

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,  
petrOvich, 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, kainehave, 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.

**DECLARATION OF WILLIAM B. NELSON IN SUPPORT OF PLAINTIFFS'  
APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER,  
SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

FILED  
CLERK  
2012 MAR 19 AM 8:51  
U.S. DISTRICT COURT  
EASTERN DISTRICT  
OF NEW YORK

**CV 12-1335**

Case No.

**FILED UNDER SEAL**

**KORMAN, J.**

**MANN, M.J.**

I, William B. Nelson, declare as follows:

1. I am President and CEO of the Financial Services Information Sharing & Analysis Center (FS-ISAC). 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.

**FS-ISAC**

2. The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

3. The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,400 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 20 trade associations representing the majority of the U.S. financial services sector.

4. The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments, as well as U.S. CERT.

5. With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also

work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various payments, clearing houses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), the various payment card brands and most of the card payment processors in the U.S.

6. The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the originator and shared for the good of the sector, the membership and the nation. The FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry. Among other activities carried out on behalf of its members, FS-ISAC develops risk mitigation best practices, threat viewpoints and toolkits, provides technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics and facilitates member sharing of thread, vulnerability and incident information. Of particular relevance to this matter is FS-ISAC's Account Takeover Task Force, a special project to address the specific risk of account takeovers by the Zeus, Ice-IX and SpyEye botnets.

#### **Injury To FS-ISAC Members Caused By The Zeus Botnets**

7. I have conducted an assessment regarding the impact of financial account takeovers carried out through botnets on the financial institution members of FS-ISAC, on the financial services industry generally and on consumers who carry out financial transactions online.

8. Through my role and experience at FS-ISAC, I have knowledge relating to

reporting of online banking fraud by FS-ISAC members to various government agencies. In particular, FS-ISAC members report such fraud to (1) The Federal Deposit Insurance Corporation (“FDIC”), the agency that identifies, monitors and addresses risks to deposit insurance funds, and (2) FinCEN, a bureau of the U.S. Department of the Treasury with a mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems from abuse.

9. The FDIC and FinCEN receive a variety of confidential reports from financial institutions regarding online banking fraud. Almost all of the incidents reported to the FDIC and FinCEN relate to malicious software on online banking customers’ computers. Typically, a victim is tricked into visiting a malicious website or downloading malicious software that gives perpetrators access to victims’ banking passwords and credentials. The perpetrators use that information to transfer money out of victims’ accounts using the Automated Clearing House (ACH) system or the Federal Reserve’s Fedwire transfer system. Both the ACH and Fedwire systems are used by banks and credit unions to process payments on behalf of their customers.

10. Since 2005, financial institutions have reported to FDIC and FinCEN a cumulative \$477 million in consumer loss from such online banking fraud. The rate of such loss has been substantial in recent years and was virtually nonexistent before 2005.

11. I have reviewed the technical analysis and investigation of the Zeus Botnets, set forth in the Declaration of Mark Debenham, submitted in this case. The Zeus Botnets are used to carry out precisely the type of online banking fraud that has resulted in \$477 million in consumer loss since 2005.

12. Mr. Debenham’s declaration sets forth a number of institutions targeted by the Zeus Botnets, including numerous U.S. financial institutions and NACHA, the organization that manages the ACH Network (the primary infrastructure for electronic transfers of money). Nearly all of those U.S. financial institutions and NACHA itself are members of FS-ISAC and FS-ISAC represents their interests in protecting these financial institutions, consumers and the industry from cybercrime and fraud.

13. I have independently discussed the Zeus Botnets with financial institution members of FS-ISAC and with NACHA, which have collected and analyzed information regarding the Zeus Botnets. FS-ISAC's members report that they view the Zeus Botnets as a major threat, which damages their brands and causes injury to both consumers engaged in online banking and the financial services industry generally.

14. Based on the analysis set forth in Mr. Debenham's declaration, information provided to me by FS-ISAC's members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the Zeus Botnets have caused, and continue to cause, extreme damage to FS-ISAC members, consumers and the financial industry. If allowed to continue, such damage will be compounded as this case proceeds.

15. Third party reports regarding the Zeus Botnets support this conclusion and demonstrate that the Zeus Botnets are a very significant part of the overall online banking fraud loss reported each year by FS-ISAC's financial institution members and by NACHA. For example, in May 2010, the technology company Unisys issued a report entitled "Zeus Malware: Threat Banking Industry," which estimated that the Zeus Botnets had targeted more than 960 different banks and had stolen over \$100 million since its inception in approximately 2007. A true and correct copy of the Unisys report is attached to this declaration as Exhibit 1.

16. Based on the analysis set forth in Mr. Debenham's declaration, information provided to me by FS-ISAC's members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the defendant operators of the Zeus Botnets access without authorization information from FI servers. I conclude that through such intrusion, defendants steal account credentials and other personal information from the customers of those FS-ISAC members and ultimately steal money from the accounts of those customers. I have also confirmed with FS-ISAC members that they have collected and observed evidence of such access without authorization from FI servers, in order to steal information and funds. This activity causes injury to the FS-ISAC member institutions and their customers.

