js	admin@bankencryption.net
411.	barcodejoyness.com	dropzone	arcade@mailae.com
412.	bariousauk.com	dropzone	andpushon@hotmail.com
413.	barpetra.com	source	barpetra.com@contactprivacy.com
414.	bassyfromsolhost.com	dropzone	admin@bassyfromsolhost.com
415.	battlewright.com	infector	howellinsuperable@yahoo.com
416.	bb4f.net	source	bb4f.net@domainsbyproxy.com
417.	bbbyyygd3yggbc.com	dropzone, infector, updater	laurakels@gmail.com
418.	bedmany.com	source	domains@netfirms.com
419.	bedthese.com	source	d20bj44f259909765df@w86bna54f21bffa2ffd1.privatewhois.net
420.	bedwill.com	source	texasboy00@rocketmail.com
421.	bedwould.com	source	c/o Verisign
422.	beermoth.com	infector	tulukhulhu@yahoo.com
423.	befzdzxfgvvtsjs.com	dropzone, infector	a86af8ue8ca@nameprivacy.com
424.	beggardield.com	dropzone	c/o Verisign
425.	belisimo1.com	dropzone	c/o Verisign
426.	beluga88.com	dropzone, source, infector	zhongguancun@yahoo.com
427.	bertonald.com	dropzone	contact@privacyprotect.org
428.	bestparoels.com	embedded_js	contact@privacyprotect.org
429.	best-trololo.com	dropzone	noreply@centrohost.ru
430.	betterheousermy.com	updater	c/o Verisign
431.	biggestblazer.com	source	wanetka@tlen.pl
432.	biggestchief.com	source	wanetka@tlen.pl

433.	biggestclone.com	source	whois@fastdomain.com
434.	biggestcoin.com	infector	gogofreeze@hushmail.com
435.	biggestfunds.com	infector	gogofreeze@hushmail.com
436.	biggestloop.com	source	e3up3ib4f5a9242cf795@w86bna54f21bffa2ffd 1.privatewhois.net
437.	biggestmaster.com	source	pendingrenewalordeletion@networksolutions.com
438.	biggestmate.com	source	gogofreeze@hushmail.com
439.	biggestioneer.com	source	pendingrenewalordeletion@namesecure.com
440.	biggestpilot.com	source	wanetka@tlen.pl
441.	biggestsetter.com	source	admin@overseedomainmanagement.com
442.	billychalk.com	source	vazzamoon@rocketmail.com
443.	billycharge.com	source	vazzamoon@rocketmail.com
444.	billycheerful.com	source	domains@netfirms.com
445.	billydie.com	source	hostmaster@directnic.com
446.	billydoghouse.com	source	accounting@moniker.com
447.	bisiteles.com	infector	hobbitgod@ymail.com
448.	bitebeehive.com	source	techarts@globalsources.com
449.	biteblew.com	source	pendingrenewalordeletion@networksolutions.com
450.	biteblind.com	source	h6ad4g34f25990771c70@w86bna54f21bffa2ff d1.privatewhois.net
451.	biteblown.com	source	domains@netfirms.com
452.	blestim.com	dropzone	nat.khilkevich@gmail.com
453.	blogoettindia.com	updater	c/o Verisign
454.	blueberrymo.com	updater	blueberrymo.com@privacy.above.com
455.	bluemator.com	source	whois@fastdomain.com
456.	blumswell.com	source	support@neturf.com
457.	boatordenoras.com	updater	alanmcwilliams@live.co.uk
458.	boletin_turistico.com	dropzone	cacueto@comcast.net
459.	borsteksavalu.com	updater	borsteksavalu.com@privacy.above.com
460.	boxtaditp.com	dropzone	iirnn@yahoo.co.uk
461.	brigatexgluc.com	updater	c/o Verisign
462.	broadbandinternetspeedtest.com	source	contact@privacyprotect.org
463.	bryandsighter.com	dropzone, updater	alanmcwilliams@live.co.uk
464.	bstunvzykqqpj.com	dropzone, infector	wv4k596n5se@nameprivacy.com
465.	burneter.com	dropzone	c/o Verisign
466.	burningidea.com	source	jinterva@ucsd.edu
467.	bursayserry.com	dropzone	c/o Verisign
468.	busiene.com	embedded_js	uquirjj@yahoo.com
469.	buttorfos.com	dropzone	admin@buttorfos.com
470.	buut7ar.com	dropzone	c/o Verisign
471.	camesd.com	dropzone	perolsp@yahoo.com
472.	campingrange.com	source	lcjg@citcom.net
473.	campingshelf.com	source	lcjg@citcom.net
474.	campingstack.com	source	lcjg@citcom.net
475.	canceled-transfer.com	source	contact@myprivateregistration.com
476.	cardholder-security.com	source	georgewashere51@yahoo.com
477.	card-security.net	source	card-security.net@contactprivacy.com
478.	careonnetcompowerfew.com	updater	lauraboschetti@aol.com
479.	caronivarium.com	source	spruebeatty@yahoo.com
480.	cartapps.com	updater	waved@mailti.com
481.	cartethont.com	dropzone	gmvjcxkxhs@whoisservices.cn

482.	cavanaghandcompany.com	updater	chriscavanagh@yahoo.com
483.	cccdfgethyn76.com	updater	c/o Verisign
484.	cdnsecurehost.com	embedded_js	cadet@fastermail.ru
485.	cedeophys.com	dropzone	admin@cedeophys.com
486.	celequidictor.com	updater	celequidictor.com@privacy.above.com
487.	chacecipe.com	dropzone	xkcrdqfg@whoisprivacyprotect.com
488.	chapedclothes.com	dropzone	mgfrjjsn@whoisprivacyprotect.com
489.	chbytechipemen.com	updater	chbytechipemen.com@privacy.above.com
490.	chdormante.com	dropzone	chdormante.com@privacy.above.com
491.	checkip4u.net	dropzone, updater	checkip4u@yahoo.com
492.	checkmelater.com	dropzone	bill@haiau.tv
493.	chetteaditas.com	updater	c/o Verisign
494.	chipsiedok.com	source	spruebeatty@yahoo.com
495.	chorinav.com	dropzone	andpushon@hotmail.com
496.	clickhere67.com	dropzone	admin@clickhere67.com
497.	clingcornem.com	dropzone, updater	admin@clingcornem.com
498.	clixa.com	updater	peterbrown@ceneb.com
499.	cloisan.com	dropzone	c/o Verisign
500.	coffien.net	dropzone	admin@coffien.net
501.	coll1.com	dropzone	contact@privacy-protect.cn
502.	coll2.com	dropzone	gasmenqqrr@yahoo.com
503.	coll3.com	dropzone	gasmenqqrr@yahoo.com
504.	colobird.com	source	duckymums@yahoo.com
505.	colocurl.com	infector	duckymums@yahoo.com
506.	colocycle.com	infector	duckymums@yahoo.com
507.	coloquel.com	source	duckymums@yahoo.com
508.	colowheel.com	source	support@neturf.com
509.	combigave.com	source	legal@moniker.com
510.	combigiving.com	infector	korpicscan@skynet.be
511.	combijump.com	source	korpicscan@skynet.be
512.	combimyself.com	source	hostmaster@word.net
513.	combiplease.com	source	korpicscan@skynet.be
514.	complexfix.com	dropzone, source, infector	gmvjcxxhs@whoisservices.cn
515.	connectsharelearn.com	source	eileenroseod@aol.com
516.	conwortonnent.com	updater	conwortonnent.com@privacy.above.com
517.	cooldgaggle.com	source	mariodibattista@gelservicesrl.com
518.	cooldherd.com	source	mariodibattista@gelservicesrl.com
519.	cooldhorde.com	source	mariodibattista@gelservicesrl.com
520.	copelixell.com	updater	c/o Verisign
521.	coralaw.com	infector	admin@coralaw.com
522.	coralaw123.com	infector	c/o Verisign
523.	coreamesents.com	updater	c/o Verisign
524.	corpsecnet.com	dropzone	gmvjcxxhs@whoisservices.cn
525.	crappycrappy123.com	dropzone	da4m97i4f25acc25c2fe@w86bna54f21bffa2ffd1.privatewhois.net
526.	creamottonovati.com	updater	c/o Verisign
527.	cremasl.com	dropzone	c/o Verisign
528.	cronoblinkostarahmake206.net	updater	cronoblinkostarahmake206.net@domainsbyproxy.com
529.	cryogiwigater.com	updater	cryogiwigater.com@privacy.above.com
530.	css-lib.com	embedded_js	robertokelly5@yahoo.com
531.	csspan.net	embedded_js	timfranklin38@yahoo.com
532.	cuficellimaad.com	dropzone, updater	marlenehobbsawm@live.co.uk
533.	cumberiangle.com	updater	c/o Verisign

534.	curcandle.net	source	hostmaster@word.net
535.	curcell.net	source	b6wlpec4f2599056c30f@w86bna54f21bffa2ff d1.privatewhois.net
536.	curcent.com	source	tryagain@tpg.com.au
537.	curchart.com	source	dewus123@embarqmail.com
538.	curvechess.com	source	tryagain@tpg.com.au
539.	curvechild.com	source	printing@laserprinterchecks.com
540.	curvechime.com	source	printing@laserprinterchecks.com
541.	curvechirp.com	source	printing@laserprinterchecks.com
542.	curvechore.com	source	yyjnclx4f259903671a8@w86bna54f21bffa2ffd 1.privatewhois.net
543.	customernacha-tools.com	source	donnawillard57@yahoo.com
544.	cwlrguvioemezr.com	dropzone, infector, source	rn3q264z34h@nameprivacy.com
545.	cyanicuma.com	dropzone	c/o Verisign
546.	cyberistrolax.com	updater	cyberistrolax.com@privacy.above.com
547.	cytomedici.com	dropzone	c/o Verisign
548.	cyytmmlxsthywst.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
549.	da3a4no.com	dropzone	c/o Verisign
550.	dasyucorbit.com	updater	c/o Verisign
551.	Datangoo.com	dropzone	stefan.hoheisel@gmx.net
552.	datejebemupicku.com	dropzone, updater	mihakurcnik@gmail.com
553.	dazerfest.com	dropzone, updater	nvpfydgrs@whoisprivacyprotect.com
554.	dbase-security.com	embedded_js	jfrey43@yahoo.com
555.	dbdata-check.com	dropzone	binder@haiau.tv
556.	dddvdvreb46hj.com	updater	c/o Verisign
557.	debaketo.info	dropzone	c/o Verisign
558.	decalintos.com	source	bitbitbord@rocketmail.com
559.	deepinch.com	dropzone	poltavtzeva.svetlana@yandex.ru
560.	delallosa.com	source	dominios@colombiahosting.com
561.	deligatemynname.com	dropzone	admin@deligatemynname.com
562.	demanajelo.com	dropzone	admin@demanajelo.com
563.	dempeighternya.com	updater	dempeighternya.com@privacy.above.com
564.	denitraspetr.com	updater	admin@denitraspetr.com
565.	deratirelcomni.com	updater	repossesseddomain@godaddy.com
566.	deressenwarpol.com	updater	deressenwarpol.com@privacy.above.com
567.	derkicide.com	dropzone, updater	admin@derkicide.com
568.	desafiodefe.com	source	pastor@desafiodefe.com
569.	dgmrsyrtkosxcjp.com	dropzone, infector	ht8qj6p2277@nameprivacy.com
570.	diandres.com	dropzone	c/o Verisign
571.	diksdirect.com	dropzone	waggner788889@yahoo.com
572.	discount-london-tours.com	dropzone	domain-admin@easily.co.uk
573.	dohturboob.com	source	DOHTURBOOB.COM@domainsbypoxy.com
574.	doliv777.com	dropzone	admin@doliv777.com
575.	doliv7770.com	dropzone	the.malware.cabal@gmail.com
576.	doliv7771.com	dropzone	admin@doliv7771.com
577.	doliv7772.com	dropzone	c/o Verisign
578.	doliv7773.com	dropzone	c/o Verisign
579.	doliv7774.com	dropzone	gmvjcxkxhs@whoisservices.cn
580.	doliv7775.com	dropzone	c/o Verisign
581.	doliv7776.com	dropzone	c/o Verisign
582.	doliv7777.com	dropzone	c/o Verisign
583.	doliv7778.com	dropzone	c/o Verisign
584.	doliv7779.com	dropzone	c/o Verisign
585.	domozhe.com	dropzone	gmvjcxkxhs@whoisservices.cn

586.	domritu.com	updater	zhongguancun@yahoo.com
587.	domsterns.com	embedded_js	admorg122@yahoo.com
588.	donottouchme739.com	dropzone	admin@donottouchme739.com
589.	dotmascript.com	source	kalavernguard@yahoo.com
590.	doublewin.com	dropzone	steven@shalom6000.com
591.	doutektronumni.com	updater	doutektronumni.com@privacy.above.com
592.	dpoougasjkshpms.com	dropzone, source, infector	zy3ar8s37zn@nameprivacy.com
593.	dpouark.com	embedded_js	nhghtrwly@whoisprivacyprotect.com
594.	dqsrneipgzhqkrp.com	dropzone, infector	t57hy5u68dr@nameprivacy.com
595.	drillnews.com	infector	reeks@mailae.com
596.	dsjkkwlhddd.com	dropzone	liberral@gmail.com
597.	dskjhiukwlw.com	dropzone	liberral@gmail.com
598.	dualforcegate.com	source	dualforce@gmail.com
599.	dyaybriaik0.com	dropzone	c/o Verisign
600.	dyaybriaik1.com	dropzone	Monicabrown1911@hotmail.com
601.	dyaybriaik2.com	dropzone	the.malware.cabal@gmail.com
602.	dyaybriaik3.com	dropzone	c/o Verisign
603.	dyaybriaik4.com	dropzone	c/o Verisign
604.	dyaybriaik5.com	dropzone	the.malware.cabal@gmail.com
605.	dyaybriaik6.com	dropzone	the.malware.cabal@gmail.com
606.	dyaybriaik7.com	dropzone	c/o Verisign
607.	dyaybriaik8.com	dropzone	c/o Verisign
608.	dyaybriaik9.com	dropzone	c/o Verisign
609.	dz-greenhat.com	dropzone	repossesseddomain@wildwestdomains.com
610.	eaiitykhxsnkgnqm.com	dropzone, infector	t57hy5u68dr@nameprivacy.com
611.	eartherd.com	source	denunzioanthony@yahoo.com
612.	earthorde.com	source	z42mb88u475@nameprivacy.com
613.	ebaliu.com	dropzone	benedettennodimele@yahoo.com
614.	ebuityketfinus.com	updater	c/o Verisign
615.	edeniu.com	dropzone	c/o Verisign
616.	eeejkcduyrhjv.com	updater	c/o Verisign
617.	efexxxef.com	dropzone	admin@efexxxef.com
618.	efexxxef0.com	dropzone	c/o Verisign
619.	efexxxef1.com	dropzone	the.malware.cabal@gmail.com
620.	efexxxef2.com	dropzone	admin@efexxxef2.com
621.	efexxxef3.com	dropzone	the.malware.cabal@gmail.com
622.	efexxxef4.com	dropzone	c/o Verisign
623.	efexxxef5.com	dropzone	the.malware.cabal@gmail.com
624.	efexxxef6.com	dropzone	c/o Verisign
625.	efexxxef7.com	dropzone	admin@efexxxef7.com
626.	efexxxef8.com	dropzone	c/o Verisign
627.	efexxxef9.com	dropzone	c/o Verisign
628.	eftpsinfo-center.com	source	nicholaswiltz@yahoo.com
629.	eguildaycock.com	updater	c/o Verisign
630.	eieniomxzliljlnj.net	dropzone, infector	rf7ph2w73fw@nameprivacy.com
631.	elekingshop.com	embedded_js	c/o Verisign
632.	elitbasak.com	dropzone	ELITBASAK.COM@domainsbyproxy.com
633.	emerati.com	dropzone	c/o Verisign
634.	encrypted-security-agency.com	embedded_js	noqtcha@mail.ru
635.	encorose.com	dropzone	contact@myprivateregistration.com
636.	eponamindranthe.com	updater	c/o Verisign
637.	erodssmnjjmthnk.net	dropzone, infector	waterscomprehensive@yahoo.com
638.	errorsuz.com	source	support@hostmonster.com

639.	eryirs.com	source	stopgop@ymail.com
640.	eslikerbuna.net	dropzone, source, infector	contact@webdomainsbyproxy.com
641.	etflftvbiwisxnr.com	dropzone, infector	rd9cp4t73dq@nameprivacy.com
642.	eunitynewgbc.com	updater	c/o Verisign
643.	everyyouneverymecomm.com	updater	lauraboschetti@aol.com
644.	evraffeyplings.com	updater	c/o Verisign
645.	evrymonthnighttry.com	source, infector	admin@jajahbinksdiesforyou.com
646.	exedrininsteadna.com	updater	c/o Verisign
647.	faggowh.com	dropzone	admin@mymysteryisle.net
648.	fanzinatra.com	dropzone	amilcarortega@gmail.com
649.	fdic-advantage.com	source	dodsworthmike@yahoo.com
650.	fdic-customeragent.com	source	jeschkemary@yahoo.com
651.	fdiccustomer-news.com	source	c/o Verisign
652.	fdic-insurance.com	source	contact@myprivateregistration.com
653.	fdicnewsforcustomer.com	source	lekpericlendita@yahoo.com
654.	fdicuser-advice.com	source	hollfelderjeff@yahoo.com
655.	facticalry.com	dropzone	c/o Verisign
656.	federalreserve-goverment.com	source	contact@myprivateregistration.com
657.	federalreserve-security.com	source	lionelmerrdok@yahoo.com
658.	federalresrv.com	source	contact@myprivateregistration.com
659.	fgbnutyfhfgjdfghjil.com	dropzone	repossesseddomain@godaddy.com
660.	fheskmrozstshwo.com	dropzone, infector	a35yx3bq2hc@nameprivacy.com
661.	fiboxencercha.com	dropzone, source, updater	carriefraser@live.co.uk
662.	files-irs-pdf.com	source	info@premiumregistrations.com
663.	filmv.net	dropzone	celikseyhmu@gmail.com
664.	finance-customer.com	source	simmonsjames1980@yahoo.com
665.	financedata-store.com	source	cresencioedgar@yahoo.com
666.	financialstatements.mrsdl.com	source	barton@fxmail.net
667.	financialtime.name	dropzone	sukiblyadi@yahoo.com
668.	findnachareport.com	source	gingerellis75@yahoo.com
669.	finewcreautomp.com	updater	finewcreautomp.com@privacy.above.com
670.	firelinesecrets.com	embedded_js	kyvepavavace@yahoo.com
671.	first.lib-invest.net	dropzone	qtu6ta64f2a0ac865ca9@w86bna54f21bffa2ffd 1.privatewhois.net
672.	first.lib-invest1.net	dropzone	the.malware.cabal@gmail.com
673.	first.lib-invest2.net	dropzone	squc6ss4f2b8c8d68f0e@w86bna54f21bffa2ffd 1.privatewhois.net
674.	first.lib-invest3.net	dropzone	ben.jonson88@yahoo.com
675.	first.lib-invest4.net	dropzone	the.malware.cabal@gmail.com
676.	firstdir.cc	embedded_js	brat@mailti.com
677.	fletteeierin.com	dropzone	c/o Verisign
678.	fillmpiphpxpwqeyhj.net	dropzone, source, infector	y77jc7ys7xp@nameprivacy.com
679.	division16000.net	dropzone, source, infector	michalasnick@yahoo.com
680.	flsunstate333.com	updater	flsunstate333.com@domainsbyproxy.com
681.	fmsalberta.com	infector	Reactivation-Pending@enom.com
682.	fmvyywjqlpitous.net	dropzone, infector	d38679a55tn@nameprivacy.com
683.	fnnkwlyvvronqv.net	dropzone, infector	d67rg3d97jp@nameprivacy.com
684.	fokswltine.com	embedded_js	webmaster@thefinhouse.com
685.	fokwsdfrld.com	embedded_js	webmaster@thefinhouse.com
686.	foodwhisky.com	updater	asset@cutemail.org
687.	foolieracceiv.com	updater	c/o Verisign
688.	foreveryouandmee.com	embedded_js	admin@foreveryouandmee.com
689.	forviclemo.com	updater	repossesseddomain@godaddy.com
690.	fpowmtyzqsdfsxl.net	dropzone, infector	js5gx56c7w8@nameprivacy.com

691.	frameworkdisable.com	dropzone, source, infector	gmvjcxkxhs@whoisservices.cn
692.	france-facebook.com	source	delcore@gcn.cx
693.	freac.net	source	colorsandforms@aol.com
694.	freakinas.com	dropzone	admin@freakinas.com
695.	freetreebreamree46364.com	updater	c/o Verisign
696.	fresheurope.com	embedded_js	garykwatterson@solv.net
697.	fretolu.com	dropzone	chris.deakle82@ymail.com
698.	fteur.com	dropzone	waggner788889@yahoo.com
699.	fucktheabuse.com	dropzone, source, infector	john.may24@yahoo.com
700.	furniture-lux.com	dropzone	ordova@ya.ru
701.	fvpluxlvnfktsf.com	dropzone, infector	downingcinerama@yahoo.com
702.	fvxyrrojqrskpvr.com	dropzone, infector	x73v27f67z@nameprivacy.com
703.	gadidthen.com	dropzone	c/o Verisign
704.	gafatys.com	dropzone	gafatys@yahoo.com
705.	gageri.com	dropzone	c/o Verisign
706.	gavildippurum.com	updater	c/o Verisign
707.	gavnoebanoe.com	dropzone	dillingmnnnn@yahoo.com
708.	gavnoebanoe.net	dropzone	gasmenqqrrr@yahoo.com
709.	gdemamaruka.com	dropzone	admin@gdemamaruka.com
710.	gdemamaruka0.com	dropzone	c/o Verisign
711.	gdemamaruka1.com	dropzone	the.malware.cabal@gmail.com
712.	gdemamaruka2.com	dropzone	c/o Verisign
713.	gdemamaruka3.com	dropzone	c/o Verisign
714.	gdemamaruka4.com	dropzone	the.malware.cabal@gmail.com
715.	gdemamaruka5.com	dropzone	c/o Verisign
716.	gdemamaruka6.com	dropzone	c/o Verisign
717.	gdemamaruka7.com	dropzone	c/o Verisign
718.	gdemamaruka8.com	dropzone	c/o Verisign
719.	gdemamaruka9.com	dropzone	c/o Verisign
720.	gedpoil.com	dropzone	perolsp@yahoo.com
721.	gertyphacqueier.com	updater	c/o Verisign
722.	get2-nacha-report.com	source	rogov.vasya@yahoo.com
723.	get-ach-report.com	source	amadasunpatrick@yahoo.com
724.	getcompanyreport.com	source	baomat@dichvubaomattenmien.vn
725.	getnacha-info.com	source	charles boyette@yahoo.com
726.	getnachanews.com	source	info@premiumregistrations.com
727.	get-nacha-news.com	source	get-nacha-news.com@contactprivacy.com
728.	getodkeltyo.com	dropzone	perolsp@yahoo.com
729.	gettingpregnantips.com	source	mihaitaraipan@gmail.com
730.	getworldnewsfast.com	embedded_js	dickensextrovert@yahoo.com
731.	gi0sti.com	updater	bassia1985@gmail.com
732.	getbussinesinfo.com	embedded_js	admin@getbussinesinfo.com
733.	gillettpublishing.com	source, infector	5t1i4f0686@nojunkemailaddress.com
734.	girodiza.com	dropzone	admin@girodiza.com
735.	giupmcehjstwqeqt.com	dropzone, infector	e255f24x5pb@nameprivacy.com
736.	glasseseverydaynow.com	source	admin@jahahbinksiesforyou.com
737.	globalmassretrieval.com	updater	c/o Verisign
738.	globalnxtrereival.com	updater	c/o Verisign
739.	globalwebanalytics.com	dropzone, infector	admin@globalwebanalytics.com
740.	globalwebz.net	dropzone, infector	admin@macro-store.com
741.	globridolumet.com	updater	c/o Verisign
742.	gloomglboom.com	embedded_js	admin@gloomglboom.com
743.	godlikelosers.com	dropzone	binder@haiau.tv

744.	gomosekov.net	dropzone, updater	nizag@mail.ru
745.	gooeylouiecake.com	dropzone	dstieferman@hotmail.com
746.	gordongraduation.com	source	pg9xx6xu7a8@networksolutionsprivateregistration.com
747.	gramablessatro.com	updater	c/o Verisign
748.	grandtarf.com	embedded_js	admin@fastosmile.com
749.	grascowallmastmyway.com	dropzone, source, infector	jones@cutemail.org
750.	grathile.com	dropzone	c/o Verisign
751.	greenballsoft.com	embedded_js	contact@privacyprotect.org
752.	groatcoats.com	dropzone, updater	admin@groatcoats.com
753.	grounaxyxin.com	updater	grounaxyxin.com@privacy.above.com
754.	grz97.com	updater	admin@macro-store.com
755.	grz971.com	updater	admin@macro-store.com
756.	gsobj.net	embedded_js	judith.ebrahim@yahoo.com
757.	gtpgomqbngpjmypr.com	dropzone, infector	c/o Verisign
758.	guishalf.com	dropzone	c/o Verisign
759.	gurmentpass.com	embedded_js	Reactivation-Pending@enom.com
760.	gxxelfrsqtkgry.net	dropzone, infector	c/o Verisign
761.	h2323yrturyuk.com	dropzone	c/o Verisign
762.	hacothailand.com	updater	thewhoisguard@gmail.com
763.	halflife.com	dropzone	halflife.com@contactprivacy.com
764.	hambusb.com	dropzone	c/o Verisign
765.	hatefelony111.com	dropzone, source, infector	john.may24@yahoo.com
766.	hbasdauadhg.com	dropzone	admin@hbasdauadhg.com
767.	heeerr1.com	dropzone	heeerr1.com@contactprivacy.com
768.	heeerr2.com	dropzone	the.malware.cabal@gmail.com
769.	heeerr3.com	dropzone	c/o Verisign
770.	heeerr4.com	dropzone	c/o Verisign
771.	heeerr5.com	dropzone	c/o Verisign
772.	heeerr6.com	dropzone	c/o Verisign
773.	heeerr7.com	dropzone	c/o Verisign
774.	heiotorqmevizmorvvcio.com	dropzone, infector, updater	mikamelio@yahoo.com
775.	hellofromhere98213.com	dropzone	admin@hellofromhere98213.com
776.	hemqmqizxibgkkmk.com	dropzone, infector	wv4k596n5se@nameprivacy.com
777.	hetlittuptuyyyf.com	dropzone, infector	downingcinerama@yahoo.com
778.	hfcpdaonlines6324.com	updater	c/o Verisign
779.	highnetlifeletrasx.com	updater	highnetlifeletrasx.com@domainsbyproxy.com
780.	hjfpknpnzixuxox.com	dropzone, source, infector	wu4an2xy74s@nameprivacy.com
781.	hmqwuxnzwyeqkls.com	dropzone, source, infector	admin@boostsalesguru.com
782.	hoffmarketraph.com	updater	c/o Verisign
783.	hogaric.com	dropzone	c/o Verisign
784.	holmancybeac.com	updater	c/o Verisign
785.	hostei.com	dropzone	abuse@000webhost.com
786.	hotbgirls.com	dropzone	perolsp@yahoo.com
787.	hotrinkolistnetbiz.com	updater	carminatimarina@yahoo.it
788.	hottenmejenetcominfo.com	dropzone, infector, updater	carminatimarina@yahoo.it
789.	howellsheatingandair.com	dropzone	howellsheatingandair.com@protecteddomainservices.com
790.	hpfuqhftxurbsoll.net	dropzone, infector	b52fp2qw5ys@nameprivacy.com
791.	htdellnoiseunivercom.com	dropzone, infector, updater	vmilenacarla@yahoo.com
792.	htdellnoiseunivercou.com	updater	c/o Verisign

793.	htdellnoiseunivercoz.com	updater	m-renewals@register.com
794.	huckside.com	dropzone	c/o Verisign
795.	hugegiantyouth.com	dropzone	admin@ikeainyourmindgiraf.com
796.	hullimpair.com	embedded_js	gmvjcxkxhs@whoisservices.cn
797.	huniloz.com	dropzone	admin@huniloz.com
798.	hunlchemical.com	source	info@premiumregistrations.com
799.	hvlqmwtedesdkktgo.net	dropzone, infector	apprehensivebrandt@yahoo.com
800.	hydroliets.com	dropzone	andpushon@hotmail.com
801.	hygrofi.com	dropzone	c/o Verisign
802.	hzmrnvkbsqqpt.com	dropzone, infector	c/o Verisign
803.	iamnothere823.com	dropzone	admin@iamnothere823.com
804.	iaywtztjwkndfqtm.com	dropzone, infector	z34jb9zq2a5@nameprivacy.com
805.	idina-here.com	dropzone	starbuckqaf@netscape.net
806.	ignarysama.com	updater	c/o Verisign
807.	iigmvqrhotnkqsp.net	dropzone, infector	u583p92r8uv@nameprivacy.com
808.	ijqrqinymhjsvr.net	dropzone, source, infector	c/o Verisign
809.	ijuussvpteexrx.net	dropzone, infector	c/o Verisign
810.	ilovefreewifi.com	dropzone	support@registerfly.com
811.	inboxacc.com	dropzone, source, infector	contact@privacyprotect.org
812.	indigomator.com	source	watervis@planet.nl
813.	indosyslife.com	source	pkarthik24@yahoo.com
814.	inforksonseia.com	updater	c/o Verisign
815.	infrarotendamkevforo.com	dropzone, infector, updater	albanaliaj16@yahoo.com
816.	ingbrownfour.com	infector	bulbulighter@yahoo.com
817.	init-js.com	embedded_js	gildertamra@yahoo.com
818.	inloggen-ing.com	embedded_js	contact@privacyprotect.org
819.	innovazipowenetyunwcz.com	updater	c/o Verisign
820.	insurancepublicliability.net	source	admin@mail2u.com.au
821.	intelinellouse.com	updater	c/o Verisign
822.	interponsseella.com	updater	c/o Verisign
823.	intesasanpaolo.com	embedded_js	hostmaster@intesasanpaolo.com
824.	invetechinte.com	updater	c/o Verisign
825.	invintor.net	dropzone	bornd@yahoo.com
826.	iosahdoias.com	dropzone	admin@iosahdoias.com
827.	ipchecker001.com	dropzone, updater	ipchecker001@yahoo.com
828.	ipchecker002.com	dropzone, updater	admin@overseedomainmanagement.com
829.	ipchecker003.com	dropzone, updater	admin@overseedomainmanagement.com
830.	ipchecker911.com	dropzone, updater	ipchecker911.com
831.	ipuimurqmerpvl.net	dropzone, infector	w72p35dd5tt@nameprivacy.com
832.	irs-00038004800us.com	source	info@premiumregistrations.com
833.	irs-000787002900us.com	source	jukioleroa@yahoo.com
834.	irs-alerts-report.com	source	rp5xmbykruvdbquupu2u0qabfgsvifmjhnqer2 vhsuchyam@irs-alerts-report.com.whoisproxy.org
835.	irs-charge.com	source	irs-charge.com@domainsbyproxy.com
836.	irsdatafilereport.com	source	contact@privacyprotect.org
837.	irs-data-storage.com	source	info@premiumregistrations.com
838.	irs-events.com	source	irs-events.com@contactprivacy.com
839.	irs-reports.com	source	nilonana@yahoo.com
840.	isopect.com	dropzone	c/o Verisign
841.	isportes.com	dropzone	contact@myprivateregistration.com
842.	isslessensual.com	embedded_js	isslessensual.com@privacy.above.com

843.	itimezonenetcomwerytt.com	updater	c/o Verisign
844.	ixvwpvwulcgenlim.com	dropzone, infector	c/o Verisign
845.	iylsorzrjlmsuwy.com	dropzone, infector, source	ns5m23ur84w@nameprivacy.com
846.	jabber911.com	dropzone, updater	jabber911.com@privacy.above.com
847.	jockeydu.com	dropzone	admin@denitraspetr.com
848.	jahsdiuasbdiaa.com	dropzone	admin@jahsdiuasbdiaa.com
849.	jajahbinksdiesforyou.com	source	admin@jajahbinksdiesforyou.com
850.	jambsulumency.com	updater	c/o Verisign
851.	jdfslkjldssd.com	dropzone	liberral@gmail.com
852.	jeancena.com	dropzone	c/o Verisign
853.	jellabillat.com	updater	c/o Verisign
854.	jerikold.com	dropzone	c/o Verisign
855.	jetuodiresbepourtua.com	dropzone	the.malware.cabal@gmail.com
856.	jimpnea.com	dropzone	c/o Verisign
857.	jitteryworld.com	source	jitteryworld.com@contactprivacy.com
858.	jjuegsqqekypjsg.com	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
859.	jlojsunoymwtkjt.com	dropzone, infector	t57hy5u68dr@nameprivacy.com
860.	jobinedianingfo.com	updater	c/o Verisign
861.	jockesnotliked.com	updater	jockesnotliked.com@privacy.above.com
862.	johnsonforums3.com	dropzone	admin@johnsonforums3.com
863.	jollyconcierge.com	dropzone	domain-admin@easily.co.uk
864.	jonathanhaasdesign.com	dropzone	jonhaas@gmail.com
865.	jovamekoz.com	dropzone	jovamekoz@yahoo.com
866.	jpfvgkrioqvnswtn.com	dropzone, infector	bp24s6n2497@nameprivacy.com
867.	jrxuysrpposum.com	dropzone, infector	z39hp8ky6rj@nameprivacy.com
868.	jscripts.net	embedded_js	lindseybowman56@yahoo.com
869.	jsdlfkhusfds.com	dropzone	contact@privacyprotect.org
870.	js-includes.com	embedded_js	morrison_alisha@yahoo.com
871.	js-init.net	embedded_js	jennifer.henderson62@yahoo.com
872.	js-lib.net	embedded_js	susan.haines37@yahoo.com
873.	jsmsgb.com	embedded_js	domain.tech@yahoo-inc.com
874.	jsobj.com	embedded_js	domain.tech@yahoo-inc.com
875.	juiorkbopglrijuy.net	dropzone, source, infector	zy3vb4em6bb@nameprivacy.com
876.	jujuity.com	dropzone	c/o Verisign
877.	julithos.com	dropzone	c/o Verisign
878.	jumemmheavennetcomdre.com	updater	c/o Verisign
879.	junesommerlivey.com	dropzone, source, infector	m-renewals@register.com
880.	justdrv.net	dropzone, infector	admin@macro-store.com
881.	kadonisoft.com	dropzone	admin@kadonisoft.com
882.	kadonisoft0.com	dropzone	c/o Verisign
883.	kadonisoft1.com	dropzone	the.malware.cabal@gmail.com
884.	kadonisoft2.com	dropzone	admin@kadonisoft3.com
885.	kadonisoft3.com	dropzone	kadonisoft3.com@contactprivacy.com
886.	kadonisoft4.com	dropzone	admin@kadonisoft4.com
887.	kadonisoft5.com	dropzone	the.malware.cabal@gmail.com
888.	kadonisoft6.com	dropzone	c/o Verisign
889.	kadonisoft7.com	dropzone	c/o Verisign
890.	kadonisoft8.com	dropzone	c/o Verisign
891.	kadonisoft9.com	dropzone	c/o Verisign
892.	karakumma.com	dropzone, source, infector	admin@buttonfos.com
893.	kdsnrakdvnezxpwq.com	dropzone	contact@privacyprotect.org
894.	kecisygeawayixp.com	dropzone, infector	k63we9nm3yx@nameprivacy.com
895.	kenamersoftvu.com	updater	repossesseddomain@godaddy.com

896.	keorqovrrnetsrfo.com	dropzone, source, infector	k35hx8dk6nc@nameprivacy.com
897.	kgkdominas.com	source	registrar@macrohost.com
898.	khkhkjhiocgsgs.com	dropzone	c/o Verisign
899.	khuvvzqpowtmknby.com	dropzone, infector	yj55n8hw5nb@nameprivacy.com
900.	killdfymerraque.com	updater	c/o Verisign
901.	kilotran.com	dropzone	contact@privacyprotect.org
902.	kjpqetncnrjothzs.net	dropzone, infector, source	d38679a55tn@nameprivacy.com
903.	kniferiddin.com	dropzone	c/o Verisign
904.	knspqntnrlqkeos.net	dropzone, infector	contact@privacyprotect.org
905.	koklip.com	dropzone	tayosaladeen@yahoo.com
906.	koletrezzo44.com	dropzone	repossesseddomain@godaddy.com
907.	koletrezzo55.com	dropzone	repossesseddomain@godaddy.com
908.	koletrezzo66.com	dropzone	koletrezzo66.com@contactprivacy.com
909.	koletrezzo77.com	dropzone	the.malware.cabal@gmail.com
910.	koletrezzo88.com	dropzone	admin@koletrezzo88.com
911.	koletrezzo99.com	dropzone	admin@koletrezzo99.com
912.	kovjmkilwfqmlpws.com	dropzone, infector	u583p92r8uv@nameprivacy.com
913.	kpcpoqyflrdqpr.net	dropzone, infector	ba55f7xs5g6@nameprivacy.com
914.	krewqskynesscompowime.com	updater	c/o Verisign
915.	kristradentro.com	updater	kristradentro.com@privacy.above.com
916.	krivoglazeg.net	updater	pe0id4z4f2b6ace21c71@w86bna54f21bffa2ffd 1.privatewhois.net
917.	kvazimoder.com	dropzone	kvazimoder.com@privacy.above.com
918.	kwalai.com	infector	rnsoe@yahoo.fr
919.	kynhsqpnbjrwvqi.net	dropzone, infector	c/o Verisign
920.	kzqorrmpplugwstm.com	dropzone, source, infector	d38679a55tn@nameprivacy.com
921.	ladybugecards.com	source	studio@rinatgaz.com
922.	lantallyga.com	dropzone	c/o Verisign
923.	layuplaeani.com	dropzone	c/o Verisign
924.	lazysit.net	source	stevehisey@gmail.com
925.	leakedbyzer0.com	dropzone	the.malware.cabal@gmail.com
926.	lekaleo.com	dropzone	perolsp@yahoo.com
927.	lekhauserex.com	updater	c/o Verisign
928.	lenkzetrqvsnk.net	dropzone, infector	wc2ve8y48hv@nameprivacy.com
929.	leopodentargit.com	updater	c/o Verisign
930.	lftrtettnwmmnppmi.com	dropzone, source, infector	apprehensivebrandt@yahoo.com
931.	lhbtbsotjisgvwvp.net	dropzone, infector	n97b76fk87g@nameprivacy.com
932.	lilaussieprems.com	updater	admin@lilaussieprems.com
933.	linindi.com	dropzone	jkcqhygr@whoisprivacyprotect.com
934.	linsela.com	dropzone	c/o Verisign
935.	liviarylink.com	updater	c/o Verisign
936.	lmtljukqunydhxuz.net	dropzone, infector	a35yx3bq2hc@nameprivacy.com
937.	lobsterliveverrolad.com	dropzone, infector, updater	m-renewals@register.com
938.	lobsterliveverromem.com	dropzone, source, infector	m-renewals@register.com
939.	lobsterliveverromez.com	dropzone, infector, updater	admin@overseedomainmanagement.com
940.	locaresplicutl.com	updater	c/o Verisign
941.	loreviningbranta.com	updater	c/o Verisign
942.	loudworld.net	infector	almonarion@rocketmail.com
943.	lpaokum.com	dropzone	c/o Verisign
944.	lpnksckywkyymqh.com	dropzone, infector	hostmaster@above.com
945.	lqhkhqohqsqvjokr.com	dropzone, infector	d97f84nn9rq@nameprivacy.com
946.	lqlktuzitgtghqem.com	dropzone, infector	bx7q476c6sv@nameprivacy.com

947.	lra7nef.com	dropzone	repossesseddomain@godaddy.com
948.	lsthupsocdbncqnn.net	dropzone, infector	rf7ph2w73fw@nameprivacy.com
949.	ltdstar.com	dropzone	admin@ltdstar.com
950.	lucascattientop.com	updater	c/o Verisign
951.	lucassfield.com	updater	c/o Verisign
952.	luckystrike0.com	updater	gmvjcxkxhs@whoisservices.cn
953.	ludos-apparare.com	source	8n6ptzv7oky5psll7ik@f.o-w-o.info
954.	lunedesign.com	embedded_js	lunedesign@mailti.com
955.	lvqdsuimvkxpupro.com	dropzone, infector	kh3te68h3mx@nameprivacy.com
956.	manageality.com	source	accounting@moniker.com
957.	manageient.com	source	boogievoogieoscar@ymail.com
958.	manageity.com	source	boogievoogieoscar@ymail.com
959.	manageium.com	embedded_js	jz95p5cw76d@nameprivacy.com
960.	managenetwor.com	updater	c/o Verisign
961.	martinololo.com	dropzone	admin@ikeainyourmindgiraf.com
962.	mastersili.com	dropzone	contact@zinkhole.org
963.	mastik756bombastik12.com	updater	russelllimbat@yahoo.com
964.	matdugt4.com	dropzone	admin@overseedomainmanagement.com
965.	materryon.com	dropzone	c/o Verisign
966.	mateumer.com	dropzone	c/o Verisign
967.	matoroad.com	infector	huligator@yahoo.com)
968.	matoway.com	infector	huligator@yahoo.com
969.	mctqyvjmcktrmvsw.net	dropzone, source, infector	sw5ct9bh7sg@nameprivacy.com
970.	meandyounow.net	dropzone	bill@haiau.tv
971.	meazeridashloc.com	updater	c/o Verisign
972.	mediacoif.com	infector, source	lulu@cutemail.org
973.	medlya.com	dropzone	chris.deakle82@ymail.com
974.	meinliffenetbizcomzz.com	dropzone, infector, updater	nsrm@register.com
975.	melbamb.com	dropzone	c/o Verisign
976.	meligarm.com	dropzone	meligarm@yahoo.com
977.	mentripete.com	updater	c/o Verisign
978.	meslefot.com	dropzone	perolsp@yahoo.com
979.	metabolez.com	dropzone, infector	admin@macro-store.com
980.	mhjqptzoirgkhhm.com	dropzone, source, infector	k86c98xv6bx@nameprivacy.com
981.	mijningeu.com	embedded_js	zilvinasbutkus@hotmail.com
982.	minienenl.com	embedded_js	info@minienenl.com
983.	minollumentlynx.com	updater	c/o Verisign
984.	misskissoftheryear.net	dropzone	binder@haiau.tv
985.	misternet.com	source	contact@privacyprotect.org
986.	mjmaatmandesigns.com	dropzone	mjmaatmandesigns@gmail.com
987.	mmskwqowxpgtwt.com	dropzone, source, infector	wm6vn79m42s@nameprivacy.com
988.	moderheittrack.com	updater	c/o Verisign
989.	mofoqglsinxslc.com	dropzone, infector	k35hx8dk6nc@nameprivacy.com
990.	moksdog.com	infector	floweflyer@ymail.com
991.	moksfinc.com	infector	floweflyer@ymail.com
992.	mokshark.com	infector	floweflyer@ymail.com
993.	moneancens.com	dropzone	c/o Verisign
994.	mpykqsrhnpitnq.com	dropzone, infector	reasonhickey@yahoo.com
995.	mqjmusjopkvuqnu.com	dropzone, infector	t57hy5u68dr@nameprivacy.com
996.	msrrevukwitgpog.com	dropzone, infector	rn3q264z34h@nameprivacy.com
997.	mtufxdylzvomnub.net	dropzone, infector	xy96q63g6sy@nameprivacy.com
998.	muieptbass.com	dropzone	admin@muieptbass.com
999.	mumbaiescortsdirectory.com	source	baby@baby.com

1000.	musesquad.com	infector	accounting@moniker.com
1001.	mutanisopendsie.com	updater	c/o Verisign
1002.	muticeptad.com	updater	c/o Verisign
1003.	muvpihoovdqvyzh.net	dropzone, infector	wc2ve8y48hv@nameprivacy.com
1004.	muzwniitlpgmpn.com	dropzone, source, infector	mq8ka9m235j@nameprivacy.com
1005.	mvdjeqonofivwurr.com	dropzone, source, infector	qc2bg2669pw@nameprivacy.com
1006.	mvuuorhqhofpwmu.net	dropzone, infector	fraserAfrica@yahoo.com
1007.	myescortsdirectory.com	source	bhupendraacharya@gmail.com
1008.	myhandsareeveryfying.com	dropzone	admin@ikeainyourmindgiraf.com
1009.	mynettube.net	source	sngll_orthnn@hotmail.com
1010.	myrtlebeachscreenprinting.com	source	beachscreenprint@aol.com
1011.	mysubmissionservice.com	source	webmanil@gmail.com
1012.	naberlin.net	dropzone, source, infector	gmvjcxkxhs@whoisservices.cn
1013.	nacha-ach.com	source	nacha-ach.com@contactprivacy.com
1014.	nacha-achalert.com	source	pilomakkie@yahoo.com
1015.	nacha-advertisement.com	source	caillet.victoria@yahoo.com
1016.	nacha-alarm.com	source	nacha-alarm.com@privacy.above.com
1017.	nachabank-users.com	source	nachabank-users.com@contactprivacy.com
1018.	nachabank-usertools.com	source	nachabank-usertools.com@contactprivacy.com
1019.	nacha-cashier.com	source	markskinner56@yahoo.com
1020.	nachaclientsinfo.com	source	lizbethguerrero75@yahoo.com
1021.	nacha-comparison.com	source	floechristine@yahoo.com
1022.	nacha-cosm.com	source	info@premiumregistrations.com
1023.	nacha-creditor.com	source	c/o Verisign
1024.	nacha-customer.com	source	nacha-customer.com@privacy.above.com
1025.	nachacustomer-alarm.com	source	katherinebannan@yahoo.com
1026.	nacha-custmerequipment.com	source	pancharlene@yahoo.com
1027.	nachacustomer-news.com	source	nachacustomer-news.com@privacy.above.com
1028.	nacha-custmertools.com	source	oyerdarrell@yahoo.com
1029.	nachadata-alarm.com	source	nachadata-alarm.com@contactprivacy.com
1030.	nachadataallocation.com	source	nachadataallocation.com@contactprivacy.com
1031.	nachadatafile.com	source	dohertysean20@yahoo.com
1032.	nachadepartment.com	source	garnetzip3456@yahoo.com
1033.	nachaemployee.com	source	sequeiral@rocketmail.com
1034.	nacha-equipmentstore.com	source	pdustin61@yahoo.com
1035.	nacha-feedback.com	source	edwincabrera55@yahoo.com
1036.	nacha-files.com	source	contact@myprivateregistration.com
1037.	nacha-industry.com	source	info@premiumregistrations.com
1038.	nachainfo-store.com	source	kiflombirhane@rocketmail.com
1039.	nacha-info-store.com	source	baomat@dichvubaomattenmien.vn
1040.	nacha-instructionsuser.com	source	qphsrywymt@whoisprivacyprotect.com
1041.	nachanewsarchive.com	source	michellebyrne96@yahoo.com
1042.	nacha-news-archive.com	source	keiserglen@yahoo.com
1043.	nacha-news-download.com	source	carol.brooks85@yahoo.com
1044.	nacha--news-download.com	source	walshshirla@yahoo.com
1045.	nachanewsportal.com	source	admin@overseedomainmanagement.com
1046.	nachanews-portal.com	source	nachanews-portal.com@contactprivacy.com
1047.	nacha-newsportal.com	source	nacha-newsportal.com@contactprivacy.com
1048.	nacha-news-portal.com	source	javaruskijames@yahoo.com
1049.	nacha-news--portal.com	source	tylermelanie47@yahoo.com
1050.	nachaorgcompany.com	source	baomat@dichvubaomattenmien.vn
1051.	nacha-plex.com	source	info@premiumregistrations.com
1052.	nachaport.com	source	arcosmarilyn@yahoo.com

1053.	nacha-port.com	source	mildredeileensparks@yahoo.com
1054.	nachaportal.com	source	marissawienhold@yahoo.com
1055.	nacha-portal.com	source	paul_perrotta@yahoo.com
1056.	nachaportalserver.com	source	nachaportalserver.com@privacy.above.com
1057.	nacha-portal-server.com	source	butlersteve93@yahoo.com
1058.	nacha-rejectedalert.com	source	contact@myprivateregistration.com
1059.	nachareport.com	source	edpwzqbdl3jdafk6xe1xkvff0wlhzzuvwbflqdufs eb1cfalk@nachareport.com
1060.	nacha-report-downlod.com	source	carcinogenicwashingtonum@yahoo.com
1061.	nacha-reporte.com	source	albertha.burke@yahoo.com
1062.	nacha-reports-domain.com	source	nacha-reports- domain.com@contactprivacy.com
1063.	nacha-reportslink.com	source	contact@myprivateregistration.com
1064.	nachaserverportal.com	source	loita10@yahoo.com
1065.	nachaserver-portal.com	source	nachaserver-portal.com@privacy.above.com
1066.	nacha-server-portal.com	source	nacha-server-portal.com@privacy.above.com
1067.	nachasfast-equipment.com	source	long.erik53@yahoo.com
1068.	nacha-shire.com	source	cvarker@ymail.com
1069.	nachasnewsportal.com	source	info@premiumregistrations.com
1070.	nachas-portal.com	source	reginaldsanders86@yahoo.com
1071.	nachasuser-alarm.com	source	neillm68@yahoo.com
1072.	nacha-transferreport.com	source	contact@myprivateregistration.com
1073.	nacha-urgent-portal.com	source	paulbrinkley39@yahoo.com
1074.	nachauser-account.com	source	aida_fairman@yahoo.com
1075.	nacha-userauthorization.com	source	henricksonselena@yahoo.com
1076.	nachauser-banktools.com	source	nachauser-banktools.com@contactprivacy.com
1077.	nacha-userbudget.com	source	dianegibson29@yahoo.com
1078.	nachauser-budgetinfo.com	source	jameswagoner49@yahoo.com
1079.	nacha-usercommission.com	source	raynor_charles@yahoo.com
1080.	nachauser-equipment.com	source	nachauser- equipment.com@contactprivacy.com
1081.	nachauser-estimatefee.com	source	edwardsrandy93@yahoo.com
1082.	nachauser-feedback.com	source	jim80murfuf@yahoo.com
1083.	nachauserinfo.com	source	christopherharms17@yahoo.com
1084.	nachauser-info.com	source	marydurand14@yahoo.com
1085.	nacha--user--news.com	source	charlarichins@yahoo.com
1086.	nachausers-account.com	source	wxcbshvb@whoisprivacyprotect.com
1087.	nacha-usersalarm.com	source	delgadoclaro@yahoo.com
1088.	nachausersalert.com	source	susanswanson51@yahoo.com
1089.	nachausers-bank.com	source	nachausers-bank.com@contactprivacy.com
1090.	nacha-users-bank.com	source	nacha-users-bank.com@contactprivacy.com
1091.	nachausersbluebook.com	source	shoemakerjames88@yahoo.com
1092.	nachausers-book.com	source	witherspoonfranklin@yahoo.com
1093.	nachausers-industry.com	source	robertson.sandra70@yahoo.com
1094.	nacha-users-info.com	source	augustinecontreras@yahoo.com
1095.	nachauser-storeinfo.com	source	jerrylynnhinnantjr@yahoo.com
1096.	nachausers-wirecosts.com	source	vogelsongjosh@yahoo.com
1097.	nachauser-tools.com	source	nachauser-tools.com@contactprivacy.com
1098.	nacha-wirecosts.com	source	flaglerjaime@yahoo.com
1099.	napieriarjournals.com	source	contact@privacyprotect.org
1100.	nastysmell.com	source	prizak@gmail.com
1101.	nationalcity.com	embedded_js	billing@pnc.com
1102.	neoprenant.com	source	neoprenant.com@domainsbyproxy.com
1103.	neoprenhopper.com	source	neoprenhopper.com@privacy.above.com

1104.	neoprenpillar.com	source	c/o Verisign
1105.	nernnkkqxrns.com	dropzone, source, infector	wh6ar6z58hn@nameprivacy.com
1106.	neropisap.com	dropzone	contact@privacyprotect.org
1107.	neweuropeconsult.com	dropzone	faulkner28@yahoo.com
1108.	newhachainfogetnow.com	source	paulbrinkley61@yahoo.com
1109.	newsfig.com	dropzone	whois@bluehost.com
1110.	newsnachausers.com	source	crandellgeorge@yahoo.com
1111.	nexusworldnet.com	embedded_js	ejeytylaoqi@yahoo.com
1112.	nhknrwuo0zndnv.com	dropzone, infector	c/o Verisign
1113.	nholnwtjrdctjr.com	dropzone, infector	wv4k596n5se@nameprivacy.com
1114.	nightycrowlingninjas.com	dropzone	admin@weknewthatallthetime.com
1115.	nilsgriectyed.com	updater	braginikolaj@yandex.com
1116.	nkktqqqtjundslp.com	dropzone, infector	x73v27rf67z@nameprivacy.com
1117.	nmhutixnfriondpo.net	dropzone, source, infector	vf5vt9yz384@nameprivacy.com
1118.	nnpijflsofknlkx.com	dropzone, infector	bx7q476c6sv@nameprivacy.com
1119.	nongoonis.com	dropzone	c/o Verisign
1120.	northdakotastatesite.com	dropzone	citrads@gmail.com
1121.	norwitols.com	dropzone	c/o Verisign
1122.	novodebt.com	dropzone	anatoliylis@yahoo.com
1123.	novodebt.net	dropzone	anatoliylis@yahoo.com
1124.	npxwzlxvrzsxhox.com	dropzone, infector	c/o Verisign
1125.	nrrstlxovkkdc.com	dropzone, infector	mv6sg27r5t@nameprivacy.com
1126.	nsnwrspvpghntwp.com	dropzone, infector	x73v27rf67z@nameprivacy.com
1127.	nssbc-security.cc	embedded_js	felice@mailti.com
1128.	nvfogwptkvheh.com	dropzone, infector, source	ns5m23ur84w@nameprivacy.com
1129.	nwtispzwpgotek.com	dropzone, infector	rf7ph2w73fw@nameprivacy.com
1130.	nylon-kingdom.com	dropzone	webmaster@nylon-kingdom.com
1131.	nyrtsvlqjtsoioq.com	dropzone, infector	js5gx56c7w8@nameprivacy.com
1132.	oceandomore.com	dropzone, source, infector	purvikanji@ymail.com
1133.	okivoob.com	infector	admin@naliora.com
1134.	oldgraber.com	dropzone	the.malware.cabal@gmail.com
1135.	onefrpliteztnh.net	dropzone, infector	y687276j9vh@nameprivacy.com
1136.	onespointheadia.com	updater	c/o Verisign
1137.	onlineshop24blog.com	source	c/o Verisign
1138.	opionisa0.com	dropzone	contact@privacyprotect.org
1139.	oralania.com	dropzone	chris.deakle82@ymail.com
1140.	osforpvqlmpijm.com	dropzone, infector	amadeus logan@yahoo.com
1141.	ouopdvzbjflqozo.net	dropzone, infector	hy4r394j6ja@nameprivacy.com v
1142.	ouovoswqognqrpg.com	dropzone, source, infector	gg6k45nc366@nameprivacy.com
1143.	ovokslvqpwonrww.com	dropzone, source, infector	cr65g2ap483@nameprivacy.com
1144.	p3736t6oa.com	dropzone	c/o Verisign
1145.	p3a32rltp.com	dropzone	c/o Verisign
1146.	p3a372rtp.com	dropzone	c/o Verisign
1147.	p3a377rtp.com	dropzone	c/o Verisign
1148.	p3o3676oa.com	dropzone	c/o Verisign
1149.	p3o36t6oa.com	dropzone	c/o Verisign
1150.	p3o38t6oa.com	dropzone	c/o Verisign
1151.	p9a372rtp.com	dropzone	c/o Verisign
1152.	p9o36t6oa.com	dropzone	c/o Verisign
1153.	pa37rtp.com	dropzone	c/o Verisign
1154.	padesionittatu.com	updater	c/o Verisign
1155.	palaksi.net	dropzone	c/o Verisign
1156.	palonit.com	source	admin@nalorian.com

1157.	panamachnlms.com	embedded_js	admin@panamachnlms.com
1158.	parofin.com	embedded_js	contact@privacyprotect.org
1159.	pasazz.net	updater	Pasazz.net@domainsbypoxy.cco
1160.	patroqualarva.com	updater	c/o Verisign
1161.	pc4hita.com	dropzone	repossesseddomain@godaddy.com
1162.	peindlsadesk.com	dropzone	liberral@gmail.com
1163.	pending-payment.com	source	pending-payment.com@contactprivacy.com
1164.	perisoneterts.com	updater	c/o Verisign
1165.	perveneratio.com	source	lhenderson@gt.rr.com
1166.	pganalytics.net	dropzone, source, infector	admin@macro-store.com
1167.	phasefines.com	dropzone	c/o Verisign
1168.	photalegraza.com	updater	photalegraza.com@privacy.above.com
1169.	picassoss.net	dropzone	bill@haiau.tv
1170.	pinkhatbackup.com	dropzone	the.malware.cabal@gmail.com
1171.	pinkmite.com	infector	cadacadabun@yahoo.com
1172.	pintamierback.com	updater	c/o Verisign
1173.	pirjsqgpmnomxs.com	dropzone, infector	u583p92r8uv@nameprivacy.com
1174.	planeostsquavep.com	updater	c/o Verisign
1175.	planevipescort.com	infector	mckeesummon@yahoo.com
1176.	platinumhd.tv	source	linda.clements@platinumhd.tv
1177.	plhypjumukjupk.com	dropzone, source, infector	dd3t93pu55u@nameprivacy.com
1178.	plwfryqvvhvoiuyr.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
1179.	pnltnksxsswzkk.net	dropzone, source, infector	d38679a55tn@nameprivacy.com
1180.	po3t6oa.com	dropzone	c/o Verisign
1181.	pofikpofikfikfik.com	dropzone	gmvjcxkxhs@whoisservices.cn
1182.	pofikpofikfikfik0.com	dropzone	c/o Verisign
1183.	pofikpofikfikfik1.com	dropzone	admin@pofikpofikfikfik1.com
1184.	pofikpofikfikfik2.com	dropzone	admin@pofikpofikfikfik2.com
1185.	pofikpofikfikfik3.com	dropzone	pofikpofikfikfik3.com@contactprivacy.com
1186.	pofikpofikfikfik4.com	dropzone	c/o Verisign
1187.	pofikpofikfikfik5.com	dropzone	c/o Verisign
1188.	pofikpofikfikfik6.com	dropzone	the.malware.cabal@gmail.com
1189.	pofikpofikfikfik7.com	dropzone	c/o Verisign
1190.	pofikpofikfikfik8.com	dropzone	c/o Verisign
1191.	pofikpofikfikfik9.com	dropzone	c/o Verisign
1192.	pontviewer.com	embedded_js	js7oz4o4ea6938faa70c@oqjj874d9300d54bd9 5.privatewhois.net
1193.	pooletleyep.com	dropzone	c/o Verisign
1194.	poptarinto.com	embedded_js	ylynokybeduresal@yahoo.com
1195.	pornxyx.com	dropzone, updater	ybxrfdvsvy@whoisprivacyprotect.com
1196.	portalnchas.com	source	admin@overseedomainmanagement.com
1197.	portsterba.com	dropzone	c/o Verisign
1198.	potixmssufpuurl.com	dropzone, source, infector	zm4j68fm3ze@nameprivacy.com
1199.	pquoixuzoaxolmof.net	dropzone, infector	x73v27f67z@nameprivacy.com
1200.	ppuqvsssgniwpy.net	dropzone, source, infector	y687276j9vh@nameprivacy.com
1201.	primedyl.com	dropzone, updater	admin@primedyl.com
1202.	proaxistherapy.com	updater	maverickg@maverickgarrett.com
1203.	projens.com	dropzone	venubr@gmail.com
1204.	promoshuffle.com	source	promoshuffle.com@domainsbypoxy.com
1205.	pszwxwuyyhmktouj.net	dropzone, infector	c/o Verisign
1206.	pultaine.com	dropzone	c/o Verisign
1207.	pupikola.com	dropzone	c/o Verisign
1208.	pvhweojsmnnpqov.com	dropzone, source, infector	rd9cp4t73dq@nameprivacy.com
1209.	pxpnksrwoqmjzotk.com	dropzone, infector	epossesseddomain@godaddy.com

1210.	pxtnbziashnulfgu.com	dropzone, infector	em4xy6bx7a7@nameprivacy.com
1211.	pygmance.com	dropzone	c/o Verisign
1212.	qhumrnslklxtixrv.com	dropzone, infector	amadeus_logan@yahoo.com
1213.	qlxxrxjoeqppwir.com	dropzone, infector	yt8ng93c3tb@nameprivacy.com
1214.	qnvryodunlmlj.com	dropzone, infector	f868g9ck5pk@nameprivacy.com
1215.	qpmuqqpdprpqhkf.com	dropzone, source, infector	y77jc7ys7xp@nameprivacy.com
1216.	qtmjwghrgmloamt.com	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
1217.	qualitta.com	source	soporte@m mindsetco.com
1218.	quantraxactor.com	updater	c/o Verisign
1219.	quickreportnacha.com	source	googlprofil@yahoo.com
1220.	quick-report-nacha.com	source	1vcipylyzyb0gifsml27kvbk4ubd59t2llpga7x1z bvxgebn0@quick-report-nacha.com
1221.	quiverain.com	infector	quivertip@rocketmail.com
1222.	quivercove.com	source	quivertip@rocketmail.com
1223.	quiverforge.com	infector	quivertip@rocketmail.com
1224.	quiverform.com	infector	quivertip@rocketmail.com
1225.	quiversea.com	infector	hostmaster@above.com
1226.	quiverwave.com	infector	quivertip@rocketmail.com
1227.	qulqhpiornuvltp.com	dropzone, infector	uz9u78n867p@nameprivacy.com
1228.	qwdxkgpcwpolrlrh.com	dropzone, infector	dd3t93pu55u@nameprivacy.com
1229.	qwhmtksyqlohccxk.net	dropzone, infector	hy4r394j6ja@nameprivacy.com
1230.	qxprnprccrajhxtt.com	dropzone, infector	vv73a9jm5wh@nameprivacy.com
1231.	qzltljpkvrndtwq.net	embedded_js	exytihazonac@yahoo.com
1232.	racindo.com	dropzone	c/o Verisign
1233.	ragsmile.com	source	finkka@verizon.net
1234.	ragsmog.com	source	finkka@verizon.net
1235.	ragsmoke.com	source	finkka@verizon.net
1236.	ragsmug.com	source	RAGSMUG.COM@domainsbyproxy.com
1237.	ragsnake.com	source	c/o Verisign
1238.	ragsnip.com	source	9l78ko4f2ab5db9ff67@w86bna54f21bffa2ffd1. privatewhois.net
1239.	ragsnipe.com	source	hostmaster@word.net
1240.	ragsnub.com	source	whois@fastdomain.com
1241.	randomawdowibda.com	dropzone	dmin@randomawdowibda.com
1242.	randomawidnao.com	dropzone	admin@randomawdowibda.com
1243.	randomnamefordomain1.com	dropzone	p3u2mpj4f23c3aeb29ad@w86bna54f21bffa2ff d1.privatewhois.net
1244.	raz43op.com	dropzone	c/o Verisign
1245.	rcktiqotpsulzlz.net	dropzone, source, infector	bx7q476c6sv@nameprivacy.com
1246.	rcspknmpzqmukfnl.net	dropzone, infector	g856y7f88nz@nameprivacy.com
1247.	readmedocument83.com	dropzone	admin@readmedocument83.com
1248.	recavatech.com	updater	c/o Verisign
1249.	recellhelsen.com	updater	c/o Verisign
1250.	reetexista.com	updater	c/o Verisign
1251.	reflectivelayer.com	source	dexnet@dextech.com
1252.	rejectedach-report.com	source	luticeferrio@yahoo.com
1253.	rekqbepytokpfol.com	dropzone, infector	rf7ph2w73fw@nameprivacy.com
1254.	relationshipamersoftwarevu.com	dropzone	repossesseddomain@godaddy.com
1255.	rembranddt.com	dropzone	bill@haiau.tv
1256.	repetitirovnet.net	dropzone	ch5m6hg4f2be56c3d025@w86bna54f21bffa2ff d1.privatewhois.net
1257.	report-007298492us.com	source	info@premiumregistrations.com
1258.	report-nacha.com	source	contact@myprivateregistration.com
1259.	reportnachaapprove.com	source	info@premiumregistrations.com

1260.	reports-federalreserve.com	source	loresrias@yahoo.com
1261.	reports-info.com	source	reports-info.com@contactprivacy.com
1262.	reportsnacha.com	source	ronaldfedders@yahoo.com
1263.	reports-nacha.com	source	rckjv82i68uomyhlkydzqm2ytan8dxaykcv8xb1 hyz35ifew@reports-nacha.com.whoisproxy.org
1264.	reserveddomain.com	updater	09520379481034- a5d04a@whoisprivacyservices.com.au
1265.	resolym.com	dropzone	plvhghqyhd@whoisprivacyprotect.com
1266.	restramerer.com	dropzone	c/o Verisign
1267.	rghnyofujnqgqejiw.com	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
1268.	rheady.com	dropzone	c/o Verisign
1269.	rhunseal.com	dropzone	admin@rhunseal.com
1270.	rjrqkzujejjpfyq.com	dropzone, infector	thurmanpang@yahoo.com
1271.	rksiuojplkkovqk.com	dropzone, infector	k87td33t8xf@nameprivacy.com
1272.	rkwwnrqrpiqymvj.com	dropzone, infector	c/o Verisign
1273.	rmhkrrufvxjoznp.com	embedded_js	erivegutixo@yahoo.com
1274.	rmoytrpxmloeogk.com	dropzone, infector	vf5vt9yz384@nameprivacy.com
1275.	rmsjsuhunyjivg.com	dropzone, source, infector	a35yx3bq2hc@nameprivacy.com
1276.	rnmmmpqjzipxip.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
1277.	rolermpyhvnrrhp.com	dropzone, infector	uvitydareqanyha@yahoo.com
1278.	rollingthemydicenetbe.com	updater	lauraboschetti@aol.com
1279.	romario279.com	dropzone	romariodonate@hotmail.com
1280.	runtroadeatb.com	updater	c/o Verisign
1281.	rwmxtdoequwoyop.net	dropzone, source, infector	c/o Verisign
1282.	ryljzfmxdmqrpfog.net	embedded_js	exytihazonac@yahoo.com
1283.	rzvqvoiqlpnkln.com	dropzone, infector	c/o Verisign
1284.	s0ndell.net	dropzone	admin@s0ndell.net
1285.	sa67634dt.com	dropzone	c/o Verisign
1286.	sa69634dt.com	dropzone	c/o Verisign
1287.	sa6n634dt.com	dropzone	c/o Verisign
1288.	sa6n884dt.com	dropzone	c/o Verisign
1289.	sa7n634dt.com	dropzone	richardpalmer90@yahoo.com
1290.	sackbatfish.info	dropzone	c/o Verisign
1291.	sadclapped.com	source	sadclapped.com@domainsbyp proxy.com
1292.	sadjumped.com	source	bibermoot@ymail.com
1293.	sadlooked.com	infector	bibermoot@ymail.com
1294.	sadmissed.com	source	bibermoot@ymail.com
1295.	safeinetscripts.net	dropzone	admin@secwaystorage.net
1296.	safesaction.com	embedded_js	vinovao@yahoo.ca
1297.	sahhosse.com	embedded_js	Reactivation-Pending@enom.com
1298.	saldchwettheach.com	updater	c/o Verisign
1299.	saln634dt.com	dropzone	c/o Verisign
1300.	san34dt.com	dropzone	c/o Verisign
1301.	santeconference.com	source	santeconference.com@domainsbyp proxy.com
1302.	rouxiety.com	dropzone	c/o Verisign
1303.	royhnnqrumycqtq.com	dropzone, source, infector	n63pv6wx9jq@nameprivacy.com
1304.	rrhxilokmjytnlmy.com	dropzone, infector	c/o Verisign
1305.	rrvnxnioefttgrw.net	dropzone, infector	yj55n8hw5nb@nameprivacy.com
1306.	rshqaohvmqrkfo.com	dropzone, infector	exorbitantbonilla@yahoo.com
1307.	rumbt.com	dropzone	anatoliyliis@yahoo.com
1308.	rumbt.net	dropzone	anatoliyliis@yahoo.com
1309.	sardballierman.com	updater	admin@sardballierman.com
1310.	sausandergere.com	updater	marlenehobbsawm@live.co.uk
1311.	saxtumi.com	dropzone	c/o Verisign

1312.	schoolboygetout.com	infector	gxwx9ur4f2be5929d2e4@w86bna54f21bffa2ff d1.privatewhois.net
1313.	sciteleganal.com	updater	c/o Verisign
1314.	scqnipltesymwqn.net	dropzone, infector	hostmaster@above.com
1315.	sddkoios.com	dropzone	sdfgsdfghf@msn.com
1316.	secariadna.com	embedded_js	admin@overseedomainmanagement.com
1317.	secstat.com	embedded_js	contact@privacyprotect.org
1318.	secur3storag3.com	dropzone	b6349815@klzlk.com
1319.	secure-cibc.com	embedded_js	jwcasher@gmail.com
1320.	securedfrag888.com	updater	andpushon@hotmail.com
1321.	secureloggin.net	embedded_js	admin@secureloggin.net
1322.	secureweb5ervice5.net	dropzone	admin@secwaystorage.net
1323.	securewebtests.com	embedded_js	falkenstire@yahoo.com
1324.	securitychecking.com	embedded_js	admin@securitychecking.com
1325.	securitylkins.com	embedded_js	justinporten@yahoo.com
1326.	securitywebguard.com	embedded_js	admin@security-defense.com
1327.	secwaystorage.net	dropzone	admin@secwaystorage.net
1328.	seg-opales1.net	dropzone	c/o Verisign
1329.	senstonymy.com	updater	c/o Verisign
1330.	senvironment.com	embedded_js	snvironment@mail.com
1331.	seppower.net	embedded_js	perolsp@yahoo.com
1332.	seqrutry.com	embedded_js	angelasavina@yahoo.com
1333.	serlene.com	dropzone	gmvjcxkxhs@whoisservices.cn
1334.	setteredradi.com	dropzone	c/o Verisign
1335.	shgkgwgkls.com	dropzone	liberral@gmail.com
1336.	shippoltise.com	updater	c/o Verisign
1337.	silvarnetinn.com	updater	c/o Verisign
1338.	simontfica.com	updater	c/o Verisign
1339.	skinze.com	dropzone	jtmdrwze@gmail.com
1340.	skjbldkjksfhu.com	dropzone	liberral@gmail.com
1341.	slqorykvknmerkz.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
1342.	sludential.com	embedded_js	admin@sludential.com
1343.	sneckstrumo.com	updater	c/o Verisign
1344.	sntdr-services.cc	embedded_js	c/o Verisign
1345.	so47nop.com	dropzone	kristynlauner@yahoo.com
1346.	soa4gol.com	dropzone	nyenaiwilliams@yahoo.com
1347.	softmarketvalu.com	embedded_js	c/o Verisign
1348.	softmarketvalue.com	embedded_js	kovic26@gmail.com
1349.	softthrifty.com	embedded_js	melodimatkovic26@gmail.com
1350.	somanyontion.com	updater	c/o Verisign
1351.	somebackupdomain123.com	dropzone	admin@somebackupdomain123.com
1352.	sonnersbale.com	dropzone	gmvjcxkxhs@whoisservices.cn
1353.	sop3not.com	dropzone	jaffemizell@yahoo.com
1354.	sorbentoiq.com	updater	zanuidaaa@yahoo.com
1355.	sotkmnqjeoxqlun.com	dropzone, infector	cz99x6ay7h2@nameprivacy.com
1356.	spectums.com	dropzone	meromax@online.ua
1357.	splashnetcombizauron.com	dropzone, source, infector, updater	albanaliaj16@yahoo.com
1358.	splatsplit.com	infector	support@name.com
1359.	splatspunk.com	infector	hostmaster@word.net
1360.	splatstamp.com	source	klausstork@earthlink.net
1361.	squoajponbtekil.com	dropzone, infector	yj55n8hw5nb@nameprivacy.com
1362.	sqrzdjjwmlvger.net	dropzone, infector	c/o Verisign
1363.	sqwed.net	dropzone	perolsp@yahoo.com

1364.	srepolik20.com	dropzone	contact@privacyprotect.org
1365.	srimeenakshiagencies.com	source	klmn.mohan@gmail.com
1366.	srqirlswrglcmr.net	dropzone, infector	ts8fn4bw89r@nameprivacy.com
1367.	srztrvrrnomsuyzp.net	dropzone, infector, source	c/o Verisign
1368.	sshwklwjjen.com	dropzone	liberral@gmail.com
1369.	ssl-autoris.com	embedded_js	voffchih@yandex.ua
1370.	stamperglut.com	dropzone	c/o Verisign
1371.	standinghost.com	embedded_js	gmvjcxkxhs@whoisservices.cn
1372.	startalertmos.com	infector	accounting@moniker.com
1373.	startancientmos.com	infector	romewarior@ymail.com
1374.	statusonline.net	embedded_js	admin@statusonline.net
1375.	stattime.net	embedded_js	admin@stattime.net
1376.	sterientai.com	dropzone	c/o Verisign
1377.	sterijnccompan.com	updater	c/o Verisign
1378.	sticumed.com	dropzone	c/o Verisign
1379.	strohertinzeocomne.com	dropzone, infector, updater	carminatimarina@yahoo.it
1380.	stylendeco.com	source	hslee0220@yahoo.com
1381.	suitionsaway.com	updater	c/o Verisign
1382.	sukablyatimes.com	source	krishnamistry73@yahoo.com
1383.	sunageoshighvi.com	updater	c/o Verisign
1384.	sunaitenprin.com	dropzone	the.malware.cabal@gmail.com
1385.	sustadodo.com	dropzone	c/o Verisign
1386.	svistoklex.com	dropzone	contact@privacyprotect.org
1387.	swsskhpcqzskn.com	dropzone, infector	v56dt2ey98u@nameprivacy.com
1388.	sybilladi.com	dropzone	c/o Verisign
1389.	sythpvoxjztvgp.com	dropzone, infector	wv4k596n5se@nameprivacy.com
1390.	t3a3dor.com	dropzone	c/o Verisign
1391.	t3os7pt.com	dropzone	titus.christopher@yahoo.com
1392.	ta4n6ar.com	dropzone	c/o Verisign
1393.	takers.aaa1-news.net	dropzone	craig@trexmarketing.co.za
1394.	takethatasano.com	dropzone	admin@weknewthatallthetime.com
1395.	talettedible.com	updater	c/o Verisign
1396.	tbmtwulmmswpzxzi.com	dropzone, source, infector	c/o Verisign
1397.	teerersoru.com	dropzone	c/o Verisign
1398.	teleation.com	infector	hobbitgod@ymail.com
1399.	telelope.com	infector	hobbitgod@ymail.com
1400.	telemonor.com	source	hobbitgod@ymail.com
1401.	teleoso.com	infector	hobbitgod@ymail.com
1402.	telephonemeonmyphone.com	source	admin@telephonemeonmyphone.com
1403.	temptypath.com	dropzone	c/o Verisign
1404.	teqgemscqbllmi.com	dropzone, infector	a37zk7bv7v3@nameprivacy.com
1405.	terabitscenter.cn.com	updater	livemetal88@hotmail.com
1406.	tfogtwprtluqcup.com	dropzone, infector	c/o Verisign
1407.	the557sdeee.com	dropzone	admin@the557sdeee.com
1408.	the557sdeee0.com	dropzone	c/o Verisign
1409.	the557sdeee1.com	dropzone	admin@the557sdeee1.com
1410.	the557sdeee2.com	dropzone	the.malware.cabal@gmail.com
1411.	the557sdeee3.com	dropzone	c/o Verisign
1412.	the557sdeee4.com	dropzone	c/o Verisign
1413.	the557sdeee5.com	dropzone	the.malware.cabal@gmail.com
1414.	the557sdeee6.com	dropzone	c/o Verisign
1415.	the557sdeee7.com	dropzone	c/o Verisign
1416.	the557sdeee8.com	dropzone	c/o Verisign

1417.	the557sdeee9.com	dropzone	c/o Verisign
1418.	theavtechs.com	updater	theavtechs.com@domainsbyproxy.com
1419.	theimageshare.com	dropzone	dns@videotron.ca
1420.	thernextoneter.com	updater	c/o Verisign
1421.	thesoftcheap.com	embedded_js	melodimatkovic26@gmail.com
1422.	throatylot.com	dropzone	c/o Verisign
1423.	timandjenny.com	updater	info@goldencarat.com
1424.	tlurionwxgynem.net	dropzone, infector	w72p35dd5tt@nameprivacy.com
1425.	tngvtxvwmkhirmfk.com	dropzone, source, infector	hy4r394j6ja@nameprivacy.com
1426.	tnoqypxnyijgyiss.net	dropzone, infector	equilateralfranklin@yahoo.com
1427.	to365mo.com	dropzone	c/o Verisign
1428.	to3rtol.com	dropzone	c/o Verisign
1429.	toobershmui.cjb.net	dropzone	cjb@cjbmanagement.com
1430.	toplaitit.com	embedded_js	bet222win@gmail.com
1431.	tpaprrtltpust.com	dropzone, infector	mx6np6jy4dc@nameprivacy.com
1432.	tpsuyknjrhxwswp.com	dropzone, source, infector	c/o Verisign
1433.	tqulloqrypweqhj.com	dropzone, infector	mclainfibrosis@yahoo.com
1434.	transersouthyouth.com	infector	mckeesummon@yahoo.com
1435.	transfer-canceled.com	source	derewsater@yahoo.com
1436.	transfers-ach.com	source	dstvpbwbr@whoisprivacyprotect.com
1437.	trawwers.comlu.com	dropzone	awex@hostprince.com
1438.	tremunicu.co	dropzone	c/o Verisign
1439.	tripolefourgaz.com	dropzone	admin@ikeainyourmindgiraf.com
1440.	trucktrumpet.com	infector	marvol@gmx.net
1441.	trucktugboat.com	source	annie@dentand.com
1442.	trucktulip.com	infector	riverrat@rochester.rr.com
1443.	trucktwirl.com	source	trucktwirl.com@privacy.above.com
1444.	truckunzip.com	source	hostmaster@word.net
1445.	trupledoublehardcore.com	source	admin@jajahbinksdiesforyou.com
1446.	truwofhvwlmsiv.com	dropzone, infector	d97f84nn9rq@nameprivacy.com
1447.	tskktvrxjsqopqo.com	dropzone, infector	f76ah7cb472@nameprivacy.com
1448.	ttgtwmittvsqapo.com	dropzone, infector	wm6vn79m42s@nameprivacy.com
1449.	tubehub.net	dropzone	dean@lakefrontmedia.net
1450.	tuzhjntonrszdews.net	dropzone, infector	k87td33t8xf@nameprivacy.com
1451.	tweetwinner.com	source	support@neturf.com
1452.	twistloft.com	source	rmzf5vi4f25da87bd976@w86bna54f21bffa2ffd 1.privatewhois.net
1453.	twistplex.com	source	twistplex.com@domainsbyproxy.com
1454.	typqgihpjroteqj.net	dropzone, infector	k35hx8dk6nc@nameprivacy.com
1455.	tywinderdamaku.com	updater	c/o Verisign
1456.	tzmaxi.com	dropzone	c/o Verisign
1457.	ufrlmuknqvopf.com	dropzone, infector	w72p35dd5tt@nameprivacy.com
1458.	uhahaka.com	dropzone, source, infector	admin@uhahaka.com
1459.	uhnouomrrxqjsth.com	dropzone, source, infector	de69d4d63er@nameprivacy.com
1460.	uitqfowjrhwtrzkx.com	dropzone, infector	xy96q63g6sy@nameprivacy.com
1461.	ukrainewskill.com	updater	c/o Verisign
1462.	uljnnlhshkhkldt.com	dropzone, infector	kh3te68h3mx@nameprivacy.com
1463.	ulowzvirxysntmyn.com	dropzone, infector	yj55n8hw5nb@nameprivacy.com
1464.	umwmpwulypvdok.com	dropzone, source, infector	mw73n8ed7n4@nameprivacy.com
1465.	undercovermimimi.com	dropzone	admin@ikeainyourmindgiraf.com
1466.	uosvzyppolqpjmql.net	dropzone, source, infector	k63we9nm3yx@nameprivacy.com
1467.	uptonxtwealth.com	source	uptonxtw@gmail.com
1468.	urbantoprtnitiesforme.com	source	admin@jajahbinksdiesforyou.com
1469.	ursubstootin.com	dropzone	c/o Verisign

1470.	urthcpdotfrkxp.net	dropzone, infector	cb3mu9k97eu@nameprivacy.com
1471.	usa-itunes.com	source	marina.santa13@yahoo.com
1472.	us-ccsecurity.com	source	info@premiumregistrations.com
1473.	us-credit-security.com	source	info@premiumregistrations.com
1474.	userbrick.com	source	capri@mail13.com
1475.	userdata-distribute.com	source	userdata-distribute.com@contactprivacy.com
1476.	userinfo-nacha.com	source	richardmeggers@yahoo.com
1477.	usernacha-alarm.com	source	tahboub_m@yahoo.com
1478.	usernacha-bills.com	source	info@premiumregistrations.com
1479.	usernacha-wireinfo.com	source	info@premiumregistrations.com
1480.	usersea.com	embedded_js	bunts@fxmail.net
1481.	utugkoykmwjquzg.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
1482.	uvxzzkspqxfpqpls.com	dropzone, infector	jr7v53ge4pk@nameprivacy.com
1483.	uxqpvcmoqxyutkp.net	dropzone, infector	rd9cp4t73dq@nameprivacy.com
1484.	uzkrtoomtnjpoohn.com	dropzone, infector	kh3te68h3mx@nameprivacy.com
1485.	vacantitechip.com	updater	c/o Verisign
1486.	valuetory.com	infector	jorimelodey@yahoo.com
1487.	var357.com	embedded_js	contact@myprivateregistration.com
1488.	varioldinnics.com	updater	c/o Verisign
1489.	vasexz1fhjklwa.com	dropzone	j.c.angeldeath@ymail.com
1490.	vasexzfhjklwa.com	dropzone	j.c.angeldeath@ymail.com
1491.	vavasasvb1klwa.info	dropzone	c/o Verisign
1492.	vavvb1klwa.com	dropzone	j.c.angeldeath@ymail.com
1493.	vcsturnediana.com	updater	vcsturnediana.com@privacy.above.com
1494.	veandlifronanonetworkceq.com	updater	c/o Verisign
1495.	vegatorkspeps.com	updater	c/o Verisign
1496.	vemaxxlionna.com	updater	c/o Verisign
1497.	veonset.com	dropzone	admin@naliora.com
1498.	veriary.net	infector	jessemccurdy@yahoo.com
1499.	veroabelos0.com	dropzone	quiz@mailae.com
1500.	vesryop.com	dropzone	perolsp@yahoo.com
1501.	vetricomneticejestreq.com	updater	paolosassi71@yahoo.com
1502.	vfrqsiekewtckden.com	dropzone, infector	wv4k596n5se@nameprivacy.com
1503.	vibeapnesbu.com	updater	c/o Verisign
1504.	victori1.net	dropzone	admin@victori1.net
1505.	viewcheapestways.com	embedded_js	af32tgf4ea6939035bd3@oqjj874d9300d54bd9 5.privatewhois.net
1506.	viewediesolver.com	updater	c/o Verisign
1507.	viewfdiccustomer.com	source	llekperic@yahoo.com
1508.	vigetectrockset.com	updater	c/o Verisign
1509.	vikingwer5.com	dropzone	salts@mailti.com
1510.	vincent-world.com	source	kasinakosfine@yahoo.com
1511.	vipplacetv.com	infector	paulacobb56@yahoo.com
1512.	virgull.com	dropzone	jhnvns.92@googlemail.com
1513.	vivaforelifenetcombie.com	updater	vivaforelifenetcombie.com@domainsbyproxy.com
1514.	vizonix.com	source	gu79p6a88z8@networksolutionsprivateregistration.com
1515.	vjzljyvmvqhflrlj.com	dropzone, infector	contact@privacyprotect.org
1516.	vkrrllufqweinm.net	dropzone, infector, source	c/o Verisign
1517.	vpxquhxtxhnqrfrm.com	dropzone, infector	screechydorsey@yahoo.com
1518.	vqitqvunhrevlso.com	dropzone, infector	dt6gh2wj339@nameprivacy.com
1519.	vqpfmhsplytsgejg.com	dropzone, infector	wv4k596n5se@nameprivacy.com
1520.	vqwpyeyyxjhxgri.com	dropzone, infector	z34jb9zq2a5@nameprivacy.com

1521.	vrgoryutlnqjpod.com	dropzone, infector	visitus@bitandjazzdanceclub.com
1522.	vrkmifksfoqungwu.com	dropzone, infector	b52fp2qw5ys@nameprivacy.com
1523.	vulxkncvstfukrow.com	dropzone, infector	d67rg3d97jp@nameprivacy.com
1524.	vvxriolskjgrsrs.net	dropzone, source, infector	k87td33t8xf@nameprivacy.com
1525.	wantpint.com	dropzone	the.malware.cabal@gmail.com
1526.	waweaime.com	dropzone, updater	admin@waweaime.com
1527.	wealthnxtreimbursement.com	updater	c/o Verisign
1528.	wealthnxtupdate.com	infector	c/o Verisign
1529.	webjanse.com	source	newdomains@siteground.com
1530.	weddingbee.com	dropzone	mknapp@internetbrands.com
1531.	weighan.com	dropzone	c/o Verisign
1532.	westansgualiti.com	updater	c/o Verisign
1533.	westarray.com	infector, source	kitkatwilou@yahoo.com
1534.	westdirect.net	dropzone	attic@cutemail.org
1535.	westernunlon.net	source	westernunlon.net@privacy.aboab.com
1536.	westwiserce.com	updater	c/o Verisign
1537.	wgewygkn.com	dropzone	contact@privacyprotect.org
1538.	whatixemieldin.com	updater	c/o Verisign
1539.	wheredoyouplayloveme.com	dropzone, infector, updater	pescifabio83@yahoo.fi
1540.	whitemite.com	infector	hexagenoid@yahoo.com
1541.	white-shopping.com	dropzone	viscolas@gmail.com
1542.	whole-sale2011.com	dropzone, source, infector	real.host50@yahoo.com
1543.	wickissievele.com	updater	c/o Verisign
1544.	winlaps.net	dropzone, source, infector	gmvjcxkxhs@whoisservices.cn
1545.	wmmwemptyjpqymfl.net	dropzone, infector	rf7ph2w73fw@nameprivacy.com
1546.	womidfer.com	dropzone	abc1234@qq.com
1547.	wonderchat.net	dropzone, infector	admin@macro-store.com
1548.	wonderfulworn.com	source	wonderfulworn.com@privacy.above.com
1549.	wonderfulwreath.com	source	coortus@t-online.hu
1550.	wonderfulwrench.com	source	hostmaster@word.net
1551.	wonderfullyard.com	source	lacq1ud4f088961d534d@ojijj874d9300d54bd95.privatewhois.net
1552.	wrmultsorqrjsolp.com	dropzone, source, infector	a86af8ue8ca@nameprivacy.com
1553.	wtuqiwwqsskojuft.com	dropzone, infector	benavideseuripides@yahoo.com
1554.	wviosppfhslqyyvn.com	embedded_js	exytihazonac@yahoo.com
1555.	wvzvdjbqpinqg.net	dropzone, source, infector	pt8gt97u8x5@nameprivacy.com
1556.	atlas57.com	dropzone, updater	random68@live.com
1557.	backorderru.com	dropzone, updater	contact@PrivacyProtection.org
1558.	france-facebook.com	dropzone, infector, updater	delcore@gcn.cx
1559.	h2024700065.com	updater	H2024700065.COM@domainsbyproxy.com
1560.	kwalai.com	source	rnsoe@yahoo.fr
1561.	nacha-rejected.com	source	frt57pmkq4fiu7sslywrvoallyyzd8fmegonkpawnnx05ky0c@nacha-rejected.com.whoisproxy.org
1562.	wznrifvicsjpbnv.com	dropzone, infector	c/o Verisign
1563.	xndmnojimsojqx.net	dropzone, infector	su3tc7gw94s@nameprivacy.com
1564.	xpadv.net	embedded_js	cgecexq4f3e77137f2ab@w86bna54f21bffa2ffd1.privatewhois.net
1565.	xpousnnulhihoer.com	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
1566.	xprlxottijelpvl.com	dropzone, infector	r793d9ww3fr@nameprivacy.com
1567.	xviadovjlyhltry.com	dropzone, source, infector	u65dt7q82a7@nameprivacy.com
1568.	xxvwinjqarjnw.com	dropzone, infector	dt6gh2wj339@nameprivacy.com

1569.	yazarcanyucel.com	source	bjk_habibe_22@hotmail.com
1570.	yettaillarfic.com	dropzone, updater	repossesseddomain@godaddy.com
1571.	yftuomlonknooigt.net	dropzone, infector	c/o Verisign
1572.	ymrhuvwgpfmscvf.com	dropzone, source, infector	c/o Verisign
1573.	you-ach-report.com	source	stevecremers@yahoo.com
1574.	younggirlsdomovie.com	dropzone	mantaphosting@gmail.com
1575.	younona.com	dropzone	contact@privacyp protect.org
1576.	yournachareport.com	source	melissaarnott93@yahoo.com
1577.	your-nacha-report.com	source	boggskarla@ymail.com
1578.	ypqgwphsfjinoqau.com	dropzone, infector	c/o Verisign
1579.	ypqhrijclijnnoyg.net	dropzone, source, infector	tu2f838h73z@nameprivacy.com
1580.	yregmst.com	embedded_js	contact@myprivateregistration.com
1581.	ytmvsfsijnxjnm.net	dropzone, infector	vv73a9jm5wh@nameprivacy.com
1582.	ytpseiqmednislds.com	dropzone, infector	kh3te68h3mx@nameprivacy.com
1583.	ywilkswylnvufje.net	dropzone, source, infector	c/o Verisign
1584.	ywtgytkejnke.com	dropzone	liberral@gmail.com
1585.	zauxszqulsxryw.com	dropzone, source, infector	sw5ct9bh7sg@nameprivacy.com
1586.	zfpvulopppyywmuf.com	dropzone, source, infector	cr65g2ap483@nameprivacy.com
1587.	ziiditnmcmlyjp.net	dropzone, source, infector	gv9st8nk4ka@nameprivacy.com
1588.	zjhwjnpkxqtjlqq.com	dropzone, infector, source	am9zr2nq3p8@nameprivacy.com
1589.	zjsnoklkbethqkpt.com	dropzone, source, infector	armeniangillespie@yahoo.com
1590.	zkqgrwspdxuuuprcm.net	dropzone, source, infector	k86c98xv6bx@nameprivacy.com
1591.	zooourglprftvqkd.com	dropzone, source, infector	k87td3t8xf@nameprivacy.com
1592.	zqffthhnuiwonkz.net	dropzone, source, infector	e255f24x5pb@nameprivacy.com
1593.	zqnirpqupuqmknsq.com	embedded_js	exytihazonac@yahoo.com
1594.	zuvqpubgmmqrdskd.com	dropzone, source, infector	c/o Verisign
1595.	zxyopetnzktkknd.com	dropzone, infector	yj55n8hw5nb@nameprivacy.com
1596.	zzgpmmzspzrtzood.com	dropzone, infector	ch67e4ve6tz@nameprivacy.com
1597.	123002915.cn.com	infector, dropzone	livemetal88@hotmail.com
1598.	423654m.cn.com	infector, dropzone	livemetal88@hotmail.com
1599.	90fd78b9078bd0g.com	infector, dropzone	oi@ppmail.ru
1600.	98DFGR994883798df.com	infector, dropzone	jenny@fxmail.net
1601.	googlezuju.com	infector	liuwei1000@gmail.com
1602.	accoukierlism.com	updater	c/o Verisign
1603.	acheacad.com	dropzone	keys@fxmail.net
1604.	achyroransib.com	updater	c/o Verisign
1605.	activedent.net	infector, dropzone	achuleta_salomon@yahoo.com
1606.	advdomain.com	updater	info@advdomains.com
1607.	aeractraspac.com	updater	c/o Verisign
1608.	aeronitrex.com	infector	aeronitro@ymail.com
1609.	akronislt.com	infector	jcv_s@yahoo.com
1610.	alconichill.com	updater	c/o Verisign
1611.	all-nacha-datainfo.com	infector	crystolwiedeman@yahoo.com
1612.	amberschool.com	infector, dropzone	alisonspencer95@yahoo.com
1613.	amberschool2.com	infector, dropzone	brooksallen71@yahoo.com
1614.	amersterin.com	updater	repossesseddomain@godaddy.com
1615.	analyticdns.com	infector, dropzone	dfghrter@hotmail.com
1616.	angebrethetcombiznet.com	updater	c/o Verisign
1617.	anissaeve.com	infector	0f9ecd140a1612330b421f33ef9ffae5@domain discreet.com
1618.	answertels.com	dropzone	admin@answertels.com
1619.	antiglobalgg.com	dropzone, source, infector	zhongguancun@yahoo.com
1620.	antiglobalgg2.com	updater	c/o Verisign
1621.	antisorit.cn.com	infector, dropzone	livemetal88@hotmail.com

1622.	anualiverk.com	updater	anualiverk.com@domainsbyproxy.com
1623.	aptitude.name	infector, dropzone	contact@privacyprotect.org
1624.	aquaedition.com	infector	domains@netfirms.com
1625.	aquaJaunt.com	infector	barmintual@ymail.com
1626.	aquaskiff.com	dropzone	barmintual@ymail.com
1627.	aquaSrc.com	infector	barmintual@ymail.com
1628.	ariodtalk.com	infector	admin@vistapromblog.com
1629.	articityxpqua.com	dropzone, source, updater	alanmcwilliams@live.co.uk
1630.	assmitizeree.com	updater	assmitizeree.com@privacy.above.com
1631.	astrawebservice.com	infector	astraweb@gmail.com
1632.	asus7.com	updater	gmvjcxkxhs@whoiservices.cn
1633.	atlancentuage.com	updater	c/o Verisign
1634.	au-business-customer.com	infector	krolando26@yahoo.com
1635.	audubideonety.com	updater	c/o Verisign
1636.	avectintemottis.com	updater	c/o Verisign
1637.	quizclub.net	dropzone	zealot@mail13.com
1638.	rollingthemydicenetbe.com	dropzone, infector, source	lauraboschetti@aol.com
1639.	secstat.com	embedded_js	contact@privacyprotect.org
1640.	seppower.net	embedded_js	perolsp@yahoo.com
1641.	sludential.com	embedded_js	admin@sludential.com
1642.	springautumnernetbiz.com	updater	c/o Verisign
1643.	sqwed.net	dropzone	perolsp@yahoo.com
1644.	teamten.net	updater	vomit@mail13.com
1645.	vesryop.com	dropzone	perolsp@yahoo.com
1646.	yagijakes.com	dropzone	c/o Verisign
1647.	youthinktoolovenotneco.com	updater	lauraboschetti@aol.com
1648.	level-3.net	dropzone	contact@myprivateregistration.com
1649.	edge02.net	dropzone	perezbrittany93@yahoo.com
1650.	core02.net	dropzone	ada.shapiro@yahoo.com
1651.	basedmarket.com	dropzone, infector	swansonjudy83@yahoo.com
1652.	basic-auth.com	embedded_js	admin@basic-auth.com
1653.	battlewright.com	dropzone	howellinsuperable@yahoo.com
1654.	bespar.net	infector	mousaviseehr@yahoo.com
1655.	bestlongnet.net	dropzone, infector	d0g0r0n@gmail.com
1656.	bestvideoworld.com	dropzone, infector	contact@myprivateregistration.com
1657.	betswinstrategy.cn.com	dropzone, infector	livemetal88@hotmail.com
1658.	betterheousermy.com	updater	c/o Verisign
1659.	biggestcoin.com	dropzone	gogofreeze@hushmail.com
1660.	biggestfunds.com	dropzone	gogofreeze@hushmail.com
1661.	billycheerful.com	infector	c/o Verisign
1662.	billyd.com.au	infector	c/o Verisign
1663.	bisiteles.com	dropzone	hobbitgod@ymail.com
1664.	bisonbuy.com	infector	gvgkqqrsm@whoisprivacyprotect.com
1665.	blackbuckseri.com	infector	seamy@mail13.com
1666.	blogoettindia.com	updater	c/o Verisign
1667.	blueberrymo.com	updater	blueberrymo.com@privacy.above.com
1668.	boatorldenoras.com	dropzone, source, updater	repossesseddomain@godaddy.com
1669.	borsteksavalu.com	updater	borsteksavalu.com@privacy.above.com
1670.	hppp://173.44.34.184/el/load/load.exe		sysop@iptelligent.com
1671.	tolbarqueries-google2.net		vshostmaster@verisign.com
1672.	bestlongnet.net		d0g0r0n@gmail.com
1673.	retiyulopoples.net		d0g0r0n@gmail.com
1674.	retiyulopoples.net		d0g0r0n@gmail.com

1675.	tynegertyonioloki.net		vshostmaster@verisign.com
1676.	esterraspacom		webmaster@sunstream.com
1677.	savetimeon.com		tswzyyx4f21e81bead5f@w86bna54f21bffa2ffd1.privatewhois.net
1678.	sdfkj348923rl1131.com		vshostmaster@verisign.com
1679.	fds323rwe48237rhkaj.com		brianbrodyjr@yahoo.com
1680.	11132erfw23rwqasfd.com		11132erfw23rwqasfd.com@domainsbyproxy.com
1681.	asiasoniconline.com		superpuper56@yahoo.com
1682.	sdfkjkfdsklf34j348.com		atlon_atlon@yahoo.com
1683.	fds32jfkwj43rewf3r.com		vshostmaster@verisign.com
1684.	11132erfw23rjkvsdf.com		atlon_atlon@yahoo.com
1685.	justbigtoys.net		doughertyj32@yahoo.com
1686.	downloadertempfull.net		atlon_atlon@yahoo.com
1687.	savetimeforyoulife2011.net		atlon_atlon@yahoo.com
1688.	freejumpcomptell.com		atlon_atlon@yahoo.com
1689.	freesecuritycheckname.net		atlon_atlon@yahoo.com
1690.	alabamaislandsfree.net		atlon_atlon@yahoo.com
1691.	asiasoniconline.com		superpuper56@yahoo.com
1692.	sdfkjkfdsklf34j348.com		atlon_atlon@yahoo.com
1693.	fds32jfkwj43rewf3r.com		vshostmaster@verisign.com
1694.	11132erfw23rjkvsdf.com		atlon_atlon@yahoo.com
1695.	asiasoniconline.com		superpuper56@yahoo.com
1696.	sdfkjkfdsklf34j348.com		atlon_atlon@yahoo.com
1697.	fds32jfkwj43rewf3r.com		vshostmaster@verisign.com
1698.	11132erfw23rjkvsdf.com		atlon_atlon@yahoo.com
1699.	ksljdflka23.com		billhrodriguez18423@gmail.com
1700.	sjxu297x-a.com		vshostmaster@verisign.com
1701.	yho-finan-ce-update.com		vshostmaster@verisign.com
1702.	g297xx-n.com		vshostmaster@verisign.com
1703.	tronopays.com		bobgolfsen@yahoo.com

**National Internet Exchange of India
 5th Floor, Incube Business Centre, 18, Nehru Place
 New Delhi Delhi 110 019
 India**

**Afilias Limited
 C/O Afilias USA, Inc.
 300 Welsh Road, Building 3
 Suite 105
 Horsham, PA 19044
 United States**

	Harmful Botnet Domain Name	Type	Whois Email Address
1704.	prodano.in	dropzone, infector	shishakov@inbox.ru
1705.	abrakadabradomen000.in	dropzone	donalbreen456@yahoo.com
1706.	abrakadabradomen001.in	dropzone	donalbreen456@yahoo.com
1707.	poydun.in	source	global_76@mail.ru
1708.	massa195.in	dropzone	abuseriiditenahuy@gmail.com
1709.	testofiesto0.in	dropzone	abuseriiditenahuy@gmail.com
1710.	hullamulla.in	dropzone	abuseriiditenahuy@gmail.com
1711.	trackerlohaaa.in	dropzone	abuseriiditenahuy@gmail.com
1712.	astaloscojonesback.net.in	dropzone	nemesys@nice.tld
1713.	ipwnbotsforfun.net.in	dropzone	c/o Afilias
1714.	pacman.net.in	dropzone	g4hosting@safe-mail.net
1715.	pacmanback.in	dropzone	c/o Afilias
1716.	indietours.in	dropzone	adrian4love@ymail.com
1717.	indietours.net.in	dropzone	c/o Verisign
1718.	indietoursbck.in	dropzone	adrian4love@ymail.com
1719.	indietoursbck.net.in	dropzone	c/o Afilias
1720.	indietoursbck1.in	dropzone	c/o Afilias
1721.	indietoursbck2.in	dropzone	c/o Afilias
1722.	getwolrdnewsfast.in	embedded_js	dickensextrovert@yahoo.com
1723.	bhbbhbaa6536.in	dropzone	abuseriiditenahuy@gmail.com
1724.	pppllllmdkjt2.in	dropzone	abuseriiditenahuy@gmail.com
1725.	kasoblanaka.in	embedded_js	albanovsergey@yahoo.com
1726.	zabaz.in	infector	global_76@mail.ru
1727.	coltrc.in	infector	cryasan@mail.ru
1728.	domennow.in	infector	cryasan@mail.ru
1729.	yferro.in	infector	cryasan@mail.ru
1730.	googlemaster921203.in	dropzone	admin@contentserver.ru
1731.	itismybestsite2277.in	dropzone	c/o Afilias
1732.	itismybestsite2323.in	dropzone	admin@contentserver.ru
1733.	itismybestsite2377.in	dropzone	c/o Afilias
1734.	kjrldsghslekjhgl.in	dropzone	c/o Afilias
1735.	mybackdomain8732.in	dropzone	admin@contentserver.ru
1736.	mybackdomain8733.in	dropzone	c/o Afilias
1737.	mylifeissogood.in	dropzone	admin@contentserver.ru
1738.	supportonline-posta.in	embedded_js	rsfallonMcdowell@yahoo.com
1739.	shopsoft.in	dropzone	swpower@gmail.com
1740.	c0r3.in	dropzone	dragan.plavsic91@live.com
1741.	millioneti.net.in	dropzone, updater	g4hosting@safe-mail.net
1742.	alibabadropshipping.in	embedded_js	donalbreen456@yahoo.com

1743.	itismybestsite.in	dropzone	admin@contentserver.ru
1744.	itismybestsite111.in	dropzone	admin@contentserver.ru
1745.	itismybestsite222.in	dropzone	c/o Afilias
1746.	itismybestsite333.in	dropzone	c/o Afilias
1747.	itismybestsite444.in	dropzone	c/o Afilias
1748.	postepaysystem.in	dropzone	admin@contentserver.ru
1749.	adoult-zonasjk.in	dropzone	c/o Afilias
1750.	myjabba.in	dropzone	franklinsheena@yahoo.com
1751.	myjabbaer.in	dropzone	c/o Afilias
1752.	myjabbaerer.in	dropzone	c/o Afilias
1753.	serpentarikn.in	dropzone	pro@postingscript.com
1754.	serpentarin.in	dropzone	pro@postingscript.com
1755.	wallsway15.in	source	luckyluc@mail.ru
1756.	zazazar.in	source	labasonova@mail.ru
1757.	slonoboy.in	source	albanovsergey@yahoo.com
1758.	garik-m.in	source	albanovsergey@yahoo.com
1759.	journalmy.in	source	labasonova@mail.ru
1760.	kurpin.in	source	a1931190@jnxjn.com
1761.	yellowpageschennai.in	source	thegreenvision@yahoo.in

**DotAsia Organisation Ltd.
15/F, 6 Knutsford Terrace
Tsim Sha Tsui Kowloon
Hong Kong**

	Harmful Botnet Domain Name	Type	Whois Email Address
1762.	achnachajournaldownload.asia	source	timsmith@astro-tek.com
1763.	ach-nacha-report-downloadshop.asia	source	timsmith@astro-tek.com
1764.	achnachareviewfiledownload.asia	source	timsmith@astro-tek.com
1765.	bestach-nacha-report-download.asia	source	timsmith@astro-tek.com
1766.	mynacha-filereport.asia	source	timsmith@astro-tek.com
1767.	nachafilereport.asia	source	timsmith@astro-tek.com
1768.	nacha-filereportonline.asia	source	timsmith@astro-tek.com
1769.	nacha-filereportsite.asia	source	timsmith@astro-tek.com
1770.	nacha-filereportstore.asia	source	timsmith@astro-tek.com
1771.	newnacha-filereport.asia	source	timsmith@astro-tek.com
1772.	theach-nacha-report-download.asia	source	timsmith@astro-tek.com

.CO Internet S.A.S.
Calle 100 8 A - 49
Torre B of 507
Bogotá
Colombia

NeuStar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

NeuStar, Inc.
Loudoun Tech Center
46000 Center Oak Plaza
Sterling Virginia 20166
United States

	Harmful Botnet Domain Name	Type	Whois Email Address
1773.	betterheousermy.co	updater	c/o NeuStar
1774.	blogogettindia.co	updater	c/o NeuStar
1775.	boatorldenoras.co	updater	c/o NeuStar
1776.	borsteksalu.co	updater	c/o NeuStar
1777.	thernextoneter.co	updater	c/o NeuStar
1778.	tywinderdamaku.co	updater	c/o NeuStar
1779.	ukrainewskill.co	updater	c/o NeuStar
1780.	vacantitechip.co	updater	c/o NeuStar
1781.	varioldinnics.co	updater	c/o NeuStar
1782.	vcstiturnediana.co	updater	c/o NeuStar
1783.	vegatorkspeps.co	updater	c/o NeuStar
1784.	vemaxxlionna.co	updater	c/o NeuStar
1785.	yettaillarfic.co	updater	c/o NeuStar
1786.	quantraxactor.co	updater	c/o NeuStar
1787.	recavatech.co	updater	c/o NeuStar
1788.	recellhelsen.co	updater	c/o NeuStar
1789.	reetexista.co	updater	c/o NeuStar
1790.	runtroadeatb.co	updater	c/o NeuStar
1791.	saldchwetheach.co	updater	c/o NeuStar
1792.	sardballierman.co	updater	c/o NeuStar
1793.	sausandergere.co	updater	c/o NeuStar
1794.	senstonymy.co	updater	c/o NeuStar
1795.	shippontlise.co	updater	c/o NeuStar
1796.	silvarnetinn.co	updater	c/o NeuStar
1797.	simontfica.co	updater	c/o NeuStar
1798.	sneckstrumo.co	updater	c/o NeuStar
1799.	somanyontion.co	updater	c/o NeuStar
1800.	sterijnccompan.co	updater	c/o NeuStar
1801.	suitionsaway.co	updater	c/o NeuStar
1802.	sunageoshighvi.co	updater	c/o NeuStar
1803.	talettedible.co	updater	c/o NeuStar
1804.	photalegraza.co	updater	c/o NeuStar

1805.	padesionittatu.co	updater	c/o NeuStar
1806.	patroqualarva.co	updater	c/o NeuStar
1807.	perisoneterts.co	updater	c/o NeuStar
1808.	pintamierback.co	updater	c/o NeuStar
1809.	planeostsquavep.co	updater	c/o NeuStar
1810.	vibeapnesbu.co	updater	c/o NeuStar
1811.	viewediesolver.co	updater	c/o NeuStar
1812.	vigetectrockset.co	updater	c/o NeuStar
1813.	westansgualiti.co	updater	c/o NeuStar
1814.	westwiserce.co	updater	c/o NeuStar
1815.	whatixemieldin.co	updater	c/o NeuStar
1816.	wickissievele.co	updater	c/o NeuStar
1817.	managenetwor.co	updater	c/o NeuStar
1818.	meazeridashloc.co	updater	c/o NeuStar
1819.	mentripete.co	updater	c/o NeuStar
1820.	minollumentlynx.co	updater	c/o NeuStar
1821.	moderheittrack.co	updater	c/o NeuStar
1822.	mutanisopendsie.co	updater	c/o NeuStar
1823.	muticeptad.co	updater	c/o NeuStar
1824.	onespointheadia.co	updater	c/o NeuStar
1825.	holmancybeac.co	updater	c/o NeuStar
1826.	ignarysama.co	updater	c/o NeuStar
1827.	inforksonseia.co	updater	c/o NeuStar
1828.	intelinellouse.co	updater	c/o NeuStar
1829.	interponsseella.co	updater	c/o NeuStar
1830.	invetechinte.co	updater	c/o NeuStar
1831.	jamsulumency.co	updater	c/o NeuStar
1832.	jellabillat.co	updater	c/o NeuStar
1833.	jobinedianingfo.co	updater	c/o NeuStar
1834.	kenamersoftvu.co	updater	c/o NeuStar
1835.	killdfymerraque.co	updater	c/o NeuStar
1836.	kristradentro.co	updater	c/o NeuStar
1837.	lekhauserex.co	updater	c/o NeuStar
1838.	leopodentargit.co	updater	c/o NeuStar
1839.	liverylink.co	updater	c/o NeuStar
1840.	locaresplicutl.co	updater	c/o NeuStar
1841.	lorevingbranta.co	updater	c/o NeuStar
1842.	lucascattientop.co	updater	c/o NeuStar
1843.	lucassfield.co	updater	c/o NeuStar
1844.	gavildippurum.co	updater	c/o NeuStar
1845.	gertyphacqueier.co	updater	c/o NeuStar
1846.	globridolumet.co	updater	c/o NeuStar
1847.	gramablessattro.co	updater	c/o NeuStar
1848.	grounaxyxin.co	updater	c/o NeuStar
1849.	hoffmarketraph.co	updater	c/o NeuStar
1850.	fiboxencercha.co	updater	c/o NeuStar
1851.	finewcreautomp.co	updater	c/o NeuStar
1852.	foolieracceiv.co	updater	c/o NeuStar
1853.	forviclemo.co	updater	c/o NeuStar
1854.	copelixell.co	updater	c/o NeuStar
1855.	convortonnennt.co	updater	c/o NeuStar
1856.	creamottonovati.co	updater	c/o NeuStar
1857.	cryogiwigater.co	updater	c/o NeuStar

1858.	cuficellimaad.co	updater	c/o NeuStar
1859.	cumberiangle.co	updater	c/o NeuStar
1860.	cyberistrolax.co	updater	c/o NeuStar
1861.	dasyucorbit.co	updater	c/o NeuStar
1862.	dempeighternya.co	updater	c/o NeuStar
1863.	denitraspetr.co	updater	c/o NeuStar
1864.	deratirelcomni.co	updater	c/o NeuStar
1865.	deressenwarpol.co	updater	c/o NeuStar
1866.	doutektronumni.co	updater	c/o NeuStar
1867.	ebuityketfinus.co	updater	c/o NeuStar
1868.	eguildaycock.co	updater	c/o NeuStar
1869.	eponamindranthe.co	updater	c/o NeuStar
1870.	eunitynewgbc.co	updater	c/o NeuStar
1871.	evraffeyplings.co	updater	c/o NeuStar
1872.	exedrininsteadna.co	updater	c/o NeuStar
1873.	brigatexgluc.co	updater	c/o NeuStar
1874.	bryandsighter.co	updater	c/o NeuStar
1875.	celequidictor.co	updater	c/o NeuStar
1876.	chbytechipemen.co	updater	c/o NeuStar
1877.	chetteaditas.co	updater	c/o NeuStar
1878.	accoukierlism.co	updater	c/o NeuStar
1879.	achyroransib.co	updater	c/o NeuStar
1880.	aeractraspac.co	updater	c/o NeuStar
1881.	alconichill.co	updater	c/o NeuStar
1882.	alederpe.co	dropzone	c/o NeuStar
1883.	amersterin.co	updater	c/o NeuStar
1884.	andeedna.co	dropzone	c/o NeuStar
1885.	annadiat.co	dropzone	c/o NeuStar
1886.	anualiverk.co	updater	c/o NeuStar
1887.	armrena.co	dropzone	c/o NeuStar
1888.	artechellirat.co	updater	c/o NeuStar
1889.	articityxpaqua.co	updater	c/o NeuStar
1890.	assmitizeree.co	updater	c/o NeuStar
1891.	ataghty.co	dropzone	c/o NeuStar
1892.	atlancentuage.co	updater	c/o NeuStar
1893.	auchaulu.co	dropzone	c/o NeuStar
1894.	audubideonety.co	updater	c/o NeuStar
1895.	avaintellegeron.co	updater	c/o NeuStar
1896.	avectintemottis.co	updater	c/o NeuStar
1897.	babical.co	dropzone	c/o NeuStar
1898.	beregg.co	dropzone	c/o NeuStar
1899.	berrat.co	dropzone	c/o NeuStar
1900.	betterheousermy.co	updater	c/o NeuStar
1901.	blogoettindia.co	updater	c/o NeuStar
1902.	boatorldenoras.co	updater	c/o NeuStar
1903.	bobetic.co	dropzone	c/o NeuStar
1904.	borsteksavalu.co	updater	c/o NeuStar
1905.	bottler.co	dropzone	c/o NeuStar
1906.	brigatexgluc.co	updater	c/o NeuStar
1907.	bryandsighter.co	updater	c/o NeuStar
1908.	bulingelah.co	dropzone	c/o NeuStar
1909.	bullfot.co	dropzone	c/o NeuStar
1910.	bundhaker.co	dropzone	c/o NeuStar

1911.	cantailya.co	dropzone	c/o NeuStar
1912.	carratina.co	dropzone	c/o NeuStar
1913.	cashlitype.co	dropzone	c/o NeuStar
1914.	cavient.co	dropzone	c/o NeuStar
1915.	celequidictor.co	updater	c/o NeuStar
1916.	chbytechipemen.co	updater	c/o NeuStar
1917.	chetteaditas.co	updater	c/o NeuStar
1918.	cocklemili.co	dropzone	c/o NeuStar
1919.	collex.co	dropzone	c/o NeuStar
1920.	collowestco.co	dropzone	c/o NeuStar
1921.	conwortonnent.co	updater	c/o NeuStar
1922.	coolityle.co	dropzone	c/o NeuStar
1923.	coopese.co	dropzone	c/o NeuStar
1924.	cootterian.co	dropzone	c/o NeuStar
1925.	copelixell.co	updater	c/o NeuStar
1926.	coreamesents.co	updater	c/o NeuStar
1927.	cothonal.co	dropzone	c/o NeuStar
1928.	creamottonovati.co	updater	c/o NeuStar
1929.	criterage.co	dropzone	c/o NeuStar
1930.	croesco.co	dropzone	c/o NeuStar
1931.	cryogiwigater.co	updater	c/o NeuStar
1932.	cuficellimaad.co	updater	c/o NeuStar
1933.	cyberistrolax.co	updater	c/o NeuStar
1934.	dasyucorbit.co	updater	c/o NeuStar
1935.	cumberiangle.co	updater	c/o NeuStar
1936.	dempeighternya.co	updater	c/o NeuStar
1937.	denitraspetr.co	updater	c/o NeuStar
1938.	deratirelcomni.co	updater	c/o NeuStar
1939.	deressenwarpol.co	updater	c/o NeuStar
1940.	detindi.co	dropzone	c/o NeuStar
1941.	doutektronumni.co	updater	c/o NeuStar
1942.	dwomanti.co	dropzone	c/o NeuStar
1943.	ebuityketfinus.co	updater	c/o NeuStar
1944.	eguildaycock.co	updater	c/o NeuStar
1945.	eineep.co	dropzone	c/o NeuStar
1946.	encyte.co	dropzone	c/o NeuStar
1947.	eponamindranthe.co	updater	c/o NeuStar
1948.	ernesti.co	dropzone	c/o NeuStar
1949.	eunitynewgbc.co	updater	c/o NeuStar
1950.	evraffeyplings.co	updater	c/o NeuStar
1951.	excelat.co	dropzone	c/o NeuStar
1952.	exedrininsteadna.co	updater	c/o NeuStar
1953.	exogael.co	dropzone	c/o NeuStar
1954.	exploqu.co	dropzone	c/o NeuStar
1955.	fantasynche.co	dropzone	c/o NeuStar
1956.	fiboxencercha.co	updater	c/o NeuStar
1957.	finewcreautomp.co	updater	c/o NeuStar
1958.	globridolumet.co	updater	c/o NeuStar
1959.	gertyphacqueier.co	updater	c/o NeuStar
1960.	foolieracceiv.co	updater	c/o NeuStar
1961.	forviclemo.co	updater	c/o NeuStar
1962.	gagenpau.co	dropzone	c/o NeuStar
1963.	gavildippurum.co	updater	c/o NeuStar

1964.	gramablessatro.co	updater	c/o NeuStar
1965.	grounaxyin.co	updater	c/o NeuStar
1966.	grunner.co	dropzone	c/o NeuStar
1967.	guessounthu.co	dropzone	c/o NeuStar
1968.	gulabill.co	dropzone	c/o NeuStar
1969.	heavykyly.co	dropzone	c/o NeuStar
1970.	hektary.co	dropzone	c/o NeuStar
1971.	hildarchi.co	dropzone	c/o NeuStar
1972.	hoffmarketraph.co	updater	c/o NeuStar
1973.	holmancybeac.co	updater	c/o NeuStar
1974.	hydrole.co	dropzone	c/o NeuStar
1975.	ignarysama.co	updater	c/o NeuStar
1976.	jacketerer.co	dropzone	c/o NeuStar
1977.	ileenyet.co	dropzone	c/o NeuStar
1978.	incrence.co	dropzone	c/o NeuStar
1979.	ineniali.co	dropzone	c/o NeuStar
1980.	inesilk.co	dropzone	c/o NeuStar
1981.	inesmate.co	dropzone	c/o NeuStar
1982.	inforksonseia.co	updater	c/o NeuStar
1983.	intelinellouse.co	updater	c/o NeuStar
1984.	interponsseella.co	updater	c/o NeuStar
1985.	inthou.co	dropzone	c/o NeuStar
1986.	invetechinte.co	updater	c/o NeuStar
1987.	iranitereno.co	dropzone	c/o NeuStar
1988.	jambsumency.co	updater	c/o NeuStar
1989.	jectoral.co	dropzone	c/o NeuStar
1990.	jellabillat.co	updater	c/o NeuStar
1991.	jellotr.co	dropzone	c/o NeuStar
1992.	jobinedianingfo.co	updater	c/o NeuStar
1993.	katussi.co	dropzone	c/o NeuStar
1994.	judithri.co	dropzone	c/o NeuStar
1995.	kenamersoftvu.co	updater	c/o NeuStar
1996.	killdfymerraque.co	updater	c/o NeuStar
1997.	kindjin.co	dropzone	c/o NeuStar
1998.	kristradentro.co	updater	c/o NeuStar
1999.	lekhauseurex.co	updater	c/o NeuStar
2000.	lepodentargit.co	updater	c/o NeuStar
2001.	leverry.co	dropzone	c/o NeuStar
2002.	liviarylink.co	updater	c/o NeuStar
2003.	locaresplicutl.co	updater	c/o NeuStar
2004.	lorevngbranta.co	updater	c/o NeuStar
2005.	lucascattientop.co	updater	c/o NeuStar
2006.	lucassfield.co	updater	c/o NeuStar
2007.	luristri.co	dropzone	c/o NeuStar
2008.	managenetwor.co	updater	c/o NeuStar
2009.	manillack.co	dropzone	c/o NeuStar
2010.	manmark.co	dropzone	c/o NeuStar
2011.	mannieda.co	dropzone	c/o NeuStar
2012.	measubstomy.co	dropzone	c/o NeuStar
2013.	meazeridashloc.co	updater	c/o NeuStar
2014.	mentripete.co	updater	c/o NeuStar
2015.	millewine.co	dropzone	c/o NeuStar
2016.	minollumentlynx.co	updater	c/o NeuStar

2017.	moderheittrack.co	updater	c/o NeuStar
2018.	mulleril.co	dropzone	c/o NeuStar
2019.	mutanisopendsie.co	updater	c/o NeuStar
2020.	muticeptad.co	updater	c/o NeuStar
2021.	nedataryjosc.co	dropzone	c/o NeuStar
2022.	onespointtheadia.co	updater	c/o NeuStar
2023.	openity.co	dropzone	c/o NeuStar
2024.	padesionittatu.co	updater	c/o NeuStar
2025.	pandidarma.co	dropzone	c/o NeuStar
2026.	patroqualarva.co	updater	c/o NeuStar
2027.	pederm.co	dropzone	c/o NeuStar
2028.	perisoneterts.co	updater	c/o NeuStar
2029.	phimore.co	dropzone	c/o NeuStar
2030.	photalegraza.co	updater	c/o NeuStar
2031.	pintamierback.co	updater	c/o NeuStar
2032.	pistonlover.co	dropzone	c/o NeuStar
2033.	planail.co	dropzone	c/o NeuStar
2034.	planeostsquavep.co	updater	c/o NeuStar
2035.	primasc.co	dropzone	c/o NeuStar
2036.	pucessop.co	dropzone	c/o NeuStar
2037.	quantraxactor.co	updater	c/o NeuStar
2038.	recavatech.co	updater	c/o NeuStar
2039.	rece llhelsen.co	updater	c/o NeuStar
2040.	reetexista.co	updater	c/o NeuStar
2041.	rosellewe.co	dropzone	c/o NeuStar
2042.	rozencess.co	dropzone	c/o NeuStar
2043.	runtroadeatb.co	updater	c/o NeuStar
2044.	saldchwetheach.co	updater	c/o NeuStar
2045.	salterembl.co	dropzone	c/o NeuStar
2046.	soupchi.co	dropzone	c/o NeuStar
2047.	sardballierman.co	updater	c/o NeuStar
2048.	sausandergere.co	updater	c/o NeuStar
2049.	sciteleganal.co	updater	c/o NeuStar
2050.	senstonymy.co	updater	c/o NeuStar
2051.	shalyxiard.co	dropzone	c/o NeuStar
2052.	shawler.co	dropzone	c/o NeuStar
2053.	shippotlise.co	updater	c/o NeuStar
2054.	shutiary.co	dropzone	c/o NeuStar
2055.	silvarnetinn.co	updater	c/o NeuStar
2056.	smagogre.co	dropzone	c/o NeuStar
2057.	sneckstrumo.co	updater	c/o NeuStar
2058.	simontfica.co	updater	c/o NeuStar
2059.	snowser.co	dropzone	c/o NeuStar
2060.	somanyontion.co	updater	c/o NeuStar
2061.	sterijnccompan.co	updater	c/o NeuStar
2062.	stourangebo.co	dropzone	c/o NeuStar
2063.	suitionsaway.co	updater	c/o NeuStar
2064.	sument.co	dropzone	c/o NeuStar
2065.	sunageoshighvi.co	updater	c/o NeuStar
2066.	talettedible.co	updater	c/o NeuStar
2067.	tallyso.co	dropzone	c/o NeuStar
2068.	tantainie.co	dropzone	c/o NeuStar
2069.	tegony.co	dropzone	c/o NeuStar

2070.	thernextoneter.co	updater	c/o NeuStar
2071.	toonereretry.co	dropzone	c/o NeuStar
2072.	tornallogue.co	dropzone	c/o NeuStar
2073.	tourinathol.co	dropzone	c/o NeuStar
2074.	turbiculu.co	dropzone	c/o NeuStar
2075.	turpipeltim.co	dropzone	c/o NeuStar
2076.	twalliar.co	dropzone	c/o NeuStar
2077.	tywinderdamaku.co	updater	c/o NeuStar
2078.	ukrainewskill.co	updater	c/o NeuStar
2079.	urerariece.co	dropzone	c/o NeuStar
2080.	vacantitechip.co	updater	c/o NeuStar
2081.	varioldinnics.co	updater	c/o NeuStar
2082.	vcstiturnediana.co	updater	c/o NeuStar
2083.	vegatorkspes.co	updater	c/o NeuStar
2084.	vemaxxlionna.co	updater	c/o NeuStar
2085.	veratedra.co	dropzone	c/o NeuStar
2086.	vibeapnesbu.co	updater	c/o NeuStar
2087.	viewediesolver.co	updater	c/o NeuStar
2088.	vigetectrockset.co	updater	c/o NeuStar
2089.	westansqualiti.co	updater	c/o NeuStar
2090.	westwiserce.co	updater	c/o NeuStar
2091.	whatixemieldin.co	updater	c/o NeuStar
2092.	wickissievele.co	updater	c/o NeuStar
2093.	wrieregging.co	dropzone	c/o NeuStar
2094.	yettaillarfic.co	updater	c/o NeuStar
2095.	accoukierlism.co	updater	c/o NeuStar
2096.	achyorransib.co	updater	c/o NeuStar
2097.	aeractraspac.co	updater	c/o NeuStar
2098.	alconichill.co	updater	c/o NeuStar
2099.	amersterin.co	updater	c/o NeuStar
2100.	anualiverk.co	updater	c/o NeuStar
2101.	artechellirat.co	updater	c/o NeuStar
2102.	articityxpaqua.co	updater	c/o NeuStar
2103.	assmitizeree.co	updater	c/o NeuStar
2104.	atlancentuage.co	updater	c/o NeuStar
2105.	audubideonentity.co	updater	c/o NeuStar
2106.	avaintellegeron.co	updater	c/o NeuStar
2107.	avectintemottis.co	updater	c/o NeuStar

NeuStar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States

NeuStar, Inc.
Loudoun Tech Center
46000 Center Oak Plaza
Sterling Virginia 20166
United States

	Harmful Botnet Domain Name	Type	Whois Email Address
2108.	oqocbqmmmnjzq.biz	infector	es73z29q2m5@nameprivacy.com
2109.	petroleumgroup.biz	infector	petroleumgroupp@yahoo.com
2110.	wdoyqoxnmmlqyot.biz	infector	drawnmccoy@yahoo.com
2111.	roobshall.biz	dropzone, infector	contact@webdomainsbproxy.com
2112.	seoengine.biz	dropzone, source	gmvjcxkxhs@whoisservices.cn
2113.	snaretrace.us	dropzone, infector	dunn.douglas24@yahoo.com
2114.	snaretrack.biz	dropzone, infector	jitchikoff@yahoo.com
2115.	snarework.us	dropzone, infector	portellkathy@yahoo.com
2116.	hoycktsjwqsmklnv.biz	infector	arellanoteasel@yahoo.com
2117.	iesnare.us	dropzone, infector	dadasd1231dadsadasda@yahoo.com
2118.	ilovekeks.biz	dropzone, infector	glaseranne@yahoo.com
2119.	lwbbtfrtjjsyksl.biz	infector	arellanoteasel@yahoo.com
2120.	njxnerslmmvpyto.biz	infector	arellanoteasel@yahoo.com
2121.	dasad41da4safasdasd21.biz	dropzone, infector	domain.tech@yahoo-inc.com
2122.	executivesuites.us	updater	enm@emailforyou.com
2123.	faaspouk.biz	dropzone, infector	tgwq-uanic@priv.uanic.ua
2124.	apricot-fresh.us	dropzone	himacss@yandex.ru
2125.	avocado-fresh.us	dropzone	himacss@yandex.ru
2126.	bannersurvey.biz	embedded_js	bannersurvey.biz@domainsbproxy.com
2127.	beaverday.biz	source	spruebeatty@yahoo.com
2128.	bfhoqnbpunvqymd.biz	dropzone, infector	langleyinexpiable@yahoo.com
2129.	blackcurrant-free.us	dropzone	himacss@yandex.ru
2130.	bqrhtwrykrksyl.biz	dropzone, infector	d448j8f25nx@nameprivacy.com
2131.	cprmhmmtslosmusm.biz	dropzone, infector	ge4nx92w6rk@nameprivacy.com
2132.	cherry-free.us	dropzone	himacss@yandex.ru
2133.	carbossa.biz	embedded_js	admin@carbossa.biz
2134.	clfuhmciswossut.biz	dropzone, infector	downingcinerama@yahoo.com
2135.	goojejoheqbnx.biz	dropzone, source, infector	rd9cp4t73dq@nameprivacy.com
2136.	go6po.biz	dropzone, source	abcnamecompany@gmail.com
2137.	eqpnhotnhnvsfeus.biz	dropzone, infector	d97f84nn9rq@nameprivacy.com
2138.	executivesuites.us	updater	enm@emailforyou.com
2139.	giyieqqwwxiro.biz	dropzone, infector	rh6fk9xv2q5@nameprivacy.com
2140.	gxdrnmspexrtooies.biz	dropzone, infector	wm6vn79m42s@nameprivacy.com
2141.	gxxlzrylqgplvpnp.biz	dropzone, infector	yj55n8hw5nb@nameprivacy.com
2142.	gywsiglihvdyeyupu.biz	dropzone, infector	z34jb9zq2a5@nameprivacy.com
2143.	helpsupport.biz	updater, dropzone	xabkdafmpl@whoisservices.cn
2144.	hrllmdklzoigxywn.biz	dropzone, infector	contact@privacyprotect.org
2145.	hrnngkmoyhmmoynz.biz	dropzone, infector	c/o NeuStar
2146.	hvlpmopbnutrju.biz	dropzone, infector	d97f84nn9rq@nameprivacy.com
2147.	hxvluohophnnse.biz	dropzone, source, infector	reasonhickey@yahoo.com

2148.	ijogjpkdprqpsugn.biz	dropzone, source, infector	visitus@bitandjazzdanceclub.com
2149.	injruhjxmtccrut.biz	dropzone, infector	visitus@bitandjazzdanceclub.com
2150.	ipcohyjqjxlmmgts.biz	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
2151.	jfpvqxvywordryr.biz	dropzone, infector	apprehensivebrandt@yahoo.com
2152.	ixkgojrequpooitp.biz	dropzone, infector	repossesseddomain@godaddy.com
2153.	izknfgnsrvmvswuh.biz	dropzone, infector	e255f24x5pb@nameprivacy.com
2154.	jctozilnwnwutgf.biz	dropzone, source, infector	c/o NeuStar
2155.	jmgvtnkjqtzglj.biz	dropzone, infector	a86af8ue8ca@nameprivacy.com
2156.	jptptmlpqnzdnpl.biz	dropzone, source, infector	ab5s54gb8eg@nameprivacy.com
2157.	jslpfnssrsmnqsvl.biz	dropzone, infector	hs4mk7kj38v@nameprivacy.com
2158.	kiwslqlkjvntt.biz	dropzone, infector	dw6va7pc9dk@nameprivacy.com
2159.	kkksvrmrsyxfvj.biz	dropzone, infector	je4k75up8xt@nameprivacy.com
2160.	korpupnpnqhjvvk.biz	dropzone, infector	c/o NeuStar
2161.	kyupjxrwpwxmrgn.biz	dropzone, infector	ge4nx92w6rk@nameprivacy.com
2162.	lastking.biz	source	u5ek5js4f2ab5e1b0ae7@w86bna54f21bffa2ffd1.privatewhois.net
2163.	lcocnvxlpkokso.biz	dropzone, source, infector	c/o NeuStar
2164.	lwqlmttgujtfxq.biz	dropzone, infector	apprehensivebrandt@yahoo.com
2165.	lzfudhklvocwo.biz	dropzone, infector	wv4k596n5se@nameprivacy.com
2166.	mass-money-makers.us	source	gwatene@gmail.com
2167.	mnrpxtmkkwmiliq.biz	dropzone, infector	mcroker@charter.net
2168.	mnxpeejxpvrhkrn.biz	dropzone, infector	mcroker@charter.net
2169.	mcvoqncqgnmzowno.biz	dropzone, infector	ns5m23ur84w@nameprivacy.com
2170.	mcvoqncqgnmzowno.biz	source	ns5m23ur84w@nameprivacy.com
2171.	mlhnxqlrqhycorl.biz	dropzone, infector	alle@alleopneandertal.com
2172.	mpnweiuongwwrsmq.biz	dropzone, source, infector	gv9st8nk4ka@nameprivacy.com
2173.	msh tqgh topdon.biz	dropzone, infector	c/o NeuStar
2174.	mtlrnsfbhukqj.biz	dropzone, infector	n97b76fk87g@nameprivacy.com
2175.	nacha-reports.us	source	fillopos@yahoo.com
2176.	ndlpnjnopuqsdqk.biz	dropzone, infector	c/o NeuStar
2177.	nnkpwsnovpsptl.biz	dropzone, infector	c/o NeuStar
2178.	ntfgzoeywqirupfn.biz	dropzone, source, infector	a37zk7bv7v3@nameprivacy.com
2179.	ntvwooywivrkcn.n	dropzone, source, infector	jr7v53ge4pk@nameprivacy.com
2180.	nzfyvlftthenmyqh.biz	dropzone, infector	a37zk7bv7v3@nameprivacy.com
2181.	nzvgksojootbmzk.biz	dropzone, infector, source	reasonhickey@yahoo.com
2182.	oeypjdqjnnckwd.biz	dropzone, infector	d97f84nn9rq@nameprivacy.com
2183.	ofuvjtxplutlxccr.biz	dropzone, infector	xr3sg3h779x@nameprivacy.com
2184.	oltqugnneowyolh.biz	dropzone, infector	vf5vt9yz384@nameprivacy.com
2185.	onikyhljnporunk.biz	dropzone, infector	equilateralfranklin@yahoo.com
2186.	onpqqlbpkkyfxspr.biz	dropzone, source, infector	am9zr2nq3p8@nameprivacy.com
2187.	orjvswjonrrksn.biz	dropzone, infector	fractureglen@yahoo.com
2188.	oymqseiwtolsooq.biz	dropzone, infector	wm6vn79m42s@nameprivacy.com
2189.	pdupvzqwlqw.biz	dropzone, infector	condolencelangford@yahoo.com
2190.	pnmlpmqzztvuqfrt.biz	dropzone, infector	odommclean@yahoo.com
2191.	pvglrzjzfpjipksp.biz	dropzone, infector	d67rg3d97jp@nameprivacy.com
2192.	pzfxvqwglyyksjp.biz	dropzone, source, infector	contact@privacyprotect.org
2193.	qisgmckijfxtqzf.biz	dropzone, source, infector	seymourfarsighted@yahoo.com
2194.	qmqomrppninyuls.biz	dropzone, source, infector	c/o NeuStar
2195.	qmypbeqqvqxeanu.biz	dropzone, infector	root@cheaplobstersny.com
2196.	qpfmnsmycqlujs.biz	dropzone, source, infector	ea4cy5zc9n8@nameprivacy.com
2197.	qqmypiinpwywnkq.biz	dropzone, infector	c/o NeuStar
2198.	qroslnnklpmcrmor.biz	dropzone, infector	repossesseddomain@godaddy.com
2199.	qymvlgiijnppjugv.biz	dropzone, infector	f76ah7cb472@nameprivacy.com
2200.	rbnsgniyukmkqrq.biz	dropzone, infector	d38679a55tn@nameprivacy.com

2201.	rjmxlwpoekwmrrptn.biz	dropzone, infector	c/o NeuStar
2202.	rkpwllosqmxmnhtm.biz	dropzone, infector	thurmanpang@yahoo.com
2203.	rkvtnfnqymwqgwk.biz	dropzone, infector	m84np6jd4gt@nameprivacy.com
2204.	rnoqvsomcgkmpeli.biz	dropzone, source, infector	xoxaxybetokic@yahoo.com
2205.	rronxvwqietsrlp.biz	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
2206.	rszgpgvjhgwfpl.biz	embedded_js	erivegutixo@yahoo.com
2207.	rumbt.biz	dropzone	anatoliyliis@yahoo.com
2208.	rvwpovgppaqqpax.biz	dropzone, infector	n97b76fk87g@nameprivacy.com
2209.	ryspbfpvhyqvqnq.biz	dropzone, infector	z34jb9zq2a5@nameprivacy.com
2210.	selxowomwwoirvnl.biz	dropzone, infector	t57hy5u68dr@nameprivacy.com
2211.	mzonphxtliwrw.biz	dropzone, infector	yj55n8hw5nb@nameprivacy.com
2212.	shkrvpwjyisjiu.biz	dropzone, infector	c/o NeuStar
2213.	snmwtynjppjptsi.biz	dropzone, infector	mccartybimetallism@yahoo.com
2214.	snsflrqppsuwjino.biz	dropzone, infector	sr7254hn4hn@networksolutionsprivateregistration.com
2215.	symlink.us	embedded_js	olegibanko@gmail.com
2216.	spidyyjliglsmoen.biz	dropzone, source, infector	challenge_green@yahoo.com
2217.	sspjrymvsodnqwq.biz	dropzone, source, infector	ym84e7fe3rb@nameprivacy.com
2218.	stpdwjxqltpovlg.biz	dropzone, infector	ns5m23ur84w@nameprivacy.com
2219.	tfugtqofsrnpral.biz	dropzone, infector	hy4r394j6ja@nameprivacy.com
2220.	thqlsllnooqtnyhm.biz	dropzone, source, infector	yz4rr2um7gb@nameprivacy.com
2221.	tieqlmmmspckyoohn.biz	dropzone, infector	am9zr2nq3p8@nameprivacy.com
2222.	tiqpoxpvpstpgsql.biz	dropzone, infector, source	d448j8f25nx@nameprivacy.com
2223.	tjclczxrekrpqpx.biz	dropzone, infector, source	repossesseddomain@godaddy.com
2224.	tjnmewowiqphghr.biz	dropzone, source, infector	d97f84nn9rq@nameprivacy.com
2225.	tovrzkvjxtwhvgn.biz	dropzone, infector	dd3t93pu55u@nameprivacy.com
2226.	tpckorvoxpmship.biz	dropzone, infector	qz8kp89m9e8@nameprivacy.com
2227.	ttdjeisdlpvge.biz	dropzone, infector	armeniangillespie@yahoo.com
2228.	tvhwlpwggrmoerr.biz	dropzone, infector	n97b76fk87g@nameprivacy.com
2229.	ufiwhqrjjtsdwjn.biz	dropzone, infector	waterscomprehensive@yahoo.com
2230.	ukluuioksqrirh.biz	dropzone, infector	g856y7f88nz@nameprivacy.com
2231.	umrrmimwlezmjfqb.biz	dropzone, infector	cz99x6ay7h2@nameprivacy.com
2232.	usijogzjvqtix.biz	dropzone, source, infector	fractureglenn@yahoo.com
2233.	utqworfhrkxmcmqm.biz	dropzone, infector	d97f84nn9rq@nameprivacy.com
2234.	uykrirlijldnlqfj.biz	dropzone, infector	dt6gh2wj339@nameprivacy.com
2235.	vokkvkudxxftljh.biz	dropzone, infector	a37zk7bv7v3@nameprivacy.com
2236.	vrjehsppcgprhs.biz	dropzone, infector	mcroker@charter.net
2237.	vslqkrspvrtqqu.biz	dropzone, infector	condolencelangford@yahoo.com
2238.	vttyntejoqftwkcn.biz	dropzone, infector	refectiongay@yahoo.com
2239.	vuuqqwuywtpfqno.biz	dropzone, infector	kh3te68h3mx@nameprivacy.com
2240.	wddlvxtmhqqjjsvt.biz	dropzone, infector	w72p35dd5tt@nameprivacy.com
2241.	weraty.biz	dropzone	perolsp@yahoo.com
2242.	wfsqshkrjjleojg.biz	dropzone, infector	contact@privacyprotect.org
2243.	wfzmkpwqqdvhvkso.biz	dropzone, source, infector	condolencelangford@yahoo.com
2244.	wilmrsmplszzuuup.biz	dropzone, infector	gv9st8nk4ka@nameprivacy.com
2245.	wktxuzqvbfkgln.biz	dropzone, infector	vv73a9jm5wh@nameprivacy.com
2246.	wrtohiimhvlij.biz	dropzone, infector	gv9st8nk4ka@nameprivacy.com
2247.	xiftkqniniwoirvu.biz	dropzone, source, infector	x26qt7dr3b4@nameprivacy.com

2248.	xxvtrrmbuqshu.biz	dropzone, source, infector	waterscomprehensive@yahoo.com
2249.	ylhhkuofhlpuqkp.biz	dropzone, infector	hv59t3tr3v6@nameprivacy.com
2250.	ylkhrvojxmqngidj.biz	dropzone, source, infector	c/o NeuStar
2251.	ynqguoufnfpfmtr.biz	dropzone, source, infector	k86c98xv6bx@nameprivacy.com
2252.	yxcqvqiszlkoysgn.biz	dropzone, infector	d38679a55tn@nameprivacy.com
2253.	zrpfnqyvqmxmhxfk.biz	dropzone, source, infector	d38679a55tn@nameprivacy.com
2254.	zrxymtzmrielrm.biz	dropzone, source, infector	u583p92r8uv@nameprivacy.com
2255.	ztjphpsmplboq.biz	dropzone, source, infector	seymourfarsighted@yahoo.com
2256.	11plants.biz	infector, dropzone	contact@webdomainsbyproxy.com
2257.	28843622.biz	infector, dropzone	contact@webdomainsbyproxy.com
2258.	2x5.us	infector, dropzone	keayon@hotmail.com
2259.	amstelone3.biz	infector, dropzone	nijankinchristina@yahoo.com
2260.	antifoher.biz	infector, dropzone	contact@webdomainsbyproxy.com
2261.	anysnare.us	infector, dropzone	zhoushaoming@yahoo.com
2262.	xxvtrrmbuqshu.biz	infector	waterscomprehensive@yahoo.com
2263.	level-3.us	dropzone	joegeorgeboy001@yahoo.com
2264.	level-3.biz	dropzone	contact@myprivateregistration.com

Afilias Limited
C/O Afilias USA, Inc.
300 Welsh Road, Building 3
Suite 105
Horsham, PA 19044
United States

	Harmful Botnet Domain Name	Type	Whois Email Address
2265.	robohoste.info	dropzone	toniparish@imap.cc
2266.	rokqsjhzyiusvrj.info	infector	c/o Afilias
2267.	ultimatesecurity.info	dropzone, infector	domain.tech@yahoo-inc.com
2268.	hostingguru.info	dropzone, infector	damage.smith@yandex.ru
2269.	localh0st.info	dropzone, infector	1b18ff4e8dfd40238305edda885ba968.protect@whoisguard.com
2270.	freetop.mobi	dropzone, infector	chandru.sept24@gmail.com
2271.	actinatist.info	dropzone	c/o Afilias
2272.	advertising-services.info	source	godaddy@profitsigur.ro
2273.	ahaccu.info	dropzone	c/o Afilias
2274.	akularryzare.info	dropzone	c/o Afilias
2275.	algroton.info	dropzone	c/o Afilias
2276.	alianalingta.info	dropzone	c/o Afilias
2277.	allyga.info	dropzone	support@simioffers.com
2278.	alpriate.info	dropzone	the.malware.cabal@gmail.com
2279.	amidinesfa.info	dropzone	c/o Afilias
2280.	anagodwator.info	dropzone	c/o Afilias
2281.	anateam.info	dropzone	c/o Afilias
2282.	ancevir.info	dropzone	sarahcolvin@live.co.uk
2283.	anecdadiard.info	dropzone	c/o Afilias
2284.	aniani.info	dropzone	david.austin44@yahoo.com
2285.	antifraudsolutions.info	dropzone	exitthematrix@ymail.com
2286.	apagoni.info	dropzone	c/o Afilias
2287.	aphard.info	dropzone	sarahcolvin@live.co.uk
2288.	aphasmuce.info	dropzone	c/o Afilias
2289.	apple-fresh.info	dropzone	himacss@yandex.ru
2290.	apricot-fresh.info	dropzone	himacss@yandex.ru
2291.	argiopoulos.info	source	whois@bluehost.com
2292.	ashnmjjpoljfnl.info	dropzone, infector	waterscomprehensive@yahoo.com
2293.	ass-tube.info	dropzone	himacss@yandex.ru
2294.	astroamah.info	dropzone	c/o Afilias
2295.	aubirdwa.info	dropzone	c/o Afilias
2296.	avocado-fresh.info	dropzone	himacss@yandex.ru
2297.	bad-tube.info	dropzone	himacss@yandex.ru
2298.	barsenginger.info	dropzone	c/o Afilias
2299.	bativolt.info	dropzone	sarahcolvin@live.co.uk
2300.	bbw-go.info	dropzone	himacss@yandex.ru
2301.	bilberry-free.info	dropzone	himacss@yandex.ru
2302.	binetu.info	dropzone	sarahcolvin@live.co.uk
2303.	beginestition.info	dropzone	david.austin44@yahoo.com
2304.	belleterer.info	dropzone	c/o Afilias
2305.	blackberry-free.info	dropzone	himacss@yandex.ru
2306.	blackcurrant-free.info	dropzone	himacss@yandex.ru
2307.	blaismanni.info	dropzone	c/o Afilias
2308.	blueberry-free.info	dropzone	himacss@yandex.ru

2309.	bobbiestube.info	dropzone	himacss@yandex.ru
2310.	bowsterb.info	dropzone	c/o Afilias
2311.	bptigozrtypzj.info	dropzone, source, infector	c/o Afilias
2312.	bqqsnpnvppxqq.info	dropzone, infector	wv4k596n5se@nameprivacy.com
2313.	brokedidood.info	dropzone	c/o Afilias
2314.	broncomm.info	dropzone	c/o Afilias
2315.	bucraggerie.info	dropzone	allen.peter@mail.com
2316.	bum-bam-sexy-blam.info	dropzone	himacss@yandex.ru
2317.	bum-bum.info	dropzone	himacss@yandex.ru
2318.	bumbums.info	dropzone	himacss@yandex.ru
2319.	bummaryhout.info	dropzone	c/o Afilias
2320.	burghne.info	dropzone	c/o Afilias
2321.	butteency.info	dropzone	c/o Afilias
2322.	cabinternme.info	dropzone	the.malware.cabal@gmail.com
2323.	cacheeseed.info	dropzone	c/o Afilias
2324.	cadenelec.info	dropzone	c/o Afilias
2325.	caffinform.info	dropzone	susanboyce@live.co.uk
2326.	canoede.info	dropzone	david.austin44@yahoo.com
2327.	carologel.info	dropzone	c/o Afilias
2328.	castee.info	dropzone	c/o Afilias
2329.	cdvqvnjqqtqhs0o.info	dropzone, infector	d97f84nn9rq@nameprivacy.com
2330.	cemesolele.info	dropzone	c/o Afilias
2331.	chairlorigh.info	dropzone	c/o Afilias
2332.	chariewildry.info	dropzone	c/o Afilias
2333.	cherry-free.info	dropzone	himacss@yandex.ru
2334.	chintal.info	dropzone	c/o Afilias
2335.	cholifo.info	dropzone	david.austin44@yahoo.com
2336.	chorge.info	dropzone	c/o Afilias
2337.	chuppines.info	dropzone	c/o Afilias
2338.	cjputyllqkyqylj.info	dropzone, infector	elkinselongate@yahoo.com
2339.	clemmet.info	dropzone	c/o Afilias
2340.	compapageon.info	dropzone	c/o Afilias
2341.	contocele.info	dropzone	c/o Afilias
2342.	contoppet.info	dropzone	c/o Afilias
2343.	copresiati.info	dropzone	c/o Afilias
2344.	crampinte.info	dropzone	c/o Afilias
2345.	cranian.info	dropzone	c/o Afilias
2346.	cranzartue.info	dropzone	c/o Afilias
2347.	crucery.info	dropzone	c/o Afilias
2348.	cognessa.info	dropzone	c/o Afilias
2349.	costarmo.info	dropzone	c/o Afilias
2350.	defealn.info	dropzone	c/o Afilias
2351.	deficilla.info	dropzone	c/o Afilias
2352.	defndl.info	dropzone	c/o Afilias
2353.	denistar.info	dropzone	c/o Afilias
2354.	desponechpo.info	dropzone	c/o Afilias
2355.	desprush.info	dropzone	c/o Afilias
2356.	diwance.info	dropzone	c/o Afilias
2357.	dogedbust.info	dropzone	c/o Afilias
2358.	dominmoney124.info	updater	repossesseddomain@godaddy.com
2359.	doorerti.info	dropzone	c/o Afilias
2360.	dortelwittle.info	dropzone	c/o Afilias
2361.	duceptive.info	dropzone	c/o Afilias

2362.	dulinepa.info	dropzone	c/o Afilias
2363.	dwyayer.info	dropzone	c/o Afilias
2364.	efuqxssjrwnrqeqk.info	dropzone, infector	ea2cm9ex6wp@nameprivacy.com
2365.	egiajfpsgwoqjhs.info	embedded_js	erivegutixo@yahoo.com
2366.	elsgoophqynbhkv.info	dropzone, infector	r793d9ww3fr@nameprivacy.com
2367.	eqwqpnriruqlhnhr.info	dropzone, infector	n75wc8m88ak@nameprivacy.com
2368.	eremitel0.info	dropzone	c/o Afilias
2369.	euzzpjntlskotws.info	dropzone, infector	waterscomprehensive@yahoo.com
2370.	evalgism.info	dropzone	c/o Afilias
2371.	excitta.info	dropzone	c/o Afilias
2372.	fastspy.info	dropzone, source, infector	admin@fastspy.info
2373.	federalreserve-report-domain.info	source	contact@myprivateregistration.com
2374.	federalreserve-report-download.info	source	malejo0828@yahoo.com
2375.	feudineedci.info	dropzone	c/o Afilias
2376.	fhoutive.info	dropzone	c/o Afilias
2377.	fixineed.info	dropzone	c/o Afilias
2378.	foveari.info	dropzone	c/o Afilias
2379.	fqlpvqvpvtzqpgqp.info	dropzone, infector	wm6vn79m42s@nameprivacy.com
2380.	fsojqkutpyohu.info	dropzone, infector	g856y7f88nz@nameprivacy.com
2381.	fwjvqkousppprt.info	dropzone, infector	benavideseuripides@yahoo.com
2382.	fzrgovjlvkwrwnx.info	dropzone, infector	g856y7f88nz@nameprivacy.com
2383.	galewindit.info	dropzone	c/o Afilias
2384.	ganapkinet.info	dropzone	c/o Afilias
2385.	gdolnlrqnronnn.info	dropzone, infector	jr7v53ge4pk@nameprivacy.com
2386.	giganatwo.info	dropzone	c/o Afilias
2387.	go6po.me	infector	kapany3y@mail.com
2388.	gomarichor.info	dropzone	c/o Afilias
2389.	gqvloeozbodgfwhg.info	dropzone, infector	yj55n8hw5nb@nameprivacy.com
2390.	grascowallbrick.info	updater	c/o Afilias
2391.	growupti.info	dropzone	c/o Afilias
2392.	gtgvwfqshlxtpkz.info	dropzone, infector	chenmilwaukee@yahoo.com
2393.	guenessollet.info	dropzone	c/o Afilias
2394.	guilldo.info	dropzone	c/o Afilias
2395.	gxsnxkqahaopsjnl.info	dropzone, source, infector	pu29m3h93qj@nameprivacy.com
2396.	habbiece.info	dropzone	c/o Afilias
2397.	hckqtsgpsstzmdp.info	dropzone, infector	larsenvicious@yahoo.com
2398.	hemdomance.info	dropzone	c/o Afilias
2399.	herinandrumen.info	dropzone	c/o Afilias
2400.	hgbu67bjyrturyuk.info	dropzone	purtucz@mail.ru
2401.	hjpxtnrenufxsvr.info	dropzone, infector	hjpxtnrenufxsvr.info
2402.	hjsdbkjnlsmdfa.info	source	qwdhjasvdhv@yahoo.com
2403.	hkkmqvttuqpo.info	dropzone, infector	wh6ar6z58hn@nameprivacy.com
2404.	hogchariane.info	dropzone	c/o Afilias
2405.	horali.info	dropzone	c/o Afilias
2406.	hztplrrfqmjyrrd.info	dropzone, source, infector	covizubewybebi@yahoo.com
2407.	iekfm migvpwtxpr.info	dropzone, infector	root@cheaplobstersny.com
2408.	imitall.info	dropzone	c/o Afilias
2409.	instationne.info	dropzone	c/o Afilias
2410.	jessatianator.info	dropzone	c/o Afilias
2411.	itkwvfquvnhtpi.info	dropzone, infector	waterscomprehensive@yahoo.com
2412.	iupmkmcprfnetfqs.info	dropzone, infector	wm6vn79m42s@nameprivacy.com
2413.	jmovpypolsgoqkoq.info	dropzone, infector	c/o Afilias
2414.	khchukqqsgxszr.info	dropzone, source, infector	downingcinerama@yahoo.com

2415.	killendl.info	dropzone	c/o Afilias
2416.	kkrhznwjsxgonmhk.info	dropzone, infector	rf7ph2w73fw@nameprivacy.com
2417.	korelererta.info	dropzone	c/o Afilias
2418.	kqgqmvarlsomrfql.info	dropzone, infector	kh3te68h3mx@nameprivacy.com
2419.	kratedin.info	dropzone	c/o Afilias
2420.	laconf.info	dropzone	hostmaster@proxad.net
2421.	ladyereredra.info	dropzone	c/o Afilias
2422.	lbulniluqhhlj.info	embedded_js	exytihazonac@yahoo.com
2423.	leenriller.info	dropzone	c/o Afilias
2424.	lklhprvhreuti.info	dropzone, infector	rh6fk9xv2q5@nameprivacy.com
2425.	lpsnbzozyhvpepyp.info	dropzone, infector	js5gx56c7w8@nameprivacy.com
2426.	lqfrowptqpchrxpn.info	dropzone, source, infector	bonillascenic@yahoo.com
2427.	lsusksvtvgkIrgnr.info	dropzone, source, infector	d38679a55tn@nameprivacy.com
2428.	ltiqqqslxworvm.info	dropzone, infector	nd44b2bm6z2@nameprivacy.com
2429.	mafia-wars.info	dropzone	domain-admin@easily.co.uk
2430.	manchm.info	dropzone	c/o Afilias
2431.	margagm.info	dropzone	c/o Afilias
2432.	marimettalf.info	dropzone	c/o Afilias
2433.	marisey.info	dropzone	paultribouillard@hotmail.co.uk
2434.	maximpa.info	dropzone	c/o Afilias
2435.	memoutaltyne.info	dropzone	c/o Afilias
2436.	merilia.info	dropzone	c/o Afilias
2437.	millierer.info	dropzone	c/o Afilias
2438.	mirupqtfvvvnzf.info	dropzone, infector	wv4k596n5se@nameprivacy.com
2439.	mnestrap.info	dropzone	c/o Afilias
2440.	modasiem.info	dropzone	c/o Afilias
2441.	moqlqtipnoqftrr.info	dropzone, infector	js5gx56c7w8@nameprivacy.com
2442.	morselantif.info	dropzone	c/o Afilias
2443.	motote.info	dropzone	c/o Afilias
2444.	mqqghryddzjyik.info	dropzone, infector	r793d9ww3fr@nameprivacy.com
2445.	mtqvovwtelpnuor.info	embedded_js	wycolynyhon@yahoo.com
2446.	muonuxxksinhhwv.info	dropzone, source, infector	rh6fk9xv2q5@nameprivacy.com
2447.	mupumgzpnuetqlp.info	dropzone, infector	webmaster@indianlegaltroops.com
2448.	muriadervai.info	dropzone	c/o Afilias
2449.	muskintenent.info	dropzone	c/o Afilias
2450.	myach-privacy-c.info	source	perditionMcmanusPl@yahoo.com
2451.	mynacha-solutions-o.info	source	admin@mynacha-solutions-o.info
2452.	mzoypqrctlwipiu.info	dropzone, source, infector	mx6np6jy4dc@nameprivacy.com
2453.	mzvlpddnlzguowr.info	dropzone, source, infector	uz9u78n867p@nameprivacy.com
2454.	nacha-report-domain-syst.info	source	roksoa@yahoo.com
2455.	nacha-report-downloads.info	source	milleralan42@yahoo.com
2456.	nacha-solutions-onow.info	source	admin@nacha-solutions-onow.info
2457.	nachasolutionst.info	source	carcinogenicWashingtonum@yahoo.com
2458.	newyaction.info	dropzone, source	erikschiwelnus@mailcan.com
2459.	newyaction123.info	updater	c/o Afilias
2460.	ngutoplqypnorsuu.info	dropzone, infector	benavideseuripides@yahoo.com
2461.	nisselfia.info	dropzone	c/o Afilias
2462.	nkhrutvvwnwkq.info	dropzone, source, infector	pd7hz3xc48r@nameprivacy.com
2463.	nkoqyzmlnrqo.info	dropzone, source, infector	seymourfarsighted@yahoo.com
2464.	nsjohymwqhjqiv.info	dropzone, infector	benavideseuripides@yahoo.com
2465.	ntuvpsknopsntuvg.info	dropzone, infector	a37zk7bv7v3@nameprivacy.com
2466.	nuthog.info	dropzone	c/o Afilias
2467.	nxknjssmizekbimq.info	dropzone, infector	rd9cp4t73dq@nameprivacy.com

2468.	nyctalkswag.info	dropzone	c/o Afilias
2469.	oculins.info	dropzone	c/o Afilias
2470.	oddmenterer.info	dropzone	c/o Afilias
2471.	ommlxlxlegpglhxiv.info	dropzone, infector	e255f24x5pb@nameprivacy.com
2472.	onlinecorporation.info	dropzone	exitthematrix@ymail.com
2473.	onvirudttwhfu.info	dropzone, infector	waterscomprehensive@yahoo.com
2474.	onwzpkcyvtuqq.info	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
2475.	opwhmilxsjkqdqe.info	dropzone, source, infector	rd9cp4t73dq@nameprivacy.com
2476.	orrheather.info	dropzone	orrheather.info
2477.	overnate.info	dropzone	c/o Afilias
2478.	paireeho.info	dropzone	c/o Afilias
2479.	paraud.info	dropzone	c/o Afilias
2480.	pardency.info	dropzone	c/o Afilias
2481.	paschoiceny.info	embedded_js	idymohobalu@yahoo.com
2482.	pathflite.info	dropzone	c/o Afilias
2483.	paulmasc.info	dropzone	c/o Afilias
2484.	peanerry.info	dropzone	c/o Afilias
2485.	peristoreder.info	dropzone	c/o Afilias
2486.	petrozedn.info	dropzone	c/o Afilias
2487.	phrendogm.info	dropzone	c/o Afilias
2488.	phytolo.info	dropzone	c/o Afilias
2489.	pidbusyqlzhkmqlk.info	dropzone, infector	c/o Afilias
2490.	pineapple-free.info	dropzone	himacss@yandex.ru
2491.	pingermi.info	dropzone	c/o Afilias
2492.	planacymric.info	dropzone	c/o Afilias
2493.	pnmtwnhxkgypk.info	dropzone, infector	z34jb9zq2a5@nameprivacy.com
2494.	pnudyprlhnuvzpjy.info	dropzone, infector	ea4cy5zc9n8@nameprivacy.com
2495.	poggene.info	dropzone	c/o Afilias
2496.	pookixusufvgkx.info	dropzone, source, infector	rd9cp4t73dq@nameprivacy.com
2497.	preteza.info	dropzone	c/o Afilias
2498.	pqiwumrdrmhmmtd.info	dropzone, infector	dt6gh2wj339@nameprivacy.com
2499.	provingsp.info	dropzone	c/o Afilias
2500.	pruringlyte.info	dropzone	c/o Afilias
2501.	psgzgaffrnvonvs.info	dropzone, infector	chenmilwaukee@yahoo.com
2502.	pubbeerlo.info	embedded_js	idymohobalu@yahoo.com
2503.	pxlilkqwfgxllme.info	dropzone, infector	c/o Afilias
2504.	qbdsesosgmsoqjio.info	dropzone, source, infector	d97f84nn9rq@nameprivacy.com
2505.	recalingbole.info	dropzone	c/o Afilias
2506.	recarban.info	dropzone	c/o Afilias
2507.	quantellaines.info	dropzone	c/o Afilias
2508.	querrysl.info	dropzone	c/o Afilias
2509.	quironet.info	dropzone	c/o Afilias
2510.	qvswpxlpqfwlpks.info	dropzone, infector	dt6gh2wj339@nameprivacy.com
2511.	rabotascuka.info	dropzone, updater	contact@privacyprotect.org
2512.	recrusawf.info	dropzone	c/o Afilias
2513.	redessenn.info	dropzone	c/o Afilias
2514.	relifemismiazo.info	dropzone	c/o Afilias
2515.	reneliastereren.info	dropzone	c/o Afilias
2516.	retankin.info	dropzone	c/o Afilias
2517.	retorihewor.info	dropzone	c/o Afilias
2518.	rettslrementtsInvesttsInglng.info	source	maksim_kugif@mail.ru
2519.	rhnwnnrrztoyqird.info	dropzone, source, infector	k86c98xv6bx@nameprivacy.com
2520.	rmmjmohwdnxuhqx.info	dropzone, infector	bonillascenic@yahoo.com

2521.	roxystyleech.info	dropzone	c/o Afilias
2522.	rpogugmqrpbzpp.info	dropzone, source, infector	c/o Afilias
2523.	rpxokscszptrx.info	dropzone, infector	repossesseddomain@godaddy.com
2524.	rqfqokssfomjqvd.info	dropzone, source, infector	j27vq4968ba@nameprivacy.com
2525.	rsanyhvdqhpqw.info	dropzone, infector	wh6ar6z58hn@nameprivacy.com
2526.	rumbt.info	dropzone	anatoliylis@yahoo.com
2527.	ruskiple.info	dropzone	c/o Afilias
2528.	salmidesilv.info	dropzone	c/o Afilias
2529.	saraard.info	dropzone	saraard.info@domainsbyproxy.com
2530.	sarysaileu.info	dropzone	c/o Afilias
2531.	savarideti.info	dropzone	c/o Afilias
2532.	scarlen.info	dropzone	c/o Afilias
2533.	scherce.info	dropzone	c/o Afilias
2534.	scoreboaton.info	dropzone	c/o Afilias
2535.	scoter.info	dropzone	c/o Afilias
2536.	scyton.info	dropzone	c/o Afilias
2537.	seconicil.info	dropzone	c/o Afilias
2538.	securityaim.info	source	purtucz@mail.ru
2539.	securitymark.info	source	purtucz@mail.ru
2540.	semipsium.info	dropzone	c/o Afilias
2541.	sfjpnuequoilx.info	dropzone, infector	dt6gh2wj339@nameprivacy.com
2542.	shipmess.info	dropzone	c/o Afilias
2543.	sjfwmoprjknpqq.info	dropzone, infector	c/o Afilias
2544.	skinny-hub.info	dropzone	himacss@yandex.ru
2545.	soundombrid.info	dropzone	c/o Afilias
2546.	spgjevglfnkskt.info	dropzone, infector	stepsonyoung@yahoo.com
2547.	spriguagebe.info	dropzone	c/o Afilias
2548.	sqfygstqqoyrl.info	dropzone, infector	repossesseddomain@godaddy.com
2549.	ssjgkktjugwgepz.info	dropzone, source, infector	d97f84nn9rq@nameprivacy.com
2550.	stansforgingst.info	dropzone	c/o Afilias
2551.	starmainid.info	dropzone	c/o Afilias
2552.	star-tu-o-ticket.info	source	carpBmAmbrose@yahoo.com
2553.	stepperence.info	dropzone	c/o Afilias
2554.	suierovkqoxrzmmmb.info	dropzone, source, infector	osborntablespoon@yahoo.com
2555.	sustdxvsknlbrpn.info	dropzone, infector	jt9xs7y73p5@nameprivacy.com
2556.	sweatorizzl.info	dropzone	c/o Afilias
2557.	symmhock.info	dropzone	c/o Afilias
2558.	synager.info	dropzone	c/o Afilias
2559.	syotxofmipxosijj.info	dropzone, source, infector	c/o Afilias
2560.	tempeliad.info	dropzone	c/o Afilias
2561.	teniangsymp.info	dropzone	c/o Afilias
2562.	theinternationaltravel.info	source	sachin@search-value.com
2563.	thlypter.info	dropzone	c/o Afilias
2564.	thymigr.info	dropzone	c/o Afilias
2565.	tihryljrhttowkk.info	dropzone, source, infector	d67rg3d97jp@nameprivacy.com
2566.	tioneeti.info	dropzone	c/o Afilias
2567.	titiverie.info	dropzone	c/o Afilias
2568.	tnzmolrsjrzhc.info	dropzone, infector	yc9wy3c75gv@nameprivacy.com
2569.	tonismanna.info	dropzone	c/o Afilias
2570.	touchettage.info	dropzone	c/o Afilias
2571.	tsoriantry.info	dropzone	c/o Afilias
2572.	tufsverkvghmlm.info	dropzone, infector	rd9cp4t73dq@nameprivacy.com
2573.	turnetteju.info	dropzone	c/o Afilias

2574.	tutiora.info	dropzone	c/o Afilias
2575.	uncisi.info	dropzone	c/o Afilias
2576.	uopjmzjxkrpqqt.info	dropzone, infector	vd6fy5a996t@nameprivacy.com
2577.	uralersole.info	dropzone	c/o Afilias
2578.	utuihhndtmitunv.info	dropzone, infector	root@cheaplobstersny.com
2579.	uyzrmqsuktjbqg.info	dropzone, source, infector	hv59t3tr3v6@nameprivacy.com
2580.	uznloepzpertqrs.info	dropzone, source, infector	ingrownadams@yahoo.com
2581.	venevers.info	dropzone	c/o Afilias
2582.	verstran.info	dropzone	ashlyevans@live.co.uk
2583.	vmnszmothuovvoll.info	dropzone, infector	univalentlongoria@yahoo.com
2584.	vocatagit.info	dropzone	c/o Afilias
2585.	vohrudopljluv.info	dropzone, infector	ge4nx92w6rk@nameprivacy.com
2586.	vspqtnowemfjlsu.info	dropzone, infector	uz9u78n867p@nameprivacy.com
2587.	vtkmkxtngplkkst.info	dropzone, source, infector	contact@privacyprotect.or
2588.	vvvsfmnnqowoevh.info	dropzone, infector	rd9cp4t73dq@nameprivacy.com
2589.	vxspuuqdrknvyoqw.info	dropzone, infector, source	ns5m23ur84w@nameprivacy.com
2590.	wanigle.info	dropzone	c/o Afilias
2591.	wardwatt.info	dropzone	c/o Afilias
2592.	wergerf.info	dropzone, source, infector	faterins@gmail.com
2593.	whenererer.info	dropzone	c/o Afilias
2594.	wifi-hardware.info	source	carpBmAmbrose@yahoo.com
2595.	wrapmyarmsand.info	source	admin@neverbealoneorlethim.info
2596.	wrssrjqpiyfsmwp.info	dropzone, source, infector	scripturecrocker@yahoo.com
2597.	domain123456789.info	dropzone, source	jobs@facebookjob.de
2598.	xaviestocri.info	dropzone	c/o Afilias
2599.	xfjcnoniyiwwrp.info	dropzone, source, infector	j35gg6na33k@nameprivacy.com
2600.	xjkotrupqefjnnoz.info	dropzone, source, infector	wh6ar6z58hn@nameprivacy.com
2601.	xusqryriqhztq.info	dropzone, source, infector	hv59t3tr3v6@nameprivacy.com
2602.	xvqlmellirsryh.info	dropzone, source, infector	ge2zu9xk6mp@nameprivacy.com
2603.	yjwstksxxpmul.info	dropzone, infector	ag9wf9hb8uu@nameprivacy.com
2604.	ynnssrpdcuqmlrer.info	dropzone, source, infector	repossesseddomain@godaddy.com
2605.	yqyphsmxmovzmjwu.info	dropzone, source, infector	apprehensivebrandt@yahoo.com
2606.	yrvdpwsllswkpqsbq.info	dropzone, source, infector	d448j8f25nx@nameprivacy.com
2607.	ziswptyqtjohtm.info	dropzone, infector	larsenvicious@yahoo.com
2608.	zardback.info	dropzone	c/o Afilias
2609.	zigzare.info	dropzone	c/o Afilias
2610.	zmdkjzrsmusshqqlq.info	dropzone, source, infector	jr7v53ge4pk@nameprivacy.com
2611.	zorzpyqrpkckmtfx.info	dropzone, source, infector	meansspeedometer@yahoo.com
2612.	zsoqjlsznussh.info	dropzone, source, infector	scripturecrocker@yahoo.com
2613.	charterbeans.info	dropzone, infector	srivastava.akshay1@gmail.com
2614.	dominmoney124.info	updater	repossesseddomain@godaddy.com
2615.	gotoberlin.info	infector	alexaklark@gomail.com
2616.	grascowallbrick.info	updater	c/o Afilias
2617.	renwoxing.me	dropzone, infector	e59e@qq.com
2618.	theddos.me	dropzone, infector	hostmaster@one.com
2619.	ygnlgxyzamfxvl.info	infector	c/o Afilias
2620.	level-3.me	dropzone	f18361511b324849911182c54d185df4.protect @whoisguard.com

Public Interest Registry (PIR)
1775 Wiehle Avenue
Suite 200
Reston Virginia 20190
United States

	Harmful Botnet Domain Name	Type	Whois Email Address
2621.	barclaysghana.org	dropzone, infector	sec.indi@yahoo.com
2622.	pganalytics.org	updater	c/o Public Interest Registry
2623.	wcgplaynow.org	dropzone, infector	admin@macro-store.com
2624.	wsqwehnjjppxrgxp.org	infector	c67cv95z47c@nameprivacy.com
2625.	wuvwqckpzfxrqi.org	infector	c/o Public Interest Registry
2626.	strujkysnimem.org	source	eusaok34f2bfa8becb0e@w86bna54f21bffa2ffd1.privatewhois.net
2627.	myapps-ups.org	infector	dfhcsdfs@126.com
2628.	hnwxqurqjvynwljf.org	infector	c/o Public Interest Registry
2629.	jcmtczpwontvppnt.org	infector	sb6n59an64m@nameprivacy.com
2630.	jliqigsnggdwxp.org	infector	sb6n59an64m@nameprivacy.com
2631.	just-ping.org	dropzone, infector	williammitchellworld@yahoo.com
2632.	mswqvxohtfnzj.org	infector	c/o Public Interest Registry
2633.	muzonline.org	dropzone, infector, source	admin@macro-store.com
2634.	mybackupdns.org	infector	ftgy23fge@126.com
2635.	nameservers.org	dropzone, infector	ftgy23fge@126.com
2636.	adventurefinder.org	source	rowenachauvin@ymail.com
2637.	bobevanscoupons.org	source	bobevanscoupons.org@domainsbyproxy.com
2638.	boboyes.org	updater	gmvjcxkxhs@whoisservices.cn
2639.	cosainse.org	dropzone, source	bormorler@gmail.com
2640.	cqlqycknfcoovvn.org	dropzone, source, infector	ns5m23ur84w@nameprivacy.com
2641.	dlmsonisfzsioqq.org	dropzone, infector	d97f84nn9rq@nameprivacy.com
2642.	download-report-nacha.org	source	derewsater@yahoo.com
2643.	dunegoon.org	infector	ajmorgan@pacifier.com
2644.	ehsswiirxmsmoxxc.org	dropzone, infector	b52fp2qw5ys@nameprivacy.com
2645.	eijqgpqqsuht.org	dropzone, infector	d38679a55tn@nameprivacy.com
2646.	ephmvzsnppmnzqzk.org	dropzone, infector	d38679a55tn@nameprivacy.com
2647.	evzqffspxhsvf.org	dropzone, infector	excelat.co
2648.	eyphqugjugprphvn.org	dropzone, infector	hy4r394j6ja@nameprivacy.com
2649.	fggsrmvkmlwulq.org	dropzone, source, infector	k86c98xv6bx@nameprivacy.com
2650.	fltsptygppvqdoy.org	dropzone, source, infector	cr65g2ap483@nameprivacy.com
2651.	fqkmrulylslzrtm.org	dropzone, infector	c/o Public Interest Registry
2652.	gsqptneinjuwl.org	dropzone, infector	f76ah7cb472@nameprivacy.com
2653.	gphtznwlcqgq.org	dropzone, infector	wv4k596n5se@nameprivacy.com
2654.	gtxwqptngkltozv.org	dropzone, infector	dt6gh2wj339@nameprivacy.com
2655.	gultpurplppiwt.org	dropzone, infector	xr3sg3h779x@nameprivacy.com
2656.	hgbu67bjyrturyuk.org	dropzone	hgbu67bjyrturyuk.org@domainsbyproxy.com
2657.	hisioqkdtqcotbqr.org	dropzone, infector	gv9st8nk4ka@nameprivacy.com
2658.	hrxnqnkovlvssuiv.org	dropzone, infector	refectionongay@yahoo.com
2659.	hupppszsqlqmjsp.org	dropzone, infector	y77jc7ys7xp@nameprivacy.com
2660.	huyaqwop.org	updater	contact@webdomainsbyproxy.com
2661.	hwqpgrimknqkfizg.org	dropzone, infector	hv59t3tr3v6@nameprivacy.com
2662.	iuqbutilloqhooi.org	dropzone, infector	ingramprice@yahoo.com
2663.	inqppkqajlnrsjkh.org	dropzone, infector, source	apprehensivebrandt@yahoo.com
2664.	ioqtvrnjmwrm.org	dropzone, source, infector	fraserafrica@yahoo.com
2665.	itnhtwodvkronw.org	dropzone, infector	am9zr2nq3p8@nameprivacy.com

2666.	jdzqkltenlmi.org	dropzone, infector	u583p92r8uv@nameprivacy.com
2667.	jmjjeqfunuotriion.org	dropzone, source, infector	apprehensivebrandt@yahoo.com
2668.	jpubusmoaelmept.org	dropzone, infector	hostmaster@above.com
2669.	jssqjwuqwrkxkmz.org	dropzone, infector	yj55n8hw5nb@nameprivacy.com
2670.	jxwoplyqbtqlodx.org	dropzone, infector	webmaster@indianlegaltroops.com
2671.	kdnrjewtvsqujnk.org	dropzone, infector	fn4u39er8bh@nameprivacy.com
2672.	kkhoukytqmxwxrfs.org	dropzone, infector	r46qz65d8xg@nameprivacy.com
2673.	kldsvyjjfyqdpqtv.org	dropzone, infector	amadeus_logan@yahoo.com
2674.	knxohnzsrvti.org	dropzone, infector	k87td33t8xf@nameprivacy.com
2675.	koqlplnulwksxule.org	dropzone, infector	wm6vn79m42s@nameprivacy.com
2676.	kpjprkqhsmqrmsj.org	dropzone, source, infector	am9zr2nq3p8@nameprivacy.com
2677.	ldkvpuuhxloipv.org	dropzone, source, infector	ne26s6sf8v2@nameprivacy.com
2678.	kwqocmfplthiyfs.org	dropzone, infector	wh6ar6z58hn@nameprivacy.com
2679.	lmpgvpmjfidqsw.org	dropzone, infector	wm6vn79m42s@nameprivacy.com
2680.	lntepipjekorqhi.org	dropzone, source, infector	xy9u66ja35d@nameprivacy.com
2681.	lvvuokuqwwnsjdm.org	dropzone, infector	rf7ph2w73fw@nameprivacy.com
2682.	mlslndjveljmdppr.org	dropzone, source, infector	c/o Public Interest Registry
2683.	mfevsldswrkmpjj.org	dropzone, infector	rf7ph2w73fw@nameprivacy.com
2684.	mjxjgnvcfswqwp.org	dropzone, infector	declaratoryfoote@yahoo.com
2685.	mnptwsoweulqpqo.org	dropzone, source, infector	c/o Public Interest Registry
2686.	mogstoquqrutjjto.org	dropzone, infector	amadeus_logan@yahoo.com
2687.	nacha-trans.org	source	contact@myprivateregistration.com
2688.	nacha-transactions.org	source	admin@nacha-transactions.org
2689.	nacha-ach.org	source	loralio43@yahoo.com
2690.	nacha-alert.org	source	contact@myprivateregistration.com
2691.	nacha-online.org	source	poruesaw@yahoo.com
2692.	nacha-report.org	source	admin@nacha-report.org
2693.	nacha-reports.org	source	admin@nacha-reports.org
2694.	nacha-wire.org	source	loralio43@yahoo.com
2695.	nkowprjysxxocxjy.org	dropzone, infector	nd44b2bm6z2@nameprivacy.com
2696.	nnlhruyyrkvjmr.org	dropzone, infector	d97f84nn9rq@nameprivacy.com
2697.	nnqjvqrhnqljeqn.org	dropzone, infector	wm6vn79m42s@nameprivacy.com
2698.	novodebt.org	dropzone	anatoliyliis@yahoo.com
2699.	nqurjfgjolirrrpy.org	dropzone, source, infector	wm6vn79m42s@nameprivacy.com
2700.	nsbewpkwpmrxkmup.org	dropzone, infector	k86c98xv6bx@nameprivacy.com
2701.	nuiojpgvrsqkowz.org	dropzone, infector	vd6fy5a996t@nameprivacy.com
2702.	nzighwrmvkjusvn.org	dropzone, source, infector	c/o Public Interest Registry
2703.	oqlzyrwnoixsqsom.org	dropzone, source, infector	be98f37p79m@nameprivacy.com
2704.	ospvagkqcniomozs.org	dropzone, infector	uz9u78n867p@nameprivacy.com
2705.	oswash.org	source	info@vibit.eu
2706.	ozrollfjqkrjhtor.org	dropzone, source, infector	ingrownadams@yahoo.com
2707.	peoriaautoshow.org	dropzone	contact@privacyprotect.org
2708.	perdfcovjoldtv.org	dropzone, source, infector	am9zr2nq3p8@nameprivacy.com
2709.	personal-web-security.org	source	admin@personal-web-security.org
2710.	pganalytcs.org	updater	c/o Public Interest Registry
2711.	pmqnhzymsoopqhog.org	dropzone, source, infector	wh6ar6z58hn@nameprivacy.com
2712.	pnutmmmmjclvrtnqn.org	dropzone, source, infector	d97f84nn9rq@nameprivacy.com
2713.	pozpwukkuoyhwrnm.org	dropzone, infector	dt6gh2wj339@nameprivacy.com
2714.	ppruxxpqpewtuym.org	dropzone, infector	meansspeedometer@yahoo.com
2715.	pqrymyojvrnxos.org	embedded_js	contact@privacyprotect.org
2716.	prwlunqikkawbfv.org	dropzone, source, infector	n75wc8m88ak@nameprivacy.com
2717.	psuqtoosnolpmju.org	dropzone, source, infector	wh6ar6z58hn@nameprivacy.com
2718.	pvupsppujstxpfc.org	dropzone, source, infector	dd3t93pu55u@nameprivacy.com

2719.	pxsqzfqspwklu.org	dropzone, source, infector	hv59t3tr3v6@nameprivacy.com
2720.	qcjrelphrnrojx.org	dropzone, source, infector	downingcinerama@yahoo.com
2721.	qeikltnsjojtsdgf.org	dropzone, source, infector	wn2597rp22x@nameprivacy.com
2722.	qetvlivjxwiqj.org	dropzone, infector	js5gx56c7w8@nameprivacy.com
2723.	qgwsnpgtiexlp.org	dropzone, source, infector	bonillascenic@yahoo.com
2724.	qretnmirnjmppe.org	dropzone, infector	bonillascenic@yahoo.com
2725.	qrujovkkngzlop.org	dropzone, infector	humphreyts@yahoo.com
2726.	qrwprgnrykrsvwf.org	dropzone, infector	be98f37p79m@nameprivacy.com
2727.	qtjmnpjfqosool.org	dropzone, source, infector	m84np6jd4gt@nameprivacy.com
2728.	qtqlornqkvsum.org	dropzone, source, infector	u65dt7q82a7@nameprivacy.com
2729.	quantserv.org	embedded_js	admin@quantserv.org
2730.	quqnxnqeinqohjcso.org	dropzone, infector	wv4k596n5se@nameprivacy.com
2731.	quisihtqckpgprfg.org	dropzone, infector	contact@privacyprotect.org
2732.	qymrxmskrjltps.org	dropzone, infector	cz99x6ay7h2@nameprivacy.com
2733.	repleyser.org	embedded_js	lexus333new@yahoo.com
2734.	reports-nacha.org	source	polonokias@yahoo.com
2735.	rliuvqcvxgbtyj.org	dropzone, infector	meansspeedometer@yahoo.com
2736.	rsjgssfrvmnvmiltg.org	dropzone, source, infector	am9zr2nq3p8@nameprivacy.com
2737.	rstwvoqfpqyqql.org	dropzone, infector	d67rg3d97jp@nameprivacy.com
2738.	rumbt.org	dropzone	anatoliylis@yahoo.com
2739.	rzqsundonswmtox.org	dropzone, source, infector	vf5vt9yz384@nameprivacy.com
2740.	muabanxetai.org	dropzone	muabanxetai.org@protecteddomainservices.com
2741.	mxocrmlxgkrkeppy.org	dropzone, infector	e255f24x5pb@nameprivacy.com
2742.	mxpithhmmjxpvpse.org	dropzone, infector	univalentlongoria@yahoo.com
2743.	sptospivowopxpvx.org	dropzone, infector	rd9cp4t73dq@nameprivacy.com
2744.	strujkysnimem.org	source	eusaok34f2bfa8becb0e@w86bna54f21bffa2ffd1_privatewhois.net
2745.	tfrxtwxpmjnswl.org	dropzone, source, infector	gv9st8nk4ka@nameprivacy.com
2746.	thnskivvpkimmzw.org	dropzone, source, infector	c/o Public Interest Registry
2747.	tivbekwplurydgr.org	dropzone, infector	armeniangillespie@yahoo.com
2748.	tmkclsstnskukmtj.org	dropzone, infector	am9zr2nq3p8@nameprivacy.com
2749.	tkmwplnhmdgr.org	dropzone, infector	u583p92r8uv@nameprivacy.com
2750.	tttzrivfpvlmvui.org	dropzone, source, infector	k86c98x6bx@nameprivacy.com
2751.	tynijxrmutqsnqf.org	dropzone, infector	yj55n8hw5nb@nameprivacy.com
2752.	tyussplqyvsutegr.org	dropzone, infector	s82z84x55fs@nameprivacy.com
2753.	ucwrlztmqpzumkjs.org	dropzone, infector	rf7ph2w73fw@nameprivacy.com
2754.	ujmqqkpwwpzpem.org	dropzone, source, infector	exorbitantbonilla@yahoo.com
2755.	ujzsilqouzjsqep.org	dropzone, infector	v56dt2ey98u@nameprivacy.com
2756.	uofmneuppmshqjpz.org	dropzone, infector, source	ns5m23ur84w@nameprivacy.com
2757.	vhirpnoulgmusqz.org	dropzone, infector	condolencelangford@yahoo.com
2758.	visitmyblog.org	embedded_js	gmvjcxkhs@whoisservices.cn
2759.	vuihtdsoonutxvdk.org	dropzone, source, infector	wh6ar6z58hn@nameprivacy.com
2760.	wbutitosldtnmbrf.org	dropzone, source, infector	jr7v53ge4pk@nameprivacy.com
2761.	wcgplaynow.org	infector	admin@macro-store.com
2762.	wevnorqvdkpmu.org	dropzone, infector	u65dt7q82a7@nameprivacy.com
2763.	whakrxuonsqhived.org	dropzone, source, infector	h58ys7kg989@nameprivacy.com
2764.	wkrvvojpqvqznmppm.org	dropzone, source, infector	dd3t93pu55u@nameprivacy.com
2765.	xolycnpprskxnt.org	dropzone, source, infector	d97f84nn9rq@nameprivacy.com
2766.	xomsmpotrxxrrol.org	dropzone, infector	f76ah7cb472@nameprivacy.com
2767.	ybjcqwwwnqgsinmk.org	dropzone, infector	wh6ar6z58hn@nameprivacy.com
2768.	ycyyfqsjptiorc.org	embedded_js	wycolynyhon@yahoo.com
2769.	ylklqmpuqqtmssnh.org	dropzone, source, infector	fractureglenn@yahoo.com
2770.	ymwvffjrosntpzqr.org	dropzone, infector	fitchguyana@yahoo.com
2771.	ytpczxtfxuzftxp.org	dropzone, infector, source	ns5m23ur84w@nameprivacy.com

2772.	zuidmzuhpumogq.org	dropzone, source, infector	c/o Public Interest Registry
2773.	zoflnpyvpknxolkp.org	dropzone, infector	x26qt7dr3b4@nameprivacy.com
2774.	analyticdns.org	infector, dropzone	dfghrter@hotmail.com
2775.	au.quantserv.org	embedded js	admin@quantserv.org
2776.	chamska.org	dropzone, infector	livemetal88@hotmail.com
2777.	cordsrilanka.org	infector	vasanthb@yahoo.com
2778.	countrysefa.org	infector	contact@webdomainsbyproxy.com
2779.	daraskiluk.org	dropzone, infector	hyrdbih4f2bb505cf760@w86bna54f21bffa2ffd1 .privatewhois.net
2780.	games4win.org	dropzone, infector	admin@macro-store.com
2781.	united-trans.org	infector	united-trans.org@contactprivacy.com
2782.	yuelqmpimjxsmn.org	infector	transfers-auth@names.co.uk
2783.	zapppol.org	dropzone, infector	rs7qw1b4f275a33c4d65@w86bna54f21bffa2ffd1 .privatewhois.net
2784.	pganalytics.org	updater	c/o Public Interest Registry
2785.	dev.simulinix.org	infector, dropzone	admin@simulinix.org
2786.	key-finance.org		billhrodriguez18423@gmail.com

**Coordination Center for TLD RU
8, Zoologicheskaya str.
Moscow 123242
Russian Federation**

**Coordination Center for TLD RU
Bolshoy Golovin, 23
107045 Moscow,
Russian Federation**

	Harmful Botnet Domain Name	Type	Whois Email Address
2787.	uralgaz.ru	infector	https://www.nic.ru/whois
2788.	uskamalchik.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2789.	vardington7.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2790.	vastcoins.ru	infector	http://www.reg.ru/whois/admin_contact
2791.	edgefox.ru	infector	http://www.reg.ru/whois/admin_contact
2792.	xlamonline.ru	infector	http://www.reg.ru/whois/admin_contact
2793.	xoophafiel.ru	infector	https://client.naunet.ru/c/whoiscontact
2794.	youdontfkjbaher.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2795.	youngmetal.ru	infector	http://www.reg.ru/whois/admin_contact
2796.	yourtulip.ru	dropzone	http://www.reg.ru/whois/admin_contact
2797.	zanyquery.ru	dropzone	http://www.reg.ru/whois/admin_contact
2798.	zenhour.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2799.	zlen.ru	dropzone	https://partner.r01.ru/contact_admin.khtml
2800.	zxlake3.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2801.	shoshololo.ru	dropzone, source, infector	http://www.reg.ru/whois/admin_contact
2802.	taxescell.ru	updater	http://www.reg.ru/whois/admin_contact
2803.	telefonchukcha.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2804.	tg2000.ru	dropzone, infector	https://www.nic.ru/whois
2805.	theshop.su	dropzone, infector	londry32@mail.ru
2806.	tixuanabridge.ru	infector	https://client.naunet.ru/c/whoiscontact
2807.	toplake.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2808.	topupdate.ru	infector	http://whois.webnames.ru
2809.	topupdater.ru	infector	http://whois.webnames.ru
2810.	topupdaters.ru	dropzone, infector	http://whois.webnames.ru
2811.	topupdates.ru	dropzone, infector	http://whois.webnames.ru
2812.	toxicyack.ru	dropzone	http://www.reg.ru/whois/admin_contact
2813.	truststats.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2814.	trutofmymemory.su	dropzone	trutof@ca4.ru
2815.	tunesfrag.ru	dropzone	http://www.reg.ru/whois/admin_contact
2816.	uerstatepw.ru	dropzone	http://www.reg.ru/whois/admin_contact
2817.	ukadevochka.ru	infector	http://www.reg.ru/whois/admin_contact
2818.	uklopandaberk.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2819.	underfeet.ru	infector	http://www.reg.ru/whois/admin_contact
2820.	sgy.ru	infector	https://client.naunet.ru/c/whoiscontact
2821.	shokoladdeath.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2822.	sickstage.ru	infector	http://www.reg.ru/whois/admin_contact
2823.	siimplesale.ru	dropzone, infector	http://whois.webnames.ru
2824.	simulatorimage.ru	dropzone	https://client.naunet.ru/c/whoiscontact

2825.	skykeyboard2.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2826.	smartcheat.ru	dropzone	http://www.reg.ru/whois/admin_contact
2827.	smokybear.ru	infector	http://www.reg.ru/whois/admin_contact
2828.	snotarms.ru	dropzone	http://www.reg.ru/whois/admin_contact
2829.	softmarket-drom.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2830.	softmarkets.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2831.	soretag.ru	dropzone	http://www.reg.ru/whois/admin_contact
2832.	staplescratch.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2833.	staticplan.ru	dropzone	http://whois.webnames.ru
2834.	steelcinetechs.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2835.	stfutheims.ru	infector	https://client.naunet.ru/c/whoiscontact
2836.	stripsneko.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2837.	styleforyour.ru	infector	http://www.webdrive.ru/webmail/
2838.	svjazbila.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2839.	wrapweb.ru	source	http://www.reg.ru/whois/admin_contact
2840.	deepanalyse.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2841.	potvamp.ru	infector	http://www.reg.ru/whois/admin_contact
2842.	ptichka.ru	dropzone	https://partner.r01.ru/contact_admin.khtml
2843.	purecash.ru	infector	http://www.reg.ru/whois/admin_contact
2844.	pyrohost.su	dropzone, infector	wizzardz01@hotmail.com
2845.	queenchair.ru	dropzone	http://www.reg.ru/whois/admin_contact
2846.	quoteandrun.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2847.	rabbitsgohole.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2848.	rehandntersfee.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2849.	rioamazonas.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2850.	rmlake1.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2851.	roguefood.ru	infector	http://www.reg.ru/whois/admin_contact
2852.	rogueroad.ru	infector	http://www.reg.ru/whois/admin_contact
2853.	routerstructo.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2854.	rudeink.ru	dropzone	http://www.reg.ru/whois/admin_contact
2855.	runnystorm.ru	dropzone	http://www.reg.ru/whois/admin_contact
2856.	sarjnessfundof.su	dropzone	sarjness@free-id.ru
2857.	sdkjgndfjnf.ru	infector	https://client.naunet.ru/c/whoiscontact
2858.	seawoljoystick.ru	infector	https://client.naunet.ru/c/whoiscontact
2859.	secondconcert.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2860.	secureserfingnet.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2861.	ourtulip.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2862.	ozoneiphone.ru	dropzone	http://www.reg.ru/whois/admin_contact
2863.	papertulip.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2864.	pearlrumor.ru	dropzone	http://www.reg.ru/whois/admin_contact
2865.	pellicslotersa.ru	infector	https://client.naunet.ru/c/whoiscontact
2866.	phoneajoystick.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2867.	photo-repair.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2868.	plantlunch.ru	dropzone	http://www.reg.ru/whois/admin_contact
2869.	plastpromcentr.ru	dropzone	http://whois.webnames.ru
2870.	poisk.su	dropzone	lionalex@hotmail.ru
2871.	popspostenkple.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2872.	villiam-grea.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2873.	viperos.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2874.	vologdansk.ru	dropzone, infector	http://whois.webnames.ru
2875.	vvmmp.ru	infector	https://www.nic.ru/whois
2876.	wardeed.ru	dropzone	http://www.reg.ru/whois/admin_contact
2877.	warynews.ru	infector	http://www.reg.ru/whois/admin_contact

2878.	weaktrash.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2879.	weaponomd.ru	dropzone, infector	https://cp.masternname.ru/domain_feedback/
2880.	wearysnake.ru	dropzone	http://www.reg.ru/whois/admin_contact
2881.	westfight.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2882.	wildboy.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2883.	winner-bets.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2884.	witlion.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2885.	naughtywifepal.ru	infector	https://client.naunet.ru/c/whoiscontact
2886.	nearhog.ru	dropzone	http://www.reg.ru/whois/admin_contact
2887.	netupdate1.ru	dropzone, infector	http://whois.webnames.ru
2888.	netupdate4.ru	dropzone, infector	http://whois.webnames.ru
2889.	netupdate5.ru	dropzone, infector	http://whois.webnames.ru
2890.	netupdate8.ru	dropzone, infector	http://whois.webnames.ru
2891.	netupdater.ru	dropzone, infector	http://whois.webnames.ru
2892.	netupdaters.ru	dropzone, infector	http://whois.webnames.ru
2893.	netupdates.ru	dropzone, infector	http://whois.webnames.ru
2894.	netupdatings.ru	dropzone, infector	http://whois.webnames.ru
2895.	nicefilmsa.ru	infector	https://partner.r01.ru/contact_admin.khtml
2896.	nuttyknack.ru	dropzone	http://www.reg.ru/whois/admin_contact
2897.	okrug2-bel.ru	infector	https://www.nic.ru/whois
2898.	oneant.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2899.	onemoretimehi.ru	infector	https://client.naunet.ru/c/whoiscontact
2900.	onepet.ru	infector	http://www.reg.ru/whois/admin_contact
2901.	onlinereger.ru	dropzone, infector	http://whois.webnames.ru
2902.	openlocalsnet.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2903.	makethemdie.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2904.	mationsperohe.ru	infector	https://client.naunet.ru/c/whoiscontact
2905.	midbomb.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2906.	mildtune.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2907.	minihose.ru	dropzone	http://www.reg.ru/whois/admin_contact
2908.	miniokoyokolia.su	dropzone	resaw@fastermail.ru
2909.	missboys.ru	infector	http://www.reg.ru/whois/admin_contact
2910.	missershmidt.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2911.	mlm-book.ru	infector	https://www.nic.ru/whois
2912.	moodgum.ru	updater	http://www.reg.ru/whois/admin_contact
2913.	muchachoslot.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2914.	munaeghohz.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2915.	nahwisohch.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2916.	namemybet.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2917.	kawabungashop.ru	infector	https://client.naunet.ru/c/whoiscontact
2918.	kosmovodki.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2919.	lameedge.ru	dropzone	http://www.reg.ru/whois/admin_contact
2920.	lesslane.ru	infector	http://www.reg.ru/whois/admin_contact
2921.	letstarting.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2922.	liberweb.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2923.	lostyear.ru	infector	http://www.reg.ru/whois/admin_contact
2924.	lowerdog.ru	infector	http://www.reg.ru/whois/admin_contact
2925.	logicaltrading.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2926.	makeitso.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2927.	makemealive.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2928.	holdorgold.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2929.	hotupdaters.ru	dropzone	http://whois.webnames.ru
2930.	hselrurele.ru	infector	http://whois.webnames.ru

2931.	huntersamplifi.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2932.	huntersrafters.ru	infector	https://client.naunet.ru/c/whoiscontact
2933.	ignis.net.ru	dropzone, infector	kshabanov@list.ru
2934.	indingo.ru	dropzone	http://www.reg.ru/whois/admin_contact
2935.	ionicfood.ru	infector	usage@ppmail.ru
2936.	ironsum.ru	infector	http://www.reg.ru/whois/admin_contact
2937.	ishopsystem.ru	infector	https://client.naunet.ru/c/whoiscontact
2938.	itchyclock.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2939.	itchysauce.ru	dropzone	http://www.reg.ru/whois/admin_contact
2940.	itisagooddaytodie.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2941.	jad3.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2942.	jamesbondajent.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2943.	jetcrafting.ru	infector	https://cp.mastername.ru/domain_feedback/
2944.	jjustdoit.ru	dropzone, infector	http://whois.webnames.ru
2945.	johninjucy.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2946.	jupaizeuph.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2947.	gerlsipslokane.su	infector	gerlsipslokane@bz3.ru
2948.	ghostbusters.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2949.	ghosttrick.ru	dropzone, infector	https://partner.r01.ru/contact_admin.khtml
2950.	gigasoftware.ru	infector	https://client.naunet.ru/c/whoiscontact
2951.	godfix.ru	dropzone, infector	clients.agava.ru/whois/admin_contact
2952.	gorycup.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2953.	greathell.ru	dropzone	http://www.reg.ru/whois/admin_contact
2954.	greatjazz.ru	infector	http://www.reg.ru/whois/admin_contact
2955.	hairme.ru	infector	http://www.reg.ru/whois/admin_contact
2956.	haltermancelo.ru	infector	https://client.naunet.ru/c/whoiscontact
2957.	heyitsme.ru	infector	http://www.reg.ru/whois/admin_contact
2958.	ftwtogether.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2959.	fastgoal.ru	dropzone, infector	https://www.nic.ru/whois
2960.	fattree.ru	infector	http://www.reg.ru/whois/admin_contact
2961.	favino.ru	dropzone, infector	https://partner.r01.ru/contact_admin.khtml
2962.	filebale.ru	dropzone	http://www.reg.ru/whois/admin_contact
2963.	finans-group-global.ru	infector	http://whois.webnames.ru
2964.	florianarray.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2965.	cornlion.ru	updater	http://www.reg.ru/whois/admin_contact
2966.	cruelsummer.ru	dropzone	https://cp.mastername.ru/domain_feedback/
2967.	cvmed.ru	infector	https://www.nic.ru/whois
2968.	dartzofmybpull.ru	infector	https://client.naunet.ru/c/whoiscontact
2969.	delovar999.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2970.	dolgosting.ru	dropzone, infector	http://whois.webnames.ru
2971.	domeafavour.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2972.	fabsnot.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2973.	face18.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2974.	fakepict.ru	dropzone, infector	jamcnutt111@hotmail.com
2975.	dvsdfvsw.narod2.ru	infector	https://www.nic.ru/whois
2976.	earlyship.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2977.	ecommerceone.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2978.	eepeohothe.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2979.	esperadooptic.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2980.	companian-usa.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2981.	coolsofa.ru	dropzone	http://www.reg.ru/whois/admin_contact
2982.	cooltruling.ru	infector	https://client.naunet.ru/c/whoiscontact
2983.	axeswizardpx.ru	infector	https://client.naunet.ru/c/whoiscontact

2984.	basiliskos.ru	dropzone, infector	http://whois.webnames.ru
2985.	becutie.ru	dropzone	https://www.nic.ru/whois
2986.	bellicbridge.ru	infector	https://client.naunet.ru/c/whoiscontact
2987.	bellicoreturbo.ru	infector	https://client.naunet.ru/c/whoiscontact
2988.	bestsoftics.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2989.	betternewyear.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
2990.	bigupdate.ru	infector	bigupdate.ru
2991.	bigupdater.ru	infector	http://whois.webnames.ru
2992.	bigupdaters.ru	dropzone, infector	http://whois.webnames.ru
2993.	bigupdates.ru	infector	http://whois.webnames.ru
2994.	bigupdating.ru	infector	http://whois.webnames.ru
2995.	bigupdatings.ru	dropzone, infector	http://whois.webnames.ru
2996.	bonaquadriga.ru	dropzone	https://client.naunet.ru/c/whoiscontact
2997.	boredret.ru	infector	https://client.naunet.ru/c/whoiscontact
2998.	boutique26.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
2999.	brainrace.ru	dropzone	http://www.reg.ru/whois/admin_contact
3000.	cakerecipes.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3001.	callmenowhere.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3002.	cekcuc.ru	dropzone, infector	http://www.reg.ru/whois/admin_contact
3003.	champiogogo.ru	infector	https://client.naunet.ru/c/whoiscontact
3004.	cherlend2.ru	infector	http://www.reg.ru/whois/admin_contact
3005.	chot-extreme.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3006.	cloudsaround.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3007.	cloudy-dns.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3008.	boredret.ru	source	https://client.naunet.ru/c/whoiscontact
3009.	zhremvkusno.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3010.	gulayemadolgo.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3011.	vodkavkusnaya.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3012.	pyemonnogo.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3013.	pivastemniy.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3014.	forelnamangale.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3015.	kupimbrabusik.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3016.	zubkichistim.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3017.	pyemsokifresh.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3018.	spimkreepko.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3019.	bezhimlegko.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3020.	clopsandsuits.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3021.	dishimgluboko.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3022.	yumorinacheap.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3023.	zhivemdooolgo.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3024.	poedemvpole.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3025.	odessaideribassi.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3026.	0dgt8xx.ru	dropzone	c/o Coordination Center for TLD RU
3027.	0gt5dx.ru	dropzone	c/o Coordination Center for TLD RU
3028.	0gt6dx.ru	dropzone	c/o Coordination Center for TLD RU
3029.	0gt7dx.ru	dropzone	c/o Coordination Center for TLD RU
3030.	1dgt8xx.ru	dropzone	c/o Coordination Center for TLD RU
3031.	2dgt8xx.ru	dropzone	c/o Coordination Center for TLD RU
3032.	izba4you.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3033.	registration120.ru	dropzone	c/o Coordination Center for TLD RU
3034.	registration1200.ru	dropzone	c/o Coordination Center for TLD RU
3035.	registration2300.ru	dropzone	c/o Coordination Center for TLD RU
3036.	registration400.ru	dropzone	c/o Coordination Center for TLD RU

3037.	registration4300.ru	dropzone	c/o Coordination Center for TLD RU
3038.	registration43450.ru	dropzone	c/o Coordination Center for TLD RU
3039.	registration43500.ru	dropzone	c/o Coordination Center for TLD RU
3040.	registration445.ru	dropzone	c/o Coordination Center for TLD RU
3041.	registration460.ru	dropzone	c/o Coordination Center for TLD RU
3042.	registration4768.ru	dropzone	c/o Coordination Center for TLD RU
3043.	registration500.ru	dropzone	c/o Coordination Center for TLD RU
3044.	registration600.ru	dropzone	c/o Coordination Center for TLD RU
3045.	registration700.ru	dropzone	c/o Coordination Center for TLD RU
3046.	registration800.ru	dropzone	c/o Coordination Center for TLD RU
3047.	registration900.ru	dropzone	c/o Coordination Center for TLD RU
3048.	majmun.su	dropzone, updater	admin@majmun.su
3049.	yгла.ru	dropzone	https://www.nic.ru/whois
3050.	needfortwomorebilliondollars.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3051.	ciscoc.ru	dropzone	https://cp.mastername.ru/domain_feedback/
3052.	dankin.ru	dropzone	https://cp.mastername.ru/domain_feedback/
3053.	gooddaystart.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3054.	getasamemilliondollars.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3055.	billiard-star.ru	dropzone	http://www.reg.ru/whois/admin_contact
3056.	koletrezzo44.ru	dropzone	http://www.reg.ru/whois/admin_contact
3057.	koletrezzo55.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3058.	koletrezzo66.ru	dropzone	c/o Coordination Center for TLD RU
3059.	koletrezzo77.ru	dropzone	c/o Coordination Center for TLD RU
3060.	onlinesourceget.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3061.	dkmsetchdwh-lcmntrhc.ru	dropzone	c/o Coordination Center for TLD RU
3062.	dkmsetchdwh-lcmntrhc1.ru	dropzone	c/o Coordination Center for TLD RU
3063.	remstwedber-keltbrzsemcd.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3064.	remstwedber-keltbrzsemcd1.ru	dropzone	c/o Coordination Center for TLD RU
3065.	sdemxhtruskdsh-wendtrhnzsefy.ru	dropzone	c/o Coordination Center for TLD RU
3066.	sdemxhtruskdsh-wendtrhnzsefy1.ru	dropzone	c/o Coordination Center for TLD RU
3067.	shdnherthxkdn-aldatednjfwsnc.ru	dropzone	c/o Coordination Center for TLD RU
3068.	shdnherthxkdn-aldatednjfwsnc1.ru	dropzone	c/o Coordination Center for TLD RU
3069.	happyfourfriends.ru	updater	c/o Coordination Center for TLD RU
3070.	hotfight.ru	dropzone	http://www.reg.ru/whois/admin_contact
3071.	irontea.ru	infector	http://www.reg.ru/whois/admin_contact
3072.	megahock.ru	updater	http://www.reg.ru/whois/admin_contact
3073.	nosyfan.ru	source	http://www.reg.ru/whois/admin_contact
3074.	yummyship.ru	updater	http://www.reg.ru/whois/admin_contact
3075.	dkmsetchdwh-lcmntrhc.ru	dropzone	c/o Coordination Center for TLD RU
3076.	dkmsetchdwh-lcmntrhc1.ru	dropzone	c/o Coordination Center for TLD RU
3077.	remstwedber-keltbrzsemcd.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3078.	remstwedber-keltbrzsemcd1.ru	dropzone	c/o Coordination Center for TLD RU
3079.	sdemxhtruskdsh-wendtrhnzsefy.ru	dropzone	c/o Coordination Center for TLD RU
3080.	sdemxhtruskdsh-wendtrhnzsefy1.ru	dropzone	c/o Coordination Center for TLD RU
3081.	shdnherthxkdn-aldatednjfwsnc.ru	dropzone	c/o Coordination Center for TLD RU
3082.	shdnherthxkdn-aldatednjfwsnc1.ru	dropzone	c/o Coordination Center for TLD RU
3083.	ahawualwbcnd-aewjdkasdk.ru	dropzone	c/o Coordination Center for TLD RU
3084.	andhersnmrtsh-sawahadnhsya.ru	dropzone	c/o Coordination Center for TLD RU
3085.	ctmsehbqlzth-wtnghapdnsmtrq.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3086.	shajshdthwnlkjas-erwqoabejad.ru	dropzone	c/o Coordination Center for TLD RU
3087.	sjahtewhandl-aldhiowhalndas.ru	dropzone	c/o Coordination Center for TLD RU
3088.	agedstuff.ru	updater	http://www.reg.ru/whois/admin_contact
3089.	emptyspa.ru	updater	http://www.reg.ru/whois/aadmi_contact

3090.	litfox.ru	source	http://www.reg.ru/whois/admin_contact
3091.	smartcheat.ru	infector	http://www.reg.ru/whois/admin_contact
3092.	splitflash.ru	dropzone	http://www.reg.ru/whois/admin_contact
3093.	steelstorm.su	dropzone, source, infector	william.hill146@hotmail.com
3094.	izba4you.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3095.	safetraffplace.ru	embedded_js	http://www.reg.ru/whois/admin_contact
3096.	sebezh.ru	dropzone	https://partner.r01.ru/contact_admin.khtml
3097.	arttkachev.ru	dropzone	http://www.reg.ru/whois/admin_contact
3098.	koletrezzo44.ru	dropzone	http://www.reg.ru/whois/admin_contact
3099.	koletrezzo55.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3100.	koletrezzo66.ru	dropzone	c/o Coordination Center for TLD RU
3101.	koletrezzo77.ru	dropzone	c/o Coordination Center for TLD RU
3102.	billiard-star.ru	dropzone	http://www.reg.ru/whois/admin_contact
3103.	arttkachev.ru	dropzone	http://www.reg.ru/whois/admin_contact
3104.	mega-zona.ru	dropzone	system@iphoster.ru
3105.	dishacid.ru	infector	http://www.reg.ru/whois/admin_contact
3106.	earthfile.ru	updater	http://www.reg.ru/whois/admin_contact
3107.	panbaby.ru	updater	http://www.reg.ru/whois/admin_contact
3108.	pighair.ru	dropzone	http://www.reg.ru/whois/admin_contact
3109.	vampkeys.ru	source	http://www.reg.ru/whois/admin_contact
3110.	billiard-star.ru	dropzone	http://www.reg.ru/whois/admin_contact
3111.	mega-zona.ru	dropzone	system@iphoster.ru
3112.	agedstuff.ru	updater	http://www.reg.ru/whois/admin_contact
3113.	deadpage.ru	infector	http://www.reg.ru/whois/admin_contact
3114.	mildruby.ru	dropzone	http://www.reg.ru/whois/admin_contact
3115.	piecerack.ru	updater	http://www.reg.ru/whois/admin_contact
3116.	stormhock.ru	source	http://www.reg.ru/whois/admin_contact
3117.	avforwarding.ru	dropzone, updater	http://registrant.ru/whois/form
3118.	dayan.ru	dropzone, updater	https://partner.r01.ru/contact_admin.khtml
3119.	mega-zona.ru	updater	system@iphoster.ru
3120.	angerlunch.ru	infector	http://www.reg.ru/whois/admin_contact
3121.	dealface.ru	dropzone	http://www.reg.ru/whois/admin_contact
3122.	tut-freesteam.tut.su	dropzone	domains@akavita.com
3123.	gannoover.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3124.	goreeotuma.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3125.	kaleidosskop.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3126.	komunizzm.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3127.	listriskevish.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3128.	optimizzm.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3129.	pereostanovka.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3130.	plan2000putina.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3131.	pravilozhizzni.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3132.	sheregessh.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3133.	stervyatniks.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3134.	swistertwister.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3135.	zadnjasansa.ru	dropzone	http://www.webdrive.ru/webmail/
3136.	jebote.demand.su	dropzone	demand.su@allperson.ru
3137.	mapusismiga.broke.su	dropzone	gzero@arrest.su
3138.	shop.broke.su	dropzone	gzero@arrest.su
3139.	avforwarding.ru	dropzone	http://registrant.ru/whois/form
3140.	mega-zona.ru	dropzone	system@iphoster.ru
3141.	clanquack.ru	updater	http://www.reg.ru/whois/admin_contact
3142.	laketulip.ru	updater	http://www.reg.ru/whois/admin_contact

3143.	viperheart.ru	dropzone	http://www.reg.ru/whois/admin_contact
3144.	watersod.ru	infector	http://www.reg.ru/whois/admin_contact
3145.	centralintelligenceagency.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3146.	msndctermrnd-sldnemrtchndmawlschnx.ru	dropzone	c/o Coordination Center for TLD RU
3147.	pkdnmtbczpldt-lsdetmcthnszbaas.ru	dropzone	c/o Coordination Center for TLD RU
3148.	rncswshdrkstbhl-srtmxbcchewskch.su	dropzone	admin@rncswshdrkstbhl-srtmxbcchewskch.su
3149.	tdsnmserebtbdehcnd-asrehanmedhtsn.ru	dropzone	c/o Coordination Center for TLD RU
3150.	cornlion.ru	updater	http://www.reg.ru/whois/admin_contact
3151.	linuxhour.ru	updater	http://www.reg.ru/whois/admin_contact
3152.	tunecamp.ru	updater	http://www.reg.ru/whois/admin_contact
3153.	tunepage.ru	source	http://www.reg.ru/whois/admin_contact
3154.	caserow.ru	dropzone	http://www.reg.ru/whois/admin_contact
3155.	edgefox.ru	infector	http://www.reg.ru/whois/admin_contact
3156.	angerlunch.ru	infector	http://www.reg.ru/whois/admin_contact
3157.	legcold.ru	source	http://www.reg.ru/whois/admin_contact
3158.	noseclan.ru	dropzone	http://www.reg.ru/whois/admin_contact
3159.	poleblame.ru	updater	http://www.reg.ru/whois/admin_contact
3160.	tiecorn.ru	updater	http://www.reg.ru/whois/admin_contact
3161.	moodgum.ru	updater	http://www.reg.ru/whois/admin_contact
3162.	pupwork.ru	dropzone	http://www.reg.ru/whois/admin_contact
3163.	taxescell.ru	updater	http://www.reg.ru/whois/admin_contact
3164.	edgefox.ru	infector	http://www.reg.ru/whois/admin_contact
3165.	globalnetworkingwebsitefordomainpurpose.ru	dropzone	c/o Coordination Center for TLD RU
3166.	keyforoperationinmaximumtendencyforofscurement.ru	dropzone	c/o Coordination Center for TLD RU
3167.	onlinezoneforchecknresultaboutmaintenance.ru	dropzone	c/o Coordination Center for TLD RU
3168.	planningforovertheglobesyncofexistencescenario.ru	dropzone	c/o Coordination Center for TLD RU
3169.	projectforinvertigationaboutintelligence.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3170.	projectforinvestigationaboutsubspecificintelligence.ru	dropzone	http://whois.webnames.ru
3171.	routearoundtheworlwidefordisbursement.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3172.	blingcar.ru	dropzone	http://www.reg.ru/whois/admin_contact
3173.	levischild.ru	updater	http://www.reg.ru/whois/admin_contact
3174.	balusizo.ru	dropzone, source, infector, updater	https://client.naunet.ru/c/whoiscontact
3175.	needears.ru	updater	http://www.reg.ru/whois/admin_contact
3176.	emibors.ru	updater	https://client.naunet.ru/c/whoiscontact
3177.	filesziso.ru	updater	https://client.naunet.ru/c/whoiscontact
3178.	newsearching.ru	updater	https://client.naunet.ru/c/whoiscontact
3179.	noisel.ru	updater	https://client.naunet.ru/c/whoiscontact
3180.	onlinetraids.ru	updater	https://client.naunet.ru/c/whoiscontact
3181.	rolabork.ru	updater	https://client.naunet.ru/c/whoiscontact
3182.	cakedoor.ru	source	http://www.reg.ru/whois/admin_contact
3183.	lidlip.ru	dropzone	http://www.reg.ru/whois/admin_contact
3184.	baedeequu.ru	source	http://www.reg.ru/whois/admin_contact
3185.	emivohngu.ru	updater	https://client.naunet.ru/c/whoiscontact
3186.	hubooyeew.ru	updater	https://client.naunet.ru/c/whoiscontact
3187.	joobieves.ru	dropzone	http://www.reg.ru/whois/admin_contact
3188.	zeahungee.ru	updater	https://client.naunet.ru/c/whoiscontact
3189.	brainrace.ru	dropzone	http://www.reg.ru/whois/admin_contact
3190.	chintoe.ru	source	http://www.reg.ru/whois/admin_contact
3191.	8jl.ru	dropzone, infector	https://client.naunet.ru/c/whoiscontact
3192.	9iy.ru	updater	https://client.naunet.ru/c/whoiscontact

3193.	brainrace.ru	dropzone	http://www.reg.ru/whois/admin_contact
3194.	levischild.ru	updater	http://www.reg.ru/whois/admin_contact
3195.	needears.ru	updater	http://www.reg.ru/whois/admin_contact
3196.	tablepack.ru	source	http://www.reg.ru/whois/admin_contact
3197.	vsemskazalpoka.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3198.	vsemskazalpoka0.ru	dropzone	c/o Coordination Center for TLD RU
3199.	vsemskazalpoka1.ru	dropzone	c/o Coordination Center for TLD RU
3200.	vsemskazalpoka2.ru	dropzone	c/o Coordination Center for TLD RU
3201.	vsemskazalpoka3.ru	dropzone	c/o Coordination Center for TLD RU
3202.	vsemskazalpoka4.ru	dropzone	c/o Coordination Center for TLD RU
3203.	vsemskazalpoka5.ru	dropzone	c/o Coordination Center for TLD RU
3204.	vsemskazalpoka6.ru	dropzone	c/o Coordination Center for TLD RU
3205.	vsemskazalpoka7.ru	dropzone	c/o Coordination Center for TLD RU
3206.	vsemskazalpoka8.ru	dropzone	c/o Coordination Center for TLD RU
3207.	vsemskazalpoka9.ru	dropzone	c/o Coordination Center for TLD RU
3208.	radarcourt.ru	source	http://www.reg.ru/whois/admin_contact
3209.	stuffpub.ru	dropzone	http://www.reg.ru/whois/admin_contact
3210.	0bq.ru	dropzone, infector	rake@isp-provider.ru
3211.	1digitalsmarkets.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3212.	atlantatoagofs.ru	infector, dropzone	https://client.naunet.ru/c/whoiscontact
3213.	atlantawadding.ru	dropzone	https://client.naunet.ru/c/whoiscontact
3214.	xoophafiel.ru		https://www.nic.ru/whois
3215.	eepeohothe.ru		https://client.naunet.ru/c/whoiscontact
3216.	nahwisoohch.ru		https://client.naunet.ru/c/whoiscontact
3217.	munaeghohz.ru		https://client.naunet.ru/c/whoiscontact
3218.	jupaizeuph.ru		https://client.naunet.ru/c/whoiscontact
3219.	tolbarqueries-google33.ru		https://www.nic.ru/whois
3220.	tolbarqueries-google35.ru		https://www.nic.ru/whois

Telecommunication Tokelau Corporation (Teletok)
Fenuafala
Fakaofa
Tokelau

Dot TK Limited
8 Berwick Street
London W1F 0PH
United Kingdom

	Harmful Botnet Domain Name	Type	Whois Email Address
3221.	makemoneyonline.tk	dropzone, infector	raykelly17@gmail.com
3222.	j3kxheldda.tk	updater	abuse@dot.tk
3223.	9998881.TK	dropzone	abuse@dot.tk
3224.	ARMNPLS.TK	dropzone	abuse@dot.tk
3225.	buunetfit.tk	dropzone	abuse@dot.tk
3226.	LODINGS.TK	dropzone	abuse@dot.tk
3227.	norwits.tk	dropzone	abuse@dot.tk
3228.	ntoort.tk	dropzone	abuse@dot.tk
3229.	windlonset.tk	dropzone	abuse@dot.tk
3230.	sderfytms-wcedmertpnspr.tk	dropzone	abuse@dot.tk
3231.	sderfytms-wcedmertpnspr1.tk	dropzone	abuse@dot.tk
3232.	sderfytms-wcedmertpnspr2.tk	dropzone	abuse@dot.tk
3233.	sderfytms-wcedmertpnspr3.tk	dropzone	abuse@dot.tk
3234.	sderfytms-wcedmertpnspr4.tk	dropzone	abuse@dot.tk
3235.	sderfytms-wcedmertpnspr5.tk	dropzone	abuse@dot.tk
3236.	sderfytms-wcedmertpnspr6.tk	dropzone	abuse@dot.tk
3237.	sderfytms-wcedmertpnspr7.tk	dropzone	abuse@dot.tk
3238.	sderfytms-wcedmertpnspr8.tk	dropzone	abuse@dot.tk
3239.	sderfytms-wcedmertpnspr9.tk	dropzone	abuse@dot.tk
3240.	vnlashop.tk	dropzone	abuse@dot.tk
3241.	ownnxwn2na.tk	updater	abuse@dot.tk
3242.	smk4mslnwxD1x81.tk	updater	abuse@dot.tk
3243.	j3kxhelddb.tk	updater	abuse@dot.tk
3244.	smhn44nclx.tk	updater	abuse@dot.tk
3245.	frmwm40dmh.tk	updater	abuse@dot.tk
3246.	nfp23nsmnv.tk	updater	abuse@dot.tk

Taiwan Network Information Center (TWNIC)
4F-2, No. 9, Roosevelt Road, Section 2
Taipei 100
Taiwan

	Harmful Botnet Domain Name	Type	Whois Email Address
3247.	microfreaks.com.tw	dropzone, infector	admin@microfreaks.com.tw
3248.	masterdominion.com.tw	dropzone, infector	admin@veryniceofyou.com.tw
3249.	freehost21.tw	dropzone, infector	hilarykneber@yahoo.com
3250.	foresttest218999fhjslk.com.tw	dropzone, infector	admin@foresttest218999fhjslk.com.tw
3251.	online-protection.tw	embedded_js	cafe@ppmail.ru
3252.	adminpaneltestasdf000444.com.tw	dropzone	admin@adminpaneltestasdf000444.com.tw
3253.	domainfortestingpanel999111.com.tw	infector	admin@domainfortestingpanel999111.com.tw
3254.	panelfretbbuiewnwdkhjg888333.com.tw	infector	admin@panelfretbbuiewnwdkhjg888333.com.tw
3255.	test444for555test333.com.tw	infector	admin@test444for555test333.com.tw
3256.	testeradminpanel222777.com.tw	dropzone, infector	admin@testeradminpanel222777.com.tw
3257.	testfhjtestpanel2226333.com.tw	dropzone	c/o Taiwan Network Information Center
3258.	testfortestltd444557.com.tw	dropzone, infector	admin@testfortestltd444557.com.tw
3259.	testing1testing2fhj3888222.com.tw	dropzone, infector	admin@testinglightversion999111.com.tw
3260.	testingdomainforfhj2220001.com.tw	infector	admin@testingdomainforfhj2220001.com.tw
3261.	testingforg00gle777245.com.tw	dropzone, infector	admin@testingforg00gle777245.com.tw
3262.	testingforinnovation2221999.com.tw	dropzone, infector	admin@testingforinnovation2221999.com.tw
3263.	testinglightversion999111.com.tw	dropzone, infector	admin@testinglightversion999111.com.tw
3264.	testonlyforfhj3355591.com.tw	dropzone, infector	admin@testonlyforfhj3355591.com.tw
3265.	testtestforfhj111998.com.tw	dropzone, infector	admin@testfortestltd444557.com.tw
3266.	testtestingpotatoes111222.com.tw	dropzone	admin@testtestingpotatoes111222.com.tw
3267.	testtexttost555888.com.tw	dropzone, infector	admin@testeradminpanel222777.com.tw

**ООО "Хостмастер"
04053, г. Киев, а/я 23
Украина**

**Hostmaster Ltd.
P.O.Box 89
Kiev-136, 04136
Ukraine**

	Harmful Botnet Domain Name	Type	Whois Email Address
3268.	exetsoft.org.ua	dropzone, infector	tgwq-uanic@priv.uanic.ua
3269.	buyakabuyaka.kiev.ua	infector, dropzone	tv187-uanic@priv.uanic.ua
3270.	rftnsbklebp-sndetzahcher.in.ua	dropzone	registry@ukrnames.com
3271.	rftnsbklebp-sndetzahcher0.in.ua	dropzone	c/o Hostmaster Ltd.
3272.	rftnsbklebp-sndetzahcher1.in.ua	dropzone	c/o Hostmaster Ltd.
3273.	rftnsbklebp-sndetzahcher2.in.ua	dropzone	c/o Hostmaster Ltd.
3274.	rftnsbklebp-sndetzahcher3.in.ua	dropzone	c/o Hostmaster Ltd.
3275.	rftnsbklebp-sndetzahcher4.in.ua	dropzone	c/o Hostmaster Ltd.
3276.	rftnsbklebp-sndetzahcher5.in.ua	dropzone	c/o Hostmaster Ltd.
3277.	rftnsbklebp-sndetzahcher6.in.ua	dropzone	c/o Hostmaster Ltd.
3278.	rftnsbklebp-sndetzahcher7.in.ua	dropzone	c/o Hostmaster Ltd.
3279.	rftnsbklebp-sndetzahcher8.in.ua	dropzone	c/o Hostmaster Ltd.
3280.	rftnsbklebp-sndetzahcher9.in.ua	dropzone	c/o Hostmaster Ltd.

**MNI Networks Ltd.
Olveston Drive
Olveston Salem
Montserrat
West Indies**

**Lubimal (MS) Ltd.
c/o Kelsick & Kelsick,
P.O. Box 185
Woodlands Road, Woodlands
Montserrat**

	Harmful Botnet Domain Name	Type	Whois Email Address
3281.	ownnxwn2na.ce.ms	updater	mgermann@key-systems.net
3282.	smk4mslnwa.ce.ms	updater	mgermann@key-systems.net
3283.	mt36dooxch.ce.ms	updater	mgermann@key-systems.net
3284.	oemx88dclo.ce.ms	updater	mgermann@key-systems.net
3285.	frmwm40dmh.ce.ms	updater	mgermann@key-systems.net
3286.	nfp23nsmnv.ce.ms	updater	mgermann@key-systems.net
3287.	smk4mslnwb.ce.ms	updater	mgermann@key-systems.net

SWITCH The Swiss Education & Research Network
Werdstrasse 2
Zurich CH-8004
Switzerland

Universitaet Liechtenstein
Fuerst-Franz-Josef-Strasse
Vaduz LI-9490
Liechtenstein

	Harmful Botnet Domain Name	Type	Whois Email Address
3288.	ownnxwn2na.c0m.li	updater	c/o SWITCH
3289.	smk4mslnwa.c0m.li	updater	c/o SWITCH
3290.	an50smsal2.c0m.li	updater	c/o SWITCH
3291.	j6sk5hmxkj.c0m.li	updater	c/o SWITCH
3292.	frmwm40dmh.c0m.li	updater	c/o SWITCH
3293.	nfp23nsmnv.c0m.li	updater	c/o SWITCH
3294.	dcfjctykdywrth.c0m.li	source	c/o SWITCH

Internet Verwaltungs-und Betriebsgesellschaft m.b.H.
Jakob-Haringer-Straße 8/V
5020 Salzburg
Austria

	Harmful Botnet Domain Name	Type	Whois Email Address
3295.	adv-service.at	embedded_js	milo@mailti.com
3296.	online-security.at	embedded_js	admin@online-security.at
3297.	additional-group.at	embedded_js	admin@additional-group.at
3298.	m-sservices.at	embedded_js	admin@additional-group.at
3299.	proto-service.at	embedded_js	iraqi@mail13.com
3300.	webhelper.at	embedded_js	admin@additional-group.at
3301.	optiker-gramm.at	infector	optiker.gramm@aon.at
3302.	rietzer-sk.at	infector	richard.kratzer@liebherr.com

DENIC eG
Kaiserstrasse 75-77
Frankfurt am Main 60329
Germany

	Harmful Botnet Domain Name	Type	Whois Email Address
3303.	seminarload.de	dropzone	hostmaster@serverkompetenz.de
3304.	ayjay.de	dropzone	info@all-inkl.com
3305.	sporcu.de	infector	hostmaster@serverkompetenz.de
3306.	tyou.de	infector	hostmaster@serverkompetenz.de

EURid vzw/asbl
Parkstation
Woluwelaan 150
Diegem Vlaams Brabant 1831
Belgium

	Harmful Botnet Domain Name	Type	Whois Email Address
3307.	infobbc.eu	embedded_js	domain.manager@publicdomainregistry.com
3308.	broker-vinea.eu	embedded_js	c/o EURid
3309.	sicherheit-schild.eu	embedded_js	c/o EURid
3310.	crime-club.eu	source	c/o EURid
3311.	sicherheit-schild.eu	embedded_js	c/o EURid
3312.	ymlo.eu	dropzone	c/o EURid
3313.	zaebiz.eu	dropzone, infector	tech@eurid.eu

DNS BE vzw/asbl
Ubicenter, Philipssite 5, bus 13
Leuven 3001
Belgium

	Harmful Botnet Domain Name	Type	Whois Email Address
3314.	bonfarto.be	source	hostmaster@one.com
3315.	servicespaypal.be	dropzone, infector	domeinen@hostnet.nl

**NeuStar, Inc.
21575 Ridgetop Circle
Sterling, VA 20166
United States**

**NeuStar, Inc.
Loudoun Tech Center
46000 Center Oak Plaza
Sterling Virginia 20166
United States**

**China Internet Network Information Center
4, South 4th Street, Zhongguancun,
Haidian district,
Beijing 100190, China**

	Harmful Botnet Domain Name	Type	Whois Email Address
3316.	fgbnutyfhfgjdfghjil.cn	dropzone	c/o NeuStar
3317.	trololololo.cn	dropzone	delicto@mail.ru
3318.	trololololo0.cn	dropzone	c/o NeuStar
3319.	trololololo1.cn	dropzone	c/o NeuStar
3320.	trololololo2.cn	dropzone	c/o NeuStar
3321.	trololololo3.cn	dropzone	c/o NeuStar
3322.	trololololo4.cn	dropzone	c/o NeuStar
3323.	trololololo5.cn	dropzone	c/o NeuStar
3324.	trololololo6.cn	dropzone	c/o NeuStar
3325.	trololololo7.cn	dropzone	c/o NeuStar
3326.	trololololo8.cn	dropzone	c/o NeuStar
3327.	trololololo9.cn	dropzone	c/o NeuStar

SIDN
PO Box 5022
6802 EA Arnhem
The Netherlands

SIDN
Meander 501
6825 MD Arnhem
The Netherlands

	Harmful Botnet Domain Name	Type	Whois Email Address
3328.	drankenservicestone.nl	dropzone	abuse@argeweb.nl
3329.	vakgararichtlijn.nl	dropzone	info@lapi.net
3330.	bijlesnederland.nl	dropzone	c/o SIDN
3331.	jennifermusic.nl	infector	c/o SIDN
3332.	schimmer-online.nl	dropzone	schimmer-online.nl
3333.	thunnissenexclusief.nl		keesvanduijn@thunnissenonderhoud.nl

Canadian Internet Registration Authority (CIRA)
350 Sparks Street
Suite 306
Ottawa Ontario K1R 7S8
Canada

	Harmful Botnet Domain Name	Type	Whois Email Address
3334.	americanmobile.ca	infector	c/o CIRA

**LA Registry Pte Ltd
89 Chelverton Road
London SW15 1RW**

**Lao National Internet Committee (LANIC)
Science Technology and Environment Agency
Prime Minister's Office
P. O. Box 2279
Vientiane Lao PDR
Lao People's Democratic Republic**

Harmful Botnet Domain Name	Type	Whois Email Address
3335. botcat.la	dropzone, infector	admin@alben.la

MARNet
Boulevard Partisan Set No.17
1000 Skopje
Macedonia

Булевар Партизански Одреди бр.17
1000 Скопје

Harmful Botnet Domain Name	Type	Whois Email Address
3336. 24fun.mk	dropzone, infector	c/o MARNet

**National Institute for R&D in Informatics
Bd. Averescu 8-10
Sector 1
Bucharest 011454
Romania**

	Harmful Botnet Domain Name	Type	Whois Email Address
3337.	buletindeprima.ro	infector	reposesseddomain@godaddy.com

Comite Gestor da Internet no Brasil
Av. das Nações Unidas, 11541, 7º andar
São Paulo SP 04578-000
Brazil

	Harmful Botnet Domain Name	Type	Whois Email Address
3338.	djpeterblue.com.br	dropzone, infector	c/o Comite Gestor da Internet no Brasil

Association of IT Companies of Kazakhstan
6/5 Kabanbai Batyra
Office 3
Astana AST 010000
Kazakhstan

	Harmful Botnet Domain Name	Type	Whois Email Address
3339.	duowork.kz	Infector	c/o Association of IT Companies of Kazakhstan
3340.	sox.kz	dropzone, infector	nikolai.vartanyan@mail.ru

**Institute for Research in Fundamental Sciences
 Shahid Bahonar (Niavaran) Square
 Tehran 1954851167
 Islamic Republic Of Iran**

	Harmful Botnet Domain Name	Type	Whois Email Address
3341.	e-exchanger.ir	dropzone, infector	jamcnutt111@hotmail.com
3342.	faint.ir	dropzone, infector	jamcnutt111@hotmail.com
3343.	fileservice.ir	dropzone, infector	jamcnutt111@hotmail.com
3344.	freshcomp.ir	dropzone, infector	jamcnutt111@hotmail.com
3345.	insane.ir	dropzone, infector	jamcnutt111@hotmail.com
3346.	iqservice.ir	dropzone, infector	jamcnutt111@hotmail.com
3347.	pochemuchka.ir	infector	jamcnutt111@hotmail.com

Information Systems Division, Isle of Man Government
St Andrew's House
Finch Road
Douglas Isle of Man IM1 3PX
United Kingdom

Domicilium (IoM) Ltd
Isle of Man Datacentre
Ronaldsway Isle of Man IM9 2RS
United Kingdom

	Harmful Botnet Domain Name	Type	Whois Email Address
3348.	forum4you.im	dropzone, infector	c/o Domicilium (IoM) Ltd
3349.	cc.im	dropzone, infector	c/o Domicilium (IoM) Ltd

Registro .it
Istituto di Informatica e Telematica del CNR
CNR - AREA DELLA RICERCA
Via Giuseppe Moruzzi, 1
I-56124 PISA
Italy

	Harmful Botnet Domain Name	Type	Whois Email Address
3350.	garati.it	dropzone, infector	Admin Contact: Ettore Loggia via Scala, 132 Fiumicino 00054 RM IT (no email)

GMO Registry, Inc.
26-1 Sakuragaokacho
Tokyo 150-8512
Japan

Harmful Botnet Domain Name	Type	Whois Email Address
3351. holdaslas.so	dropzone, infector	c/o GMO Registry, Inc.

.au Domain Administration (auDA)
114 Cardigan Street
Carlton VIC 3053
Australia

	Harmful Botnet Domain Name	Type	Whois Email Address
3352.	krhjfc.com.au	updater	whois.ausregistry.com.au
3353.	thestudiospace.com.au	dropzone, infector	c/o auDA

Autoriteti i Komunikimeve Elektronike dhe Postare - AKEP
Str. Reshit Collaku Nr. 43,
Tirana
Albania

Harmful Botnet Domain Name	Type	Whois Email Address
3354. hsbc.com.al	dropzone, infector	c/o AKEP

Research and Academic Computer Network - NASK
Wawozowa 18
Warsaw 02-796
Poland

	Harmful Botnet Domain Name	Type	Whois Email Address
3355.	kupie-dlugi.pl	dropzone, infector	c/o NASK

**Christmas Island Internet Administration Limited
Christmas Island Technology Centre (6RCI),
Nursery Road, Drumsite
Christmas Island Indian Ocean 6798
Christmas Island**

**CoCCA Registry Services (NZ) Limited
11a Wynyard Street
Devonport Auckland 0744
New Zealand**

Harmful Botnet Domain Name	Type	Whois Email Address
3356. syntaxhack.it.cx	dropzone, infector	gianluca@campanella.org

SWITCH The Swiss Education & Research Network
Werdstrasse 2
Zurich CH-8021
Switzerland

3357.	pinguini.ch	dropzone	c/o SWITCH
-------	-------------	----------	------------

EXHIBIT 3

Appendix B

	Harmful Botnet IP Address	Type	Hosting Company
1.	173.243.112.20	infector, source, dropzone	Continuum Data Centers LLC 835 Oak Creek Drive Lombard, IL 60148
2.	64.120.135.186	infector, source, dropzone	Burstnet Technologies, Inc. d/b/a Network Operations Center, Inc. 420-422 Prescott Ave Scranton, PA 18510

EXHIBIT 4

Appendix C

The following is a list of specific file paths or subdomains to be disabled. The general domain name may remain in operation. Only the specific file path or subdomains must be disabled.

	Harmful Botnet Web Address/File Path	Type	Whois Email Address
1.	http://maps.nexuizninja.com/check/free.php	dropzone	tyler@detrition.net
2.	http://lartery.netau.net/krrtyyer/qytret.php	dropzone	info@sprendimai.net
3.	http://sew.t1.com.ua/img/music/index5.php	dropzone	joel.mayer@t1systems.eu
4.	http://dineromode.dvrdns.org/morech/gate.php	dropzone	hostmaster@dyndns.com
5.	http://ircbot.blogdns.net/morech/gate.php	dropzone	hostmaster@dyndns.com
6.	http://raktobint.sytes.net:8080	dropzone	domains@no-ip.com
7.	http://paradoxfiles-ru.na.by/index5.php	dropzone	abuse@hetzner.de
8.	http://www.hans-dabringhausen.de/images/images-head/logo.php	dropzone	domainmaster@teamnet.de
9.	http://jade.nseasy.com/~manishar/7x19bd.html	source	sw.ns@minmaxgroup.com
10.	http://fb.servatusdev.com/~servdev/56iy2.html	source	tom.servatus@gmail.com
11.	http://costantinifoto.altervista.org/jxbqp8i/index.html	source	abuse_rs@altervista.it
12.	http://giacobbo.altervista.org/2q4cl1/index.html	source	abuse_rs@altervista.it
13.	http://costantinifoto.altervista.org/qia4cd/index.html	source	abuse_rs@altervista.it
14.	http://ecotechno.zzl.org/nx8il9/index.html	source	report@abuse.zymic.com
15.	http://ilfantoclub.altervista.org/9q8qcer/index.html	source	abuse_rs@altervista.it
16.	http://colloqui.altervista.org/psgt9uk/index.html	source	abuse_rs@altervista.it
17.	http://panchalsamaj.x10.bz/snhlcmee/index.html	source	support@x10hosting.com
18.	http://ip-184-168-92-68.ip.secureserver.net/gwot29s/index.html	source	dns@jomax.net
19.	http://paolamartelli.altervista.org/dva7hi/index.html	source	abuse_rs@altervista.it
20.	http://ssggratis.altervista.org/7i6rha/index.html	source	abuse_rs@altervista.it
21.	http://camgirlmsn.altervista.org/rmhjh5/index.html	source	abuse_rs@altervista.it
22.	http://avon.anyservers.com/~accur/q02pu9y/index.html	source	osmanski@ivhosting.com
23.	http://goldentouch.99k.org/xsjorzc/index.html	source	report@abuse.zymic.com
24.	http://ns1277.websitewelcome.com/~asoprest/z79gr2q/index.html	source	ntlfqyxhc@whoisprivacyprotect.com
25.	http://host1.hosting2000.org/~progen/inczcf/index.html	source	g.russo@hosting2000.it
26.	http://daedalus2solar.bplaced.net/u00c8qx/index.html	source	hostmaster@computino.de
27.	http://amonapolicalcio.altervista.org/wxvq7t/index.html	source	abuse_rs@altervista.it
28.	http://start1g.ovh.net/~leperilj/5nmuq6x/index.html	source	vicxc7yp05etsazcn5lr@m.o-w-o.info
29.	http://0331edc.netsolhost.com/akravs/index.html	source	nosupervisor@networksolutions.com
30.	http://ash.phpwebhosting.com/~maisel/js50098/index.html	source	domains@phpwebhosting.com
31.	http://malta.site5.com/~vividimp/20picb/index.html	source	domain.admin@site5.com
32.	http://wdbadboy2005mi.de.tl	source	support@webme.com
33.	http://lanuevaera.x10.mx/b9xow9f/index.html	source	netops@singlehop.com
34.	http://blacksite.xhost.ro/n2lzycc5/index.html	source	istoica@yahoo.com (historical)
35.	http://malta.site5.com/~vividimp/7dkxhme/index.html	source	domain.admin@site5.com
36.	http://ns1277.websitewelcome.com/~asoprest/h97pk1/index.html	source	ntlfqyxhc@whoisprivacyprotect.com
37.	http://cp05.digitalpacific.com.au/~austraqc/80s7nn/index.html	source	whois.ausregistry.com.au
38.	http://malta.site5.com/~vividimp/1ks74o/index.html	source	domain.admin@site5.com
39.	http://fly.nseasy.com/~kennelv1/m05mdl/index.html	source	sw.ns@minmaxgroup.com
40.	http://members.iinet.net.au/~maccadelic_new/ndb1nk1/index.html	source	whois.ausregistry.com.au

41.	http://www.web3.biz/index2.html	source	team@web3.ms
42.	http://qr.net/fmka	source	qr.gmbh@googlemail.com
43.	http://members.iinet.net.au/~dbw/0yeebn/index.html	source	whois.ausregistry.com.au
44.	http://tie.ly/ gaqccm	source	teknorhino@gmail.com
45.	http://shorl.com/hugarutigrami	source	filip@infix.se
46.	http://web3.biz/ep1jam/index.html	source	team@web3.ms
47.	http://host1.hosting2000.org/~progen/i86omy/index.html	source	g.russo@hosting2000.it
48.	http://host1.hosting2000.org/~progen/1tlx5h/index.html	source	g.russo@hosting2000.it
49.	http://s342953645.online.de/~thefastdesign/w7y9kh/index.html	source	hostmaster@lund1.de
50.	http://getfe1-statf11.serveirc.com/main.php?page=11750cdaf4bde6a7	source	domains@no-ip.com
51.	http://sysdev.clanteam.com/eisbcfc/index.html	source	jack@netcosolutions.com
52.	http://2.8a.5446.static.theplanet.com/~traveladmin/keq7nl/index.html	source	domains@softlayer.com
53.	http://eewqr12.servebeer.com/main.php?page=11750cdaf4bde6a7	source	domains@no-ip.com
54.	http://gent-filoz.serveirc.com/main.php?page=4749d799dd461ec7	source	domains@no-ip.com
55.	http://pass66.dizinc.com/~timbytec/nhdoum/index.html	source	webmaster@hostdime.com
56.	http://sweethome.serveirc.com/main.php?page=a4ad3cf3d5bd d384	source	domains@no-ip.com
57.	http://backlinks.99k.org/6fbcpq3/index.html	source	report@abuse.zymic.com
58.	http://s15419483.onlinehome-server.info/~bluemars/tz9aeu/index.html	source	hostmaster@lund1.de
59.	http://backlinks.99k.org/76oqhff/index.html	source	report@abuse.zymic.com
60.	http://badcompanyeredar.ba.ohost.de/gjx6wf0/index.html	source	n.buechner@unitedcolo.de
61.	http://s15419483.onlinehome-server.info/%7Ebuemars/8plo98x/index.html	source	hostmaster@lund1.de
62.	http://bookshop10.xhost.ro/gnhekx/index.html	source	istoica@yahoo.com (historical)
63.	http://badcompanyeredar.ba.ohost.de/qg8s8xe/index.html	source	n.buechner@unitedcolo.de
64.	http://bookshop10.xhost.ro/cvy7m5/index.html	source	domain-admin@listserv.rnc.ro (historical)
65.	http://fe.25.79ae.static.theplanet.com/~blindama/qzbnbc/index.html	source	domains@softlayer.com
66.	http://bumblebeeman.enixns.com/~bookmi/qcdskq/index.html	source	info@enixltd.com
67.	http://3e.2.79ae.static.theplanet.com/%7Ebizgolf/g45qnx/index.html	source	domains@softlayer.com
68.	http://badcompanyy.ba.ohost.de/tukono/index.html	source	n.buechner@unitedcolo.de
69.	http://3e.2.79ae.static.theplanet.com/~bizgolf/ggfqvqs/index.html	source	domains@softlayer.com
70.	http://bmw02.neostrada.pl/zfin.html	source	info@home.pl
71.	http://masterscomputer.altervista.org/l1f3rs/index.html	source	abuse_rs@altervista.it
72.	http://onlinenews.altervista.org/iw9u2rj.html	source	abuse_rs@altervista.it
73.	http://users100.lollipop.jp/~boy.jp-thonarafc/330u3m/index.html	source	jp@uumuu-domain.com
74.	http://gator1057.hostgator.com/~bmccrack/t7s0k9/index.html	source	support@hostgator.com
75.	http://snipr.com/2npp7n	source	privacy@dynadot.com
76.	http://snipr.com/2npircm	source	privacy@dynadot.com
77.	http://redir.ec/eGUJ	source	mail@nameaction.com
78.	http://a.md/9DT	source	admin@nocdirect.com
79.	http://gs.a.md/9Do	source	admin@nocdirect.com
80.	http://rftp.rf.ohost.de/47rdx21/index.html	source	n.buechner@unitedcolo.de
81.	http://pro.ovh.net/~ritreqiv/jdx9vv/index.html	source	vicxc7yp05etsazcn5lr@m.o-w-o.info
82.	http://chimera.lunarpages.com/~micro15/d9vsfi/index.html	source	domains@lunarpages.com

83.	http://qybo-hubybewu.freewebsitethosting.com/nonplatentiluu21.html	source	domains@netgears.com
84.	http://pdc.bplaced.net/ndiu0mw/index.html	source	xrmb2@chello.at
85.	http://wca8532g2.homepage.t-online.de/ylzvww/index.html	source	hostmaster@t-online.net
86.	http://gibubetelo.pochta.ru/meziqogu.html	source	https://cp.centrohost.ru/contact_admin.khtml
87.	http://pdc.bplaced.net/sj6cup/index.html	source	xrmb2@chello.at
88.	http://pchelpch.pc.ohost.de/2q7vwk/index.html	source	n.buechner@unitedcolo.de
89.	http://wca8532g2.homepage.t-online.de/zjs808b/index.html	source	hostmaster@t-online.net
90.	http://mariage.zxq.net/v6f8ij/index.html	source	report@abuse.zymic.com
91.	http://mattandtiera2011.zxq.net/67ejc/index.html	source	report@abuse.zymic.com
92.	http://90plan.ovh.net/~marocvud/hxegls/index.html	source	vicxc7yp05etsazcn5lr@m.o-w-o.info
93.	http://ryanandassoc.temppublish.com/s88pzpf/index.html	source	admin@dnsone.net
94.	http://TACITUS.lunariffic.com/~mecha7/sgf1nn/index.html	source	domains@lunarpages.com
95.	http://saxwksop2.freetcp.com/main.php?page=b123ee3176247430	source	nsi@changeip.com
96.	http://v008u07gar.maximumasp.com/v5k2jrh/index.html	source	joe.oesterling@cbeyond.net
97.	http://tacitus.lunariffic.com/~mecha7/t7dth1/index.html	source	domains@lunarpages.com
98.	http://pass73.dizinc.com/~rssdevil/7dzgmxg/index.html	source	webmaster@hostdime.com
99.	http://saxwksop2.freetcp.com/content/g43kb6j34kblq6jh34kb6j3kl4.jar	source	nsi@changeip.com
100.	http://pisxzxe.qpoe.com/main.php?page=b123ee3176247430	source	nsi@changeip.com
101.	http://cam0815.ca.ohost.de/ajaxam.js	source	n.buechner@unitedcolo.de
102.	http://noelg.host22.com/ajaxam.js	source	awex@hostprince.com
103.	http://safedownload.hopto.org/main.php?page=2cef279c7a3c10d2	source	domains@no-ip.com
104.	http://terstata.instanthq.com/main.php?page=3a23d8870733555a	source	nsi@changeip.com
105.	http://www.amigosdeloajeno.mihost.biz/ajaxam.js	source	dominios@arturoaparicio.com
106.	http://lookitup.webatu.com/ajaxam.js	source	awex@hostprince.com
107.	http://cirangel.net78.net/ajaxam.js	source	awex@hostprince.com
108.	http://gorecznik.home.pl/ajaxam.js	source	info@home.pl
109.	http://partnerid.ikwb.com/main.php?page=b123ee3176247430	source	nsi@changeip.com
110.	http://getmybit.servequake.com/main.php?page=01a64bf41125d37a	source	domains@no-ip.com
111.	http://domovnik.ic.cz/ajaxam.js	source	domeny@nodus.cz
112.	http://soltys.tym.cz/ajaxam.js	source	domeny@nodus.cz
113.	http://jeanpaulstocks.zxq.net/ajaxam.js	source	report@abuse.zymic.com
114.	http://nandtesystco.pochta.ru/ijomerem.html	source	https://cp.centrohost.ru/contact_admin.khtml
115.	http://philstrobi.bplaced.net/ajaxam.js	source	xrmb2@chello.at
116.	http://chattbook.pytalhost.com/ajaxam.js	source	webmaster@marjano.com
117.	http://staytuned.99k.org/ccounter.js	source	report@abuse.zymic.com
118.	http://sven89.bplaced.net/ajaxam.js	source	xrmb2@chello.at
119.	http://veldhuisen-media.woelmuis.nl/adsens.js	source	admin@nocdirect.com
120.	http://tbattitu.o2switch.net/ajaxam.js	source	support@o2switch.fr
121.	http://0058715.netsolhost.com/jjquery.js	source	nosupervisor@networksolutions.com
122.	http://therallyproductions.woelmuis.nl/ajaxam.js	source	abuse@leaseweb.com
123.	http://s207455068.online.de/adsens.js	source	hostmaster@1und1.de
124.	http://s388939403.mialojamiento.es/ajaxam.js	source	abuse@oneandone.net
125.	http://nutz.zzl.org/stcounter.js	source	report@abuse.zymic.com
126.	http://moneymaker.zymichost.com/jjquery.js	source	report@abuse.zymic.com
127.	http://downloadaddatafast.serveftp.com/main.php?page=db3408bf080473cf	source	domains@no-ip.com
128.	http://sownload.zapto.org/main.php?page=2cd37516bfc47eba	source	domains@no-ip.com

129.	http://loaddocsfast.servehttp.com/main.php?page=64078c3dc54bfa8a	source	domains@no-ip.com
130.	http://CN20090135.p-client.net/kquery.js	source	info@provider.nl
131.	http://chattbook.ch.funpic.de/kquery.js	source	n.buechner@unitedcolo.de
132.	http://czanna.webege.com/kquery.js	source	awex@hostprince.com
133.	http://ral2.ra.funpic.de/statcounter.js	source	n.buechner@unitedcolo.de
134.	http://tarracogoldfish.zxq.net/jqueri.js	source	report@abuse.zymic.com
135.	http://tbattitu.o2switch.net/statcounter.js	source	contact@gandi.net
136.	http://freefreefree.sytes.net/main.php?page=4a4fd3141d846cd	source	domains@no-ip.com
137.	http://bootle.servebeer.com/main.php?page=64078c3dc54bfa8a	source	domains@no-ip.com
138.	http://ftpstore.sytes.net/main.php?page=977334ca118fcb8c	source	domains@no-ip.com
139.	http://grankeysehteelisp3.hotbox.ru/urepemys.html	infector	https://cp.centrohost.ru/contact_admin.khtml
140.	http://pin.bissnes.net/1ei7lo/index.html	source	order@iphoster.ru
141.	http://ecommerce.nuvention-dev.org/76f4b3/index.html	source	whois@bluehost.com
142.	http://financeportal.sytes.net/main.php?page=111d937ec38dd17e	source	domains@no-ip.com
143.	http://migre.me/5ZTtq	source	jonnyken@gmail.com
144.	http://perbesuscsemeyzk42.pop3.ru/helazyj.html	infector	https://cp.centrohost.ru/contact_admin.khtml
145.	http://vs170173.vserver.de/r1d6pf.html	source	domains@domains.intergenia.de
146.	https://mlbtnnew555.cx.cc/mybt/hz/gate.php	dropzone	internetservice@gmx.com
147.	https://mlbtnnew888.cx.cc/mybt/hz/gate.php	dropzone	internetservice@gmx.com
148.	https://mlbtnnew111.cx.cc/mybt/hz/gate.php	dropzone	internetservice@gmx.com
149.	https://mltnnew222.cx.cc/mybt/hz/gate.php	dropzone	internetservice@gmx.com
150.	https://mltnnew333.cx.cc/mybt/hz/gate.php	dropzone	internetservice@gmx.com
151.	http://fff555.cx.cc/cpp/gate.php	dropzone	internetservice@gmx.com
152.	http://fff666.cx.cc/application/hthal5.php	dropzone	internetservice@gmx.com
153.	http://fff777.cx.cc/application2/hthal1.php	dropzone	internetservice@gmx.com
154.	http://tbyu657ib7k67iddro.cx.cc:8080/pic1s0fs.php	dropzone	internetservice@gmx.com
155.	http://asdfasdggghgsw.cx.cc/forum.php?tp=814e9f8081e083c2	dropzone	internetservice@gmx.com
156.	http://wergcrhvtyifupqasf.cx.cc/main.php?page=0b2d445ee4479ec7	dropzone	internetservice@gmx.com
157.	http://cdethstfrjhstfrjeadfrds.cx.cc/main.php?page=2eff3ec71fd39078	dropzone	internetservice@gmx.com
158.	http://nacha-rejected.cx.cc/main.php?page=ce862eccdc1e4cd6	dropzone	internetservice@gmx.com
159.	http://ach-rejected.cx.cc/main.php?page=ce862eccdc1e4cd6	dropzone	internetservice@gmx.com
160.	http://canceled-nacha.cx.cc/main.php?page=ce862eccdc1e4cd6	dropzone	internetservice@gmx.com
161.	http://nacha-reports.cx.cc/main.php?page=ce862eccdc1e4cd6	dropzone	internetservice@gmx.com
162.	http://nacha-details.cx.cc/main.php?page=ce862eccdc1e4cd6	dropzone	internetservice@gmx.com
163.	http://hgqkehgcvmvuqisdfkop.cx.cc/main.php?page=a85f6ff3ff9f5213	dropzone	internetservice@gmx.com
164.	http://irofojghqhyhurtjhnalsop.cx.cc/main.php?page=363cb076cf50e6a5	dropzone	internetservice@gmx.com
165.	http://hlqueghfkjhasdfcmfiaopdf.cx.cc/main.php?page=363cb076cf50e6a5	dropzone	internetservice@gmx.com
166.	http://dsfbgkjerqnjkelyhfger.cx.cc/main.php?page=19dcbf924e67dd7e	dropzone	internetservice@gmx.com
167.	http://mgrezlxnswkd-alsdsmcyrthsaqkdcu.cc/	dropzone	admin@cu.cc

168.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc0.cu.cc/	dropzone	admin@cu.cc
169.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc1.cu.cc/	dropzone	admin@cu.cc
170.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc2.cu.cc/	dropzone	admin@cu.cc
171.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc3.cu.cc/	dropzone	admin@cu.cc
172.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc4.cu.cc/	dropzone	admin@cu.cc
173.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc5.cu.cc/	dropzone	admin@cu.cc
174.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc6.cu.cc/	dropzone	admin@cu.cc
175.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc7.cu.cc/	dropzone	admin@cu.cc
176.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc8.cu.cc/	dropzone	admin@cu.cc
177.	http://mgrezlxnswkd-alsdsmcyrthsaqkdc9.cu.cc/	dropzone	admin@cu.cc
178.	http://xdcvygkiyipbkjmnds.cu.cc/forum.php?tp=861a283626b5fe6b	source	admin@cu.cc
179.	http://vpsuk.co.cc:53	dropzone	legal@co.cc
180.	http://0dgt8xx1.co.cc:443	dropzone	legal@co.cc
181.	http://1dgt8xx1.co.cc:443	dropzone	legal@co.cc
182.	http://2dgt8xx1.co.cc:443	dropzone	legal@co.cc
183.	http://jeronomkali23.co.cc/nomore123/gate.php	dropzone	legal@co.cc
184.	http://lupinaval123.co.cc/nomore123/gate.php	dropzone	legal@co.cc
185.	http://tendonina.co.cc/nomore12/gate.php	dropzone	legal@co.cc
186.	http://beshenklipt.co.cc/mulq/gate.php	dropzone	legal@co.cc
187.	http://hastlooksza.co.cc/mulq/gate.php	dropzone	legal@co.cc
188.	http://linnexmandq.co.cc/mulq/gate.php	dropzone	legal@co.cc
189.	http://mixmunelrtn.co.cc/mulq/gate.php	dropzone	legal@co.cc
190.	http://nrkloopres.co.cc/mulq/gate.php	dropzone	legal@co.cc
191.	http://pilermansox.co.cc/mulq/gate.php	dropzone	legal@co.cc
192.	http://chsparkos.co.cc:8080/pic1s0fs.php	dropzone	legal@co.cc
193.	http://uybkyukn78k67rvjyro.co.cc:8080/pic1s0fs.php	dropzone	legal@co.cc
194.	http://war9932rerew.co.cc:8080/pic1s0fs.php	dropzone	legal@co.cc
195.	http://vpsnl.co.cc/	dropzone	legal@co.cc
196.	http://vpsuk.co.cc/	dropzone	legal@co.cc
197.	http://redirlsonnapking.co.cc/bot.exe	infector	legal@co.cc
198.	http://redirrickagmentive.co.cc/redir.php	dropzone	legal@co.cc
199.	http://redirstregentedhosplings.co.cc/redir.php	dropzone	legal@co.cc
200.	http://vpsnl.co.cc/gate.php	dropzone	legal@co.cc
201.	http://vpsuk.co.cc/gate.php	dropzone	legal@co.cc
202.	http://fredxs12314.co.cc/point	dropzone	legal@co.cc
203.	http://fredxs12323.co.cc/point	dropzone	legal@co.cc
204.	http://fredxs12332.co.cc/point	dropzone	legal@co.cc
205.	http://fredxs12341.co.cc/point	dropzone	legal@co.cc
206.	http://fredxs12350.co.cc/point	dropzone	legal@co.cc
207.	http://pk123pk42er.co.cc:5788	dropzone	legal@co.cc
208.	http://pk124pk213er.co.cc:5788	dropzone	legal@co.cc
209.	http://pk125pk45er.co.cc:5788	dropzone	legal@co.cc
210.	http://pk126pk245er.co.cc:5788	dropzone	legal@co.cc
211.	http://hatefelony441.co.cc/config/bot.php	dropzone, source, infector	legal@co.cc
212.	http://1dgt8x612.co.cc:4443	dropzone	legal@co.cc
213.	http://2dgt84x13.co.cc:4443	dropzone	legal@co.cc
214.	http://3dgt82x14.co.cc:4443	dropzone	legal@co.cc
215.	http://jero2nim2kali23.co.cc/bern_gate/gate.php	dropzone	legal@co.cc
216.	http://lupi21nav3al123.co.cc/bern_gate/gate.php	dropzone	legal@co.cc
217.	http://tend4oninanos1.co.cc/bern_gate/gate.php	dropzone	legal@co.cc
218.	http://online-zona.co.cc/engine/on.php	dropzone	legal@co.cc

219.	http://thedarkzonechat.co.cc/community/images/index5.php	dropzone	legal@co.cc
220.	http://fredxs1231.co.cc/uugt/gate.php	dropzone	legal@co.cc
221.	http://fredxs1232.co.cc/uugt/gate.php	dropzone	legal@co.cc
222.	http://fredxs1233.co.cc/uugt/gate.php	dropzone	legal@co.cc
223.	http://fredxs1234.co.cc/uugt/gate.php	dropzone	legal@co.cc
224.	http://fredxs1235.co.cc/uugt/gate.php	dropzone	legal@co.cc
225.	http://fredxs1245.co.cc:3752	dropzone	legal@co.cc
226.	http://fredxs1246.co.cc:3752	dropzone	legal@co.cc
227.	http://fredxs1247.co.cc:3752	dropzone	legal@co.cc
228.	http://fredxs1248.co.cc:3752	dropzone	legal@co.cc
229.	http://fredxs1249.co.cc:3752	dropzone	legal@co.cc
230.	http://online-zona.co.cc/engine/next2.php	dropzone	legal@co.cc
231.	http://vpsuk.co.cc/_cp/gate.php	dropzone	legal@co.cc
232.	http://rajbhanse.co.cc/images/js.js	source	legal@co.cc
233.	http://rajbhanse.co.cc/js.js	source	legal@co.cc
234.	http://ttpp1.cz.cc/1/index.php	dropzone	dominique_piatti@hotmail.com
235.	http://bhood.cz.cc/spyeye/main/gate.php	dropzone	dominique_piatti@hotmail.com
236.	http://kzoklo.cz.cc/tr.php	dropzone	dominique_piatti@hotmail.com
237.	http://herrmonaglf.cz.cc/ern.php	dropzone	dominique_piatti@hotmail.com
238.	http://longerm.cz.cc/rr.php	dropzone	dominique_piatti@hotmail.com
239.	http://longernsen.cz.cc/rrr.php	dropzone	dominique_piatti@hotmail.com
240.	http://unifenmes.cz.cc/pis.php	dropzone	dominique_piatti@hotmail.com
241.	http://refg4thu56j7kfbnm.cz.cc:8080/pic1s0fs.php	dropzone	dominique_piatti@hotmail.com
242.	http://evells234858997.cz.cc/cpss/weaspp.php	dropzone	dominique_piatti@hotmail.com
243.	http://evells234858997.cz.cc:8080	dropzone	dominique_piatti@hotmail.com
244.	http://hostsolioo.cz.cc/cpss/webcred.php	dropzone	dominique_piatti@hotmail.com
245.	http://ldofoibuyas.cz.cc/forum.php?tp=8bcc822a05189962	source	dominique_piatti@hotmail.com
246.	http://nbhjbyatrsd.cz.cc/forum.php?tp=02be77593f350f96	source	dominique_piatti@hotmail.com
247.	http://dfufrghgasdf.cz.cc/forum.php?tp=90c8a53a07d5631d	source	dominique_piatti@hotmail.com
248.	http://eqrgbczbdgqer.cz.cc/index.php?tp=9d115d3281bf4214	source	dominique_piatti@hotmail.com
249.	http://dsgjhdfgath.cz.cc/forum.php?tp=ec13bb967384b4a6	source	dominique_piatti@hotmail.com
250.	http://sddghdskfjgir.cz.cc/forum.php?tp=ee2ef72f535564e9	source	dominique_piatti@hotmail.com
251.	http://bnhkdfgadfg.cz.cc/forum.php?tp=6998ca312c143687	source	dominique_piatti@hotmail.com
252.	http://jfgggggdhcvlhflu.cz.cc/main.php?page=2f692f98fde2d51e	source	dominique_piatti@hotmail.com
253.	http://dtfrsykdflofyluolpu.cz.cc/main.php?page=2f692f98fde2d51e	source	dominique_piatti@hotmail.com
254.	http://sghdyjhdtkyktrydfg.cz.cc/main.php?page=8ef63c2673c6f66a	source	dominique_piatti@hotmail.com
255.	http://cwrhryjjfdhsrsdfc.cz.cc/main.php?page=ad891989d1e4ae62	source	dominique_piatti@hotmail.com
256.	http://ajkbgbfajkdghsjkfadsfgdh.cz.cc/main.php?page=2ef5c8d245d84484	source	dominique_piatti@hotmail.com
257.	http://luggkbqwhetcvjsdfgqer.cz.cc/main.php?page=6ab9084ab99c9482	source	dominique_piatti@hotmail.com
258.	http://jfjfhfyhuqnbciper.cz.cc/main.php?page=46df6916c2a87d98	source	dominique_piatti@hotmail.com
259.	http://xwwwwhtryjqafvmjhjiouty.cz.cc/main.php?page=9647286421ee3fd6	source	dominique_piatti@hotmail.com
260.	360safeupdate02.gicp.net/360safe.bin	infector	yezi@oray.com
261.	360safeupdate02.gicp.net/360safe.php	dropzone	yezi@oray.com
262.	3apa3a.tomsk.tw/c/cfg.bin	infector	dm@ezar.ru
263.	3apa3a.tomsk.tw/web/gate.php	dropzone	dm@ezar.ru
264.	7system.ezua.com/cfg/config.php	infector	nsi@changeip.com

265.	alexej-borovickov.narod2.ru/black.bin	infector	https://www.nic.ru/whois
266.	alexej-borovickov.narod2.ru/white.bin	infector	https://www.nic.ru/whois
267.	http://asddsrtter.uni.me/led/config.php	updater	dominique_piatti@hotmail.com
268.	asia-euromillions.co.cc/iou/bot.exe	infector	legal@co.cc
269.	asia-euromillions.co.cc/iou/config.bin	infector	legal@co.cc
270.	asia-euromillions.co.cc/iou/gate.php	dropzone	legal@co.cc
271.	barugen.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
272.	barugen.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
273.	barugen.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
274.	berdonet2011.dlinkddns.com/z/ldr.ex	infector	jlai@dlink.com
275.	berdonet2011.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
276.	berdonet2011.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
277.	bionetlla.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
278.	bionetlla.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
279.	bionetlla.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
280.	drilng.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
281.	drilng.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
282.	drilng.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
283.	honestop20.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
284.	honestop20.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
285.	honestop20.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
286.	ivan-ivanovivanchenk.narod2.ru/black.bin	infector	https://www.nic.ru/whois
287.	ivan-ivanovivanchenk.narod2.ru/white.bin	infector	https://www.nic.ru/whois
288.	mpout.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
289.	mpout.dlinkddns.com/z/bot.exe	infector	jlai@dlink.com
290.	mpout.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
291.	mpout.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
292.	botnetdown.gicp.net/winupdateze.exe	infector	yezi@oray.com
293.	candy-models.co.cc/jobcfg/cfg.bin	infector	abuse@iana.org
294.	ccleanerwithsteak.co.cc/bot.exe	infector	abuse@iana.org
295.	ccleanerwithsteak.co.cc/config.bin	infector	abuse@iana.org
296.	ccleanerwithsteak.co.cc/gate.php	dropzone	abuse@iana.org
297.	choiodos.kodingen.com/tst/flower.ex	infector	domains@kodingen.com
298.	choiodos.kodingen.com/tst/config.bin	infector	domains@kodingen.com
299.	choiodos.kodingen.com/tst/lion.php	dropzone	domains@kodingen.com
300.	cooooolzz.zapto.org/local.exe	infector	domains@no-ip.com
301.	cooooolzz.zapto.org/zs.exe	infector	domains@no-ip.com
302.	cp101.sharkserve.com/cc/config.bin	infector	webmaster@sysmesh.com
303.	cp101.sharkserve.com/cc/gate.php	dropzone	webmaster@sysmesh.com
304.	dlugitarg1-10.home.pl/fo4.exe	infector	info@home.pl
305.	dns1.nsdnsrv.com/ssl.exe	infector	dfghrter@hotmail.com
306.	dns1.nsdnsrv.com/xml.php	dropzone	dfghrter@hotmail.com
307.	domainnameprovder.cz.cc/job2/shit.e	infector	dominique_piatti@hotmail.com
308.	domainnameprovder.cz.cc/job2/cfg.bin	infector	dominique_piatti@hotmail.com
309.	domainnameprovder.cz.cc/job2/exit.php	dropzone	dominique_piatti@hotmail.com
310.	domainsrecords.co.cc/job20/exit.php	dropzone	abuse@iana.org
311.	domainsrecords.co.cc/job3/exit.php	dropzone	abuse@iana.org
312.	eewqr12.servebeer.com/w.php?f=26&e=	infector	domains@no-ip.com
313.	funtime.arvixe.ru/imgs/bayy.exe	infector	http://whois.webnames.ru
314.	funtime.arvixe.ru/different_1/banner.tiff	infector	http://whois.webnames.ru
315.	funtime.arvixe.ru/different1/banner.tiff	infector	http://whois.webnames.ru

316.	funtime.arvixe.ru/myold/gate.php	dropzone ,	http://whois.webnames.ru
317.	gameslist.got-game.org/list.php	dropzone	nsi@changeip.com
318.	guiodertoll.dlinkddns.com/z/ldr.exe	infector	jlai@dlink.com
319.	guiodertoll.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
320.	guiodertoll.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
321.	h21211.srv7.test-hf.ru/bot.exe	infector	http://whois.webnames.ru
322.	h21211.srv7.test-hf.ru/config.bin	infector	http://whois.webnames.ru
323.	h21211.srv7.test-hf.ru/gate.php	dropzone	http://whois.webnames.ru
324.	hewj.ignorelist.com/backend/recycle.bin	infector	hostmaster@afraid.org
325.	hewj.ignorelist.com/backend/store.php	dropzone	hostmaster@afraid.org
326.	hewj.mooo.com/checkout/recycle.bin	infector	hostmaster@afraid.org
327.	hewj.mooo.com/backend/recycle.bin	infector	hostmaster@afraid.org
328.	hewj.mooo.com/backend/store.php	dropzone	hostmaster@afraid.org
329.	http://iasderwert.aaa.ai/led/config.php	updater	jeroen@kuiper.in
330.	iopyte.bget.ru/lol/pok.bin	infector	https://partner.r01.ru/contact admin.khtml
331.	iopyte.bget.ru/lol/loe.php	dropzone	https://partner.r01.ru/contact admin.khtml
332.	https://titolari.cartasi.it/portaleTitolari/js/ext/adapter/ext/ext-base.js	embedde d_js	angelo_dandrea@cartasi.it
333.	kabertempo.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
334.	kabertempo.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
335.	koukou.mine.nu/zadmin/bot.exe	infector	hostmaster@dyndns.com
336.	koukou.mine.nu/zadmin/config.bin	infector	hostmaster@dyndns.com
337.	koukou.mine.nu/zadmin/gate.php	dropzone	hostmaster@dyndns.com
338.	marciuxtest.co.cc/job3/shit.exe	infector	abuse@iana.org
339.	marciuxtest.co.cc/jobcfg3/cfg.bin	infector	abuse@iana.org
340.	marciuxtest.co.cc/job3/exit.php	dropzone	abuse@iana.org
341.	mibolyri.pisem.su/profi.bin	infector	manager-pochta@relax.ru
342.	microsofto.sytes.net/web/config.bin	infector	domains@no-ip.com
343.	microsofto.sytes.net/web/gate.php	dropzone	domains@no-ip.com
344.	mz.u-gu.ru/vktbot.exe	infector	https://www.nic.ru/whois
345.	mz.u-gu.ru/config.bin	infector	https://www.nic.ru/whois
346.	mz.u-gu.ru/gate.php	dropzone	https://www.nic.ru/whois
347.	ohfansub.instantfreesite.com/game.e	infector	edc5e8a9ec3d4dfa944d63e1c803c3aa.protect@whoisguard.com
348.	ohfansub.instantfreesite.com/update.bin	infector	edc5e8a9ec3d4dfa944d63e1c803c3aa.protect@whoisguard.com
349.	ohfansub.instantfreesite.com/gate.php	dropzone	edc5e8a9ec3d4dfa944d63e1c803c3aa.protect@whoisguard.com
350.	retomend.dlinkddns.com/z/cfg.bin	infector	jlai@dlink.com
351.	retomend.dlinkddns.com/z/gate.php	dropzone	jlai@dlink.com
352.	s130662.gridserver.com/zeus/config.bin	infector	mtdomains@mediatemple.net
353.	sc00d.webatu.com/00/cfg.bin	infector	awex@hostprince.com
354.	sc00d.webatu.com/00/gate.php	dropzone	awex@hostprince.com
355.	serlene.serveblog.net/move/config.bin	infector	domains@no-ip.com
356.	serlene.serveblog.net/checkout/recycle.bin	infector	domains@no-ip.com
357.	serlene.zapto.org/checkout/recycle.bin	infector	domains@no-ip.com
358.	serlene.zapto.org/move/config.bin	infector	domains@no-ip.com
359.	darkoansestg.zapto.org/efz8srnm/saberry.php	dropzone	domains@no-ip.com
360.	serva4ok.server2.eu/l0v3/cfg_z3u5.bin	infector	eurid@websuche.de
361.	serva4ok.server2.eu/l0v3/g4t3_z3u5.php	dropzone	eurid@websuche.de

362.	ssss.everywebspace.com/ZEUS/config.bin	infector	contact@myprivateregistration.com
363.	ssss.everywebspace.com/ZEUS/gate.php	dropzone	contact@myprivateregistration.com
364.	statserver.admin163biz.ru/statistics/optio	infector	http://www.webdrive.ru/webmail/
365.	statserver.admin163biz.ru/statistics/admin/statme.php	dropzone	http://www.webdrive.ru/webmail/
366.	thelookaround.net.atservers.net/temp/tmp/gate.php	dropzone	oleg@active.by
367.	tr.hyundaiita.com/w.php?f=16&e=0	infector	hyundaiita.com@domainsbyproxy.com
368.	troj.zx9.de/config.bin	infector	info@websuche.de
369.	troj.zx9.de/gate.php	dropzone	info@websuche.de
370.	vdugu39.co.cc/images/logo2.cdr	infector	abuse@iana.org
371.	vdugu39.co.cc/images/banner.php	dropzone	abuse@iana.org
372.	vitia-bolotin.narod2.ru/black.bin	infector	https://www.nic.ru/whois (historical)
373.	vitia-bolotin.narod2.ru/white.bin	infector	https://www.nic.ru/whois (historical)
374.	wisework.orge.pl/adminka/gate.php	dropzone , infector	pomoc@ovh.pl
375.	woodyalternative.ns1.name/zs/wgate.php	dropzone	pomoc@ovh.pl
376.	woodyalternative2.ns1.name/zs/woody.bin	infector	support@changeip.com
377.	zxz666.darktech.org/zeus/gate.php	dropzone , infector	leviathan@darktech.org
378.	zxz666.myftp.org/zeus/builder/bot.e	infector	domains@no-ip.com
379.	zxz666.myftp.org/zeus/builder/cfg2.bin	infector	domains@no-ip.com
380.	zxz666.myftp.org/zeus/gate.php	dropzone	domains@no-ip.com
381.	lindenbolle.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
382.	longehinter.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
383.	lresterlonhs.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
384.	mikalongesti.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
385.	mingerman.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
386.	rupertnn.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
387.	windernmvz.cjb.net/mind/index.php	dropzone	cjb@cjbmanagement.com
388.	media.e1s2.net	embedde d_js	donaldsemrau@yahoo.com
389.	roncbag.cz.cc	source	dominique_piatti@hotmail.com
390.	fisixjhia.co.be	source	hostmaster@eurodns.com
391.	mnuyspe.co.be	source	hostmaster@eurodns.com
392.	sammy.dommel.be	source	support@dommel.com
393.	3apa3a.tomsk.tw	infector, dropzone	dm@ezar.ru
394.	7system.ezua.com	infector	nsi@changeip.com
395.	isdfsrttyqza.biz.tm	updater	hostmaster@afraid.org
396.	isdfsrttyqza.c0m.li	updater	domein@kuiper.in
397.	moporikolis.bee.pl	dropzone , infector	domeny@consultingservice.pl
398.	toloveornottolove.ipq.co	infector	john@johnleach.co.uk
399.	adgga.co.cc	source	legal@co.cc
400.	shop.solution-networks.de	dropzone	info@x2-network.de
401.	asia-euromillions.co.cc	infector, dropzone	legal@co.cc
402.	polusuk.co.cc/best/bbbb.exe	source	legal@co.cc

EXHIBIT 5

Advertisement



[Subscribe to RSS](#)



[Follow me on Twitter](#)



[Join me on Facebook](#)

Krebs on Security

In-depth security news and investigation



[About the Author](#)

[About this Blog](#)

SpyEye v. ZeuS Rivalry Ends in Quiet Merger

160 tweets Leading malware developers within the cyber crime community have conspired to terminate development of the infamous **ZeuS banking Trojan** and to merge its code base with that of the up-and-coming **SpyEye Trojan**, new evidence suggests. The move appears to be aimed at building a superior e-banking threat whose sale is restricted to a more exclusive and well-heeled breed of cyber crook.

retweet

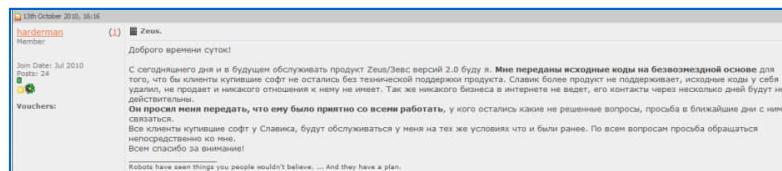
Underground forums are abuzz with rumors that the ZeuS author — a Russian hacker variously known by the monikers “Slavik” and “Monstr” — is no longer planning to maintain the original commercial crimeware kit.

According to numerous hacker forums, the source code for ZeuS recently was transferred to the developer of the **SpyEye Trojan**, a rival malware maker who drew attention to himself by dubbing his creation the “ZeuS Killer.” The upstart banking Trojan author constantly claimed that his bot creation kit bested ZeuS in functionality and form (SpyEye made headlines this year when investigators discovered it automatically searched for and removed ZeuS from infected PCs before installing itself).

In an era when it has become a truism to say that malicious hackers seek riches over renown, the SpyEye author — a coder known as either “Harderman” and “Gribodemon” on different forums — appears to have sought both, boasting on numerous forums about the greatness of his malware, using flashy logos to promote it (see below), and [granting an interview](#) with security researchers about the riches it will bring him. Although the ZeuS author chose to license his botnet creation kit to private groups through multiple intermediaries, the SpyEye creator has peddled his kit directly to buyers via online forums and instant messages.

Hack the Planet!

But — very recently — the public rivalry died down, and forum members on different sites where Harderman maintained a presence began complaining that they could no longer reach him for support issues. In an Oct. 11 message to one of the UnderWeb’s most exclusive hacker forums, Harderman can be seen breaking the news to fellow forum members. A screen shot of that message is below, followed by a translated version of it:



Good day!

I will service the Zeus product beginning today and from here on. I have been given the source codes free of charge so that clients who bought the software are not left without tech support. Slavik doesn't support the product anymore, he removed the source code from his [computer], he doesn't sell [it], and has no relationship to it. He also doesn't conduct any business on the Internet and in a few days his contact [information] will not be active.

He asked me to pass on that he was happy to work with everyone. If you have any unresolved issues remaining [there is a] request to get in touch with him as soon as possible.

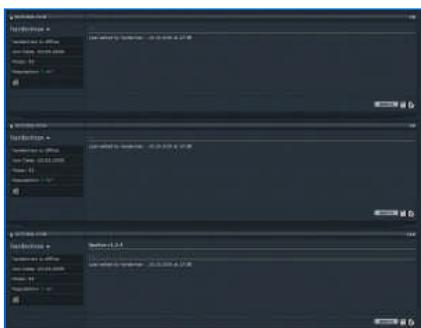
All clients who bought the software from Slavik will be serviced from me on the same conditions as previously. [I] request that [you] come directly to me regarding all issues.

Thanks to everyone for [your] attention!

In another conversation, Harderman says existing ZeuS clients will get a 30 percent discount on SpyEye, and that the two malware families will soon be “merged into one powerful Trojan.”



At the same time, Harderman has been busy changing his nicknames and contact information, and asking various online crime forum administrators to remove many of his previous posts about SpyEye, such as the deletions seen in the screen shots to right and below, taken from two different hacker forums.



Experts say all this commotion about ZeuS is natural and unsurprising, and that even criminal economies have market corrections — usually aimed at distancing the herd from threats that manage to make front page headlines. The planned assimilation of ZeuS coincides with a massive [international law enforcement push to arrest a number of individuals](#) responsible for using Zeus in hundreds of high-dollar e-banking heists from U.S. and U.K. businesses. The FBI says the password-stealing ZeuS Trojan played a central role in enabling the theft of more than [\\$70 million from nearly 400 organizations](#) in the United States over the last several years.

Steve Santorelli, director of global outreach for [Team Cymru](#), an organization that monitors underground economy activity, said his group has been predicting this change for months now.

"Each time you have a group or piece of malware that starts to get near the level of heat or public attention that ZeuS has gotten over the past year, it's inevitable that the bad guys are going to transition to something that's not on everyone's radar," Santorelli said.

Security firm **Trusteer** has warned that the recent industry focus on Zeus is making it easier for other Trojans, like [Bugat](#), SpyEye, and [Carberp](#), which are less wide spread but equally sophisticated, to avoid detection.

"We are in an arms race with criminals," said Trusteer CEO **Mickey Boodaei**. "Although Zeus gets a lot of attention from law enforcement, banks and the security industry, we need to be vigilant against new forms of financial malware like Bugat and SpyEye which are just as deadly and quietly expanding their footprint across the internet."

In response to urging from other members on the exclusive forum who apparently want fewer hackers to be able to afford the kit, Harderman acknowledges that he may have to dramatically increase — perhaps even double — the price of SpyEye, to several thousand dollars per license.

In exchange, the malware developer says he will overhaul the kit to include the best of both ZeuS and SpyEye. Specifically, Harderman says he wants to turn the guts of the Trojan into a [rootkit](#), and to build additional functionality on top, in the form of modular plug-ins. “We have a bunch of work on the way!” he promises in one online posting.

Interested buyers can probably expect the amalgamated software to contain some undocumented features. One of the more fascinating threads that survived the recent Harderman posting purge on the web forums comes from the Russian language board “DamageLab.org”, which [chronicles an incident](#) earlier this year in which fellow hackers managed to “crack” the technology the author uses to prevent SpyEye buyers from making unauthorized copies of the software.

Using the handle Gribodemon here, the software developer scoffed, saying he had secretly built in a backdoor that would allow him to seize remote control over PCs infected with his bot. "Ah, yes. I forgot to mention that in the 'leaked' version there is still a backdoor which I have now activated," Gribodemon wrote. "Thank you, rogue, for the completion of my botnet."



EXHIBIT 6

[Home](#) [Forum](#) [Research Articles](#) [What's New?](#) [Store](#)
[Today's Posts](#) [FAQ](#) [Calendar](#) [Community](#) [Forum Actions](#) [Quick Links](#)

Quick search

Member login
 User Name Password

[Register](#)

[Home](#) **Forum** [Malware](#) [Malware Samples and Information](#) Should i post ZeuS 2.0.8.9?

Join our official IRC! irc.datawhore.net #opencsc

All members should check OpenSC Password Policy under OpenSC - News

Hi Unregistered, check out our new rules in <http://www.opencsc.ws/opencsc-rules/>

Check our new page and feed your brain: <http://www.opencsc.ws/research/>

[+ Reply to Thread](#)

Results 1 to 10 of 23 [Page 1 of 3](#) [1](#) [2](#) [3](#) [»](#) [Last](#)

Thread: Should i post ZeuS 2.0.8.9?

3 Likes

[LinkBack](#) [Thread Tools](#) [Display](#)

08-04-2011

#1

nyu

Member



Join Date: Aug 2009

Posts: 84

Should i post ZeuS 2.0.8.9?

Or are banking bots still banned.

[Reply With Quote](#)

08-04-2011

#2

Mindfreak

Night's Watch



Join Date: Apr 2010

Location: Germany

Posts: 652

Originally Posted by nyu

Or are banking bots still banned.

Banking bots are still banned. ~~ and its not the latest ;D i saw 2.1.0.1 two days ago , but it has been removed ...

[Reply With Quote](#)

08-04-2011

#3

Erik_v4

Senior Member



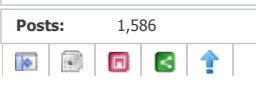
Join Date: Jun 2010

Location: Jordan

Posts: 171

u can post if u post the source with it



	Reply With Quote
08-04-2011	#4
<p>nyu ◎ Member  Join Date: Aug 2009 Posts: 84</p>	<p>Originally Posted by Mindfreak » <i>Banking bots are still banned. ~~ and its not the latest ;D i saw 2.1.0.1 two days ago , but it has been removed ...</i></p> <p>Is 2.1.0.1 even real? i thought 2.0.8.9 was the final before slavik handed over the src.</p>
	Reply With Quote
08-04-2011	#5
<p>kubano ◎ Senior Member  Join Date: Jul 2010 Location: OSC Server HDD Posts: 1,626</p>	<p>yes kids are waiting to do big heck</p> <p>1337 hax0r 3 .- likes this.</p> <p>Only GOD can judge me. its not about where you code , is all about HOW u code.</p>
	Reply With Quote
08-04-2011	#6
<p>nasGeneration! ◎ Senior Member  Join Date: May 2010 Location: #root Posts: 170</p>	<p>Originally Posted by nyu » <i>Or are banking bots still banned.</i></p> <p>Do you got the Source ?</p>
	Reply With Quote
08-04-2011	#7
<p>anti-tgou3ir ◎ Junior Member  Join Date: Mar 2011 Posts: 23</p>	just put
	Reply With Quote
08-04-2011	#8
<p>Retired boss ◎ Retired  Join Date: Mar 1998 Posts: 1,586</p>	<p>Originally Posted by Mindfreak » <i>Banking bots are still banned. ~~ and its not the latest ;D i saw 2.1.0.1 two days ago , but it has been removed ...</i></p>



2.0.8.9 is latest as neither monstr or grib0 updated it after that, 2.1.0.1 was just 2.0.8.9 created by someone that learned how to use a compiler

[Reply With Quote](#)

08-04-2011

#9

Mindfreak ◦

Night's Watch



Originally Posted by **black_rabbit**

2.0.8.9 is latest as neither monstr or grib0 updated it after that, 2.1.0.1 was just 2.0.8.9 created by someone that learned how to use a compiler

ah haven't know..
And whats the difference ?

Join Date:	Apr 2010
Location:	Germany
Posts:	652

Last edited by Mindfreak; 08-04-2011 at 18:42.

[Reply With Quote](#)

08-04-2011

#10

kari ◦

Banned

Join Date:	Jul 2009
Posts:	275

dont ask him for the difference he dont know shit

[Reply With Quote](#)

[+ Reply to Thread](#)

Page 1 of 3 [1](#) [2](#) [3](#) [»](#) [Last](#) [»](#)

[« Previous Thread](#) | [Next Thread »](#)

Thread Information

There are currently 1 users browsing this thread. (0 members and 1 guests)

Similar Threads

[\(\\$\) Post your items \(\\$\)](#) Replies: 95
By Luca in forum Off-Topic

Last Post: 12-11-2011, 04:08

[First post](#) Replies: 10
By strspeed in forum Off-Topic

Last Post: 14-02-2011, 01:45

[POST UR CHIPZ](#) Replies: 3
By aoi in forum Off-Topic

Last Post: 01-06-2010, 01:21

[where do i post requests?](#) Replies: 1
By 1337 hax0r 3 .- in forum Delphi Help

Last Post: 04-05-2010, 19:23

[ISTEALERS ANYONE CAN POST IT;D](#) Replies: 4
By abousakr in forum Malware Discussion and General Help

Last Post: 27-05-2009, 18:52

Posting Permissions

You may not post new threads
You may not post replies
You may not post attachments
You may not edit your posts

BB code is On
Smilies are On
[IMG] code is On
HTML code is Off
Trackbacks are On

Pingbacks are On
Refbacks are On

Forum Rules



[Contact Us](#)

[OpenSC](#)

[Top](#)

[Back to top](#)

All times are GMT +1. The time now is 01:11.

www.opensc.ws

Copyright ©2005 - 2012, OpenSC Forums

Search Engine Friendly URLs by vBSEO 3.6.0 ©2011, Crawlability, Inc.




[Home](#) [Forum](#) [Research Articles](#) [What's New?](#) [Store](#)
[Today's Posts](#) [FAQ](#) [Calendar](#) [Community](#) [Forum Actions](#) [Quick Links](#)

Quick search

Member login



User Name

Password

Register


[Home](#) [Forum](#) [Malware](#) [Malware Samples and Information](#) Should i post ZeuS 2.0.8.9?

Join our official IRC! irc.datawhore.net #opencsc

All members should check OpenSC Password Policy under OpenSC - News

Hi Unregistered, check out our new rules in <http://www.opencsc.ws/opencsc-rules/>Check our new page and feed your brain: <http://www.opencsc.ws/research/>[+ Reply to Thread](#)

Results 11 to 20 of 23

[Page 2 of 3](#)[«First](#)[◀](#)[1](#)[2](#)[3](#)[▶](#)[Last »](#)**Thread: Should i post ZeuS 2.0.8.9?**
[LinkBack](#) [Thread Tools](#) [Display](#)

08-04-2011

#11

nyu

Member

**Join Date:** Aug 2009**Posts:** 84Originally Posted by **kubanezi**

yes kids are waiting to do big heck

But if it isn't leaked how will all my HF friends heck banks and cvv?

[Reply With Quote](#)

08-04-2011

#12

nyu

Member

**Join Date:** Aug 2009**Posts:** 84Originally Posted by **Mindfreak** ah haven't know..
And what's the difference ?

2.1.0.1 just has modules

[Reply With Quote](#)

08-04-2011

#13

kubano

Senior Member

**Join Date:** Jul 2010**Location:** OSC Server HDD**Posts:** 1,626Originally Posted by **nyu**

But if it isn't leaked how will all my HF friends heck banks and cvv?

they use rapzo logger codet in .net very similar to zesus



Only GOD can judge me.
its not about where you code
, is all about HOW u code.

[Reply With Quote](#)

08-04-2011

#14

xpaulx ◊

Senior Member

**Join Date:** Dec 2010**Posts:** 262

the "2.1.0.1" has vnc bc and some other features enabled while the leaked 2.0.8.9 from a few weeks ago doesn't.

Last edited by xpaulx; 08-04-2011 at 20:57.

Meine Ehre heisst Treue

"Botnet's are like penis's it's not always about how big it is... it's about how you use it.. Be smart." -0x304

[Reply With Quote](#)

08-04-2011

#15

Retired boss ◊

Retired

**Join Date:** Mar 1998**Posts:** 1,586 Originally Posted by **Mindfreak** □

*ah haven't know..
And whats the difference ?*

new version number

1337 hax0r 3 .- likes this.

[Reply With Quote](#)

08-04-2011

#16

Retired boss ◊

Retired

**Join Date:** Mar 1998**Posts:** 1,586 Originally Posted by **xpaulx** □

the "2.1.0.1" has vnc bc and some other features enabled while the leaked 2.0.8.9 from a few weeks ago doesn't.

the leaked source does have all the modules

offtopic:

it's so nice to see *"This message is hidden because kari is on your ignore list."* whenever kari makes a post because you know it's irrelevant to the topic and it saves you a few seconds from reading it, y'all should try it

Last edited by Retired boss; 08-04-2011 at 22:43.

1337 hax0r 3 .- likes this.

[Reply With Quote](#)

08-04-2011

#17

hecks ◊

Member

 Originally Posted by **black_rabbit** □

Join Date:	Jan 2011
Posts:	89

it's so nice to see "This message is hidden because kari is on your ignore list." whenever kari makes a post because you know it's irrelevant to the topic and it saves you a few seconds from reading it, y'all should try it

"dont ask him for the difference he dont know shit"

[Reply With Quote](#)

08-04-2011

#18

Novakane ◎

Junior Member



Join Date:	Apr 2011
Posts:	11

post it with the sc

[Reply With Quote](#)

08-04-2011

#19

nyu ◎

Member



Join Date:	Aug 2009
Posts:	84

Selling zeus full source for \$100k.

[Reply With Quote](#)

08-04-2011

#20

kubano ◎

Senior Member



Join Date:	Jul 2010
Location:	OSC Server HDD
Posts:	1,626

Originally Posted by nyu

Selling zeus full source for \$100k.

<http://www.mediafire.com/?dwgww6it5hb4teo>
here is free
leaked [here](#)

Only GOD can judge me.
its not about where you code
, is all about HOW u code.

[Reply With Quote](#)

[+ Reply to Thread](#)

Page 2 of 3 | [« First](#) | [◀](#) | [1](#) | [2](#) | [3](#) | [▶](#) | [Last ▶](#)

[« Previous Thread](#) | [Next Thread »](#)

Thread Information

There are currently 1 users browsing this thread. (0 members and 1 guests)



Similar Threads

(\$) Post your items (\$)	Replies: 95 Last Post: 12-11-2011, 04:08
By Luca in forum Off-Topic	
First post	Replies: 10 Last Post: 14-02-2011, 01:45
By strspeed in forum Off-Topic	
POST UR CHIPZ	Replies: 3 Last Post: 01-06-2010, 01:21
By aoi in forum Off-Topic	
where do i post requests?	Replies: 1 Last Post: 04-05-2010, 19:23
By 1337 hax0r 3 : in forum Delphi Help	
ISTEALERS ANYONE CAN POST IT;D	Replies: 4 Last Post: 27-05-2009, 18:52
By abousakr in forum Malware Discussion and General Help	

Posting Permissions

You may not post new threads
 You may not post replies
 You may not post attachments
 You may not edit your posts
Pingbacks are On
Refbacks are On

BB code is On
Smilies are On
[IMG] code is On
 HTML code is Off
Trackbacks are On

Forum Rules[Contact Us](#)[OpenSC](#)[Top](#)[Back to top](#)

All times are GMT +1. The time now is 01:13.

www.opensc.ws

Copyright ©2005 - 2012, OpenSC Forums

Search Engine Friendly URLs by vBSEO 3.6.0 ©2011, Crawlability, Inc.



[Home](#) [Forum](#) [Research Articles](#) [What's New?](#) [Store](#)

Today's Posts [FAQ](#) [Calendar](#) [Community](#) [Forum Actions](#) [Quick Links](#)

Quick search

Member login
User Name Password [Register](#)

[Home](#) [Forum](#) [Malware](#) [Malware Samples and Information](#) Should i post ZeuS 2.0.8.9?

Join our official IRC! irc.datawhore.net #opencsc

All members should check OpenSC Password Policy under OpenSC - News

Hi Unregistered, check out our new rules in <http://www.opencsc.ws/opencsc-rules/>

Check our new page and feed your brain: <http://www.opencsc.ws/research/>

[+ Reply to Thread](#) Results 21 to 23 of 23 [Page 3 of 3](#) [1](#) [2](#) [3](#)

Thread: Should i post ZeuS 2.0.8.9?

3 Likes

[LinkBack](#) [Thread Tools](#) [Display](#)

09-04-2011 #21

patalocs

Member

Join Date:	Nov 2008
Location:	Cali
Posts:	89

kubanezi gave me zues source free, thanks bro i will spread your fame.

[Reply With Quote](#)

09-04-2011 #22

s6x

Junior Member

Join Date:	Apr 2011
Posts:	28

Originally Posted by **nyu**
Selling zeus full source for \$100K.

K.
Originally Posted by **patalocs**
kubanezi gave me zues source free, thanks bro i will spread your fame.

[Reply With Quote](#)

09-04-2011 #23

nasGeneration

Senior Member

nasGeneration's Avatar	
Join Date:	May 2010
Location:	#root
Posts:	170

Originally Posted by **nyu**
2.1.0.1 just has modules

i think some noobs who owned the source are playing with it xD

[Reply With Quote](#)

[+ Reply to Thread](#)
[Page 3 of 3](#) [◀ First](#) [◀](#) [1](#) [2](#) [3](#)
[« Previous Thread](#) | [Next Thread »](#)
Thread Information

There are currently 1 users browsing this thread. (0 members and 1 guests)

Similar Threads

(\$) Post your items (\$)	Replies: 95
By Luca in forum Off-Topic	Last Post: 12-11-2011, 04:08
First post	Replies: 10
By strspeed in forum Off-Topic	Last Post: 14-02-2011, 01:45
POST UR CHIPZ	Replies: 3
By aoi in forum Off-Topic	Last Post: 01-06-2010, 01:21
where do i post requests?	Replies: 1
By 1337 hax0r 3 .- in forum Delphi Help	Last Post: 04-05-2010, 19:23
ISTEALERS ANYONE CAN POST IT;D	Replies: 4
By abousakr in forum Malware Discussion and General Help	Last Post: 27-05-2009, 18:52

Posting Permissions

You may not post new threads
 You may not post replies
 You may not post attachments
 You may not edit your posts

BB code is On
Smilies are On
[IMG] code is On
 HTML code is Off
Trackbacks are On

Pingbacks are On
Refbacks are On

[Forum Rules](#)

[Contact Us](#)

[OpenSC](#)

[Top](#)

[Back to top](#)

All times are GMT +1. The time now is 01:13.

[www.opensc.ws](#)

Copyright ©2005 - 2012, OpenSC Forums

Search Engine Friendly URLs by vBSEO 3.6.0 ©2011, Crawlability, Inc.



EXHIBIT 7



Topics

Authentication

Cloud Security

Compliance

Consumer Security

Cybercrime and Fraud

Cyberwarfare

Data Loss Prevention

Encryption & Tokenization

Enterprise Security

Governance, Risk & Compliance (GRC)

Government & Policy

Insider Risk

Mobile Security

mythbusting

Other

PCI

PCI DSS Feedback

Personal Security

Podcasts

RSA Conference

scams

Organized Cybercrime: Nefarious Sophistication Featuring Zeus V2.1.0.10

Written on September 29, 2011 by RSA FraudAction Research Labs

Comments

The RSA Research Lab investigates and monitors a large number of malicious cybercrime servers operating in the wild. One of the Lab's most significant findings was kept under wraps as the Research team investigated its server-side and the general background of the gang standing behind this clandestine control central.

What our researchers discovered was nothing less than the robust mercenary workings of a virtual heist machine, one that has been operational on an ongoing basis, militating and robbing financial data from hundreds of thousands of infected users all over the world. The tool of choice—Zeus v2.1.0.10, the most advanced variant of Zeus to date. The end result: endless logs of compromised financial data and untold numbers of wire-fraud transactions.

A Privately Developed Zeus Upgrade

Unlike the large majority of banking Trojan, the Zeus Trojan has always been a commercial code, sold by its creator to those who could afford an advanced fraud tool and understood how to use it. With time, Zeus became the most infamous and most propagated Trojan in cybercrime history. In October 2010, nearly one year ago, the *bequeathing* of the Zeus Trojan's source code by its owner "*Slavik*", to his then biggest rival, the SpyEye Trojan's coder ("*Harderman*"), united the future of 2 giant commercial codes and threw a Zeus-faced wildcard into the game when its entire source code was leaked in March 2011.

But it was nearly two months *before* the announcement of the code 'merger' was even made that RSA researchers were already looking at a rather special upgrade of the Zeus Trojan: **Zeus v2.1**. A surprising and rare new version which included some of the most sophisticated additions to the Zeus code seen in recent times, making it more impervious and hardened thus shutting-out a lot of potential interference with this variant's configuration and its communication patterns.

At the time (early September 2010), our team was in the possession of a single variant of this upgrade and was not entirely sure what it represented as yet. The interesting part of the upgrade was its low propagation numbers and the time lapse it took for the Lab to see more of it in the wild. True Zeus 2.1.0.10 variants were not being sold in underground forums. These two initial observations already suggested that the new upgrade was the property of one cybercriminal or a single cybercrime gang.

Within six months, Zeus 2.1.0.10 was being detected more and more often, and although the number of variants kept growing, the trigger list in each and every one of them was *identical* – a rare case for Zeus variants in which each operator updates his own list of triggers. This was the third sign pointing to a single operations team for Zeus 2.1.0.10.

Subscribe Here

Subscribe to the RSA blogs and podcasts for the latest posts and security updates!

[Sign Me Up Now! ▶](#)

Search



Speaking of Security
Podcast

Intelligence-driven Security:
New RSA research from the
Security for Business
Innovation Council – Podcast
#233

Tokenization: An Alternative
Form of Data Protection –
Podcast# 232

CyberShop 'til You Drop –
Staying Safe Online this
Holiday Season – Podcast
#231

RSA Reaches Milestone of
500,000 Phishing Attacks
Shut Down – Podcast #230

An Online Community to
Share Threat Intelligence –
Podcast #227

RSA Connection



Blog Authors

[Idan Aharoni](#)

[Eric Baize](#)

[Erin K. Banks](#)

[Heidi Bleau](#)

[Sean Brady](#)

[Chris Corde](#)

[Sam Curry](#)

Security Information and Event Management (SIEM)

June 2011 – a sharp peak in Zeus 2.1.0.10 attacks resulted from the propagation of *hundreds* of variants of this upgraded version. To date, the RSA Research Lab detected 414 different variants, and yet, each and every variant still went after the exact same trigger list. At this point it was clear that Zeus 2.1.0.10 belongs to one gang who had the Zeus source code way before the merger, way prior to the code leak and before anyone even imagined what would become of Zeus.

Security Management

Software Assurance

Standards

transformational security

Uncategorized

Virtualization

This gang developed their own Zeus Trojan using Zeus' source codes and its mainframe; this gang operates Zeus 2.1.0.10 without sharing their malevolent creation with outsiders.

Zeus 2.1.0.10 Has its Own Techniques

More than the actual upgrade of the Trojan code, the new Zeus 2.1.0.10 behaved in a new way, unlike the one observed in other Zeus variants. Unlike other advance Trojans who contact the mothership through reverse proxies, fast flux networks, or those who use their own botnet as proxies – Zeus 2.1.0.10 never communicates directly with the mothership.

This special variant further uses another obfuscation technique for cases where it fails to find a live update point. In order to make sure the botnet always ‘calls home’ Zeus 2.1.0.10’s operators programmed a randomized, on-the-fly domain name generator, based on a constant algorithm the Trojan’s configuration dictates. The algorithm creates 1,020 domain names (URLs) per day. Each new and unique domain name is a string of letters. The suffix “**news**” or “**forum**” follows the domain name when it is used for the Trojan’s update and drop communications.

The cybercriminal operation team behind the scenes has the same algorithm. They know exactly when the whole botnet will attempt to communicate with a specific new domain name, and then simply go and buy that domain name, hosting each one through facilities located all over the world. At that point, the whole botnet queries the new domain with a request for the update file – and receives it, and the C&C queries its bots for the stolen data they have in store – and receives it. Mission accomplished.

This all happens without anyone outside the gang knowing their algorithm or being able to guess which communication channel they will choose for their botnet next. Even if an external party was to attempt to solve the algorithm, they would have to buy the domains before the gang does, thus engaging in a race against time and paying for numerous domain registrations *every hour* (!). No matter how many domains an adversary buys, the bot masters will eventually buy one and the botnet will end up communicating with it.

Figure 1: Zeus 2.1.0.10 Domain Randomization (Example)

#	client_id	time_created	log_ipm	log_email	connection	region	city	port	proto	host	domain	last_update	last_error
1	1234567890	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
2	1234567891	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
3	1234567892	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
4	1234567893	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
5	1234567894	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
6	1234567895	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
7	1234567896	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
8	1234567897	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
9	1234567898	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0
10	1234567899	2011-01-01 00:00:00	0	0	0	US	New York	8080	TCP	192.168.1.100	www.zeus-randomized.com	2011-01-01 00:00:00	0

The communication through randomized domains generated by the Trojan is directed through a list of legitimate VPS[1] and legitimate cloud services used as a proxy. This raptures any further tracking possibilities of the true motherships which militate the immense botnet.

Zeus 2.1.0.10’s behavior pattern has never been used in Zeus or SpyEye variants, but it sure is identical to another Trojan’s sophisticated and diurnal operations – **Sinowal**. A long standing, privately owned Trojan, operated by an organized cybercrime gang based out of Russia, Sinowal is perhaps one of the most persevering private banking Trojans; one whose nefarious nature has been the intrigue of many security researchers since as early as 2006.

It was initially somewhat surprising to see that Zeus 2.1.0.10 was not only a private version of Zeus, it also behaves exactly in the same manner as Sinowal similarly

Mike Foley

RSA Virtualization Evangelist

Seth Geric

Bob Griffin

Dr. Ari Juels

Shannon Kellogg

Rashmi Knowles

Chief Security Architect, EMEA

Mischel Kwon

Security Management Insights

David Marsh

Nirav Mehta

SOS Podcast

RSA FraudAction Research Labs

Uri Rivner

Jason Rohlf

Steve Schlarman

Payment Security Focus

Branden Williams CTO

Tag Cloud

Advanced Persistent Threats advanced threats APTs Archer Authentication botnet cloud Cloud Security Compliance credit card fraud **cybercrime** Cybercrime and Fraud Cyberwarfare dark cloud DLP eGRC encryption enVision Fraud fraudsters GRC malware Mobile Security mules PCI compliance PCI

DSS Phishing risk
risk management RSA
Conference SecurID
security
management security
operations security policy
SecurityWeek SIEM
SpyEye Stuxnet
tokenization **trojans**
Virtualization WikiLeaks
worms **Zeus** **Zeus**
Trojan

held by Russian-speaking cybercriminals. These common denominators raised a logical suspicion as to the possibility of the two sharing some links if not operated by the same gang altogether.

Behold, a Mothership in the Cloud

The motherships of Zeus 2.1.0.10 are somewhat of an enigma which has never been detected before or traced by security researchers. Nonetheless, in one of their research projects, the RSA Research Lab's team has managed to finally locate one of the best concealed C&C servers operating in the wild.

The Lab's findings have confirmed everything they saw in Zeus 2.1.0.10's Trojan configuration and provided for a rare glimpse into the workings of a very methodic crime gang. It was no surprise to see that both Sinowal and Zeus 2.1.0.10 variants manage to amass and manage staggering amounts of infected bots; their crimeware codes' tenacious nature and the clever way in which they keep the enemy guessing have been their strongest allies. RSA was looking at a the gang's server and concluded that it contained over 200GB of filtered compromised financial information—immense by any measure.

Zeus 2.1.0.10 – A Rare Server-Side View

Once inside the Zeus 2.1.0.10 mothership, RSA researchers have been able to confirm that a portion of **42%** of all infections on this botnet took hold of USA-based machines. Large infection numbers followed for other countries as well; the top 10 being Spain, Italy, Canada, India, Mexico, France, Russia, the UK and Brazil, all in considerably lower portions. This massive botnet has managed to amass 45,802 new infected machines in only one day in February 2011!

Control Panel

The botnet's control panel is an elaborate Zeus-type interface with a few added features. The panel has accounts set up for multiple users who may enter the platform and manage different activities for the bots. Some of the users changed over time; some have remained the same for over a year. Each of the users has a different set of privileges attributed to them, which hints to some sort of a hierarchy within the group operating this Trojan. An interesting user name choice in the panel was "**Slavik**" – the alias used by the original coder who invented the Zeus Trojan and who peddled it through underground forums before the code merger. Seeing as this gang most definitely had the Zeus source code long before Zeus was surrendered to "Harderman's" hands, it is not beyond reason that Slavik himself was somehow part of the development of Zeus 2.1.0.10 and part of this clandestine crime gang.

Zeus 2.1.0.10 Panel Options

This particular control panel is an implementation of every single Zeus innovation to date, whether it be the advanced plugins it can use, the level of control it can exercise on each bot, or the amounts of crucial financial data it contains thanks to smart data filtering scripts.

Some of the most interesting features of this Zeus 2.1.0.10 panel only exist for this variant and do not appear in other Zeus control panels. It is once again evident that the gang operating this botnet had their own ideas as to how they wanted their malware to facilitate their crimes.

- **Server-Side Trigger List**
- **VNC + SOCKS5 + Jabber Notification Set Up = MITM.** The MITM trinity; remote access, SOCKS5 and an instant messaging are all tools used by fraudsters who commit real-time fraud. These plugins are part of a session hijacking scenario and are rather telling of the type of operations carried out by Zeus 2.1.0.10's perpetrators. What this spells out is manual MiTM.
- Bot Comments
- Botnet Scripts
- "**SetHome**" A seemingly innocent script sets a new Home page on all the bots' internet browsers. This script was executed on batches of tens of thousands of zombie bots. Why so popular? How about setting a drive-by-download page and making it the first page every victim opens as soon as they launch Internet explorer, thus updating the Trojan on those bots.
- **Block URL**
- **Private Key** The private key is a PEM file designed to apply the encryption key for Zeus 2.1.0.10's configuration. Data sent from the mothership to the infected bots is signed using this private key.
- **Popular URLs** What are the URLs most often browsed by victims? By logging a list of the most popular URLs the Trojan's operator may choose to target a new entity.
- **Search Inside Data Log**
- **Bot Info**

Following the investigation into this cybercrime operation, the RSA FraudAction Research Lab has contacted several law enforcement agencies to inform them of these findings.

[1] VPS: Virtual Private Server

    Subscribe to RSS

Leave a Reply

 Name (required) Mail (will not be published) (required) Website

© Copyright 2011 EMC Corporation. All Rights Reserved.

The opinions expressed here may be personal. Content published here is not read or approved in advance by EMC and does not necessarily reflect the views and opinions of EMC.

[Legal](#) [Privacy](#) [Contact RSA](#)