17. Based on the analysis set forth in Mr. Debenham's declaration, information

provided to me by FS-ISAC's members and my knowledge of the impact of such activities on FS-ISAC's members, I conclude that the defendant operators of the Zeus Botnets make counterfeit copies of the trademarks of financial institutions that are FS-ISAC members, including but not limited to the trade names of such financial institutions, the trade name of NACHA, and the trademark logos of these institutions. I have also confirmed with FS-ISAC members that they have collected and observed such evidence of trademark infringement carried out by the Zeus Botnets. I further conclude that defendant operators of the Zeus Botnets use those counterfeit trademarks in spam email or on fake web pages, in order to deceive consumers and to carry out schemes enabling the theft of personal information and funds from the financial institutions and their customers. This activity causes injury to the FS-ISAC member institutions, by diminishing their brands and goodwill. This activity causes injury to the FS-ISAC member institutions and their customers by causing confusion to consumers and victims of such schemes, by leading them to believe that the spam email and web pages containing the counterfeit trademarks originate from the legitimate brand owner when, in fact, they do not.

18. The interests that FS-ISAC seeks to protect in this case and the injury that it is attempting to remedy, as described above, are directly related to the purposes of FS-ISAC. It is FS-ISAC's role to protect its financial institution members from cybercrime and to mitigate the threat and injury flowing from such abuse. This role is demonstrated in FS-ISAC's stated purpose and the original government mandate that led to its creation.

19. The injury described above has already occurred and continues to be immediate and threatened. This injury is common across all of FS-ISAC's members that are targeted by the Zeus Botnets and the injury, and relief sought to disable the Zeus Botnets, are not specific to any particular FS-ISAC member.

20. I conclude based on the foregoing that, unless the Zeus Botnets are disabled, the harm described above will continue and, given its scale, will irreparably damage FS-ISAC's member institutions and the financial services industry generally.

Executed this 18th day of March, 2012

*William Nelson*  
William Nelson

# **EXHIBIT 1.**





# Zeus Malware: Threat Banking Industry

Unisys Stealth Solution Team

White Paper

May 2010

Primarily a crimeware kit, Zeus is used by cyber criminals across the Globe, and is designed to steal users' online banking details as well as other important credentials. Today, Zeus is estimated to account for some 44% of the banking malware infections and has impacted an estimated 3.6 million computers in the U.S. alone. Its victims include more than 960 different banks with the latest reports indicating that it has infected almost 90% of Fortune 500 companies.

Zeus is estimated to have caused damages worth US\$100 million since its inception. Alarmingly, up-to-date anti-virus programs are effective at blocking Zeus infections only 23 percent of the time. It is clear that traditional anti-virus software alone cannot be used to combat Zeus. Companies need to consider radical innovations in security to ensure protection from online fraud and to maintain customer goodwill.

This paper provides visibility into the intrinsic risk that Zeus has over the banking industry and how Unisys can help avoid the threat through its security portfolio.

## Table of Contents

Introduction	4
Impact of Zeus	5
Financial Damage	5
Damage to Goodwill	5
Scale of Infection	5
How Zeus Works	6
Latest Developments in Zeus	7
The traditional Malware Control Approach vs. Zeus Malware	7
Conclusion	8

## Introduction

“Nordea Bank loses \$1.14 million in online fraud” – iTWire (Jan 2007)

“Heartland Payment Systems says malware breach cost \$12.6 million” – ZDNet (May 2009)

“Conficker worm affects millions of users worldwide” – New York Times (Apr 2009)

“ATM malware in Eastern Europe lets criminals steal data and cash” CNET news (June 2009)

These are just a few instances of banks and financial institutions being affected by malware (short for malicious software). With the rise of widespread broadband Internet access, malware has now emerged as the primary vehicle for organized cybercrime. As noted in Symantec’s annual report for 2009, the number of detected malware samples in 2009 grew by 71 percent as compared to 2008. Most malwares are now geared towards making profit and enabling financial gain. This has led to an increased attack on banking and financial systems. As a result, the total monetary loss related to online fraud has soared from<sup>1</sup> US\$265 million in 2008 to US\$559.7 million in 2009. The worst affected is the SMB sector (small and medium business) which, per the FBI, has lost US\$40 million since 2004 courtesy online banking scams.

A recent survey of over 500 US-based SMB organizations<sup>2</sup> revealed that approximately 55% of the SMBs experienced a fraud attack in the last year with over 50% experiencing multiple incidents. Of these, 58% of the incidents involved online banking. Alarming, 87% of the victims failed to fully recover lost funds, recovering only 44% of the losses on average. A separate study of 50 SMBs, which fell prey to online banking Trojans in 2009, revealed that they lost US\$157,000 on average.

The spread of malware has not been restricted to the SMB sector or the US alone. Losses from online banking fraud in the UK rose 14% in 2009 year-over-year to reach a total of £59.7million.<sup>3</sup> The bulk of the rise was due to an increase in the number of criminals infecting online bankers’ computers with malware capable of gathering a person’s online banking details, thus allowing fraudsters to steal money from their account. Such fraud has increased exponentially since 2007, when the Zeus malware was first detected.

The Zeus malware is one of the most pervasive and damaging banking malware known to date. It is primarily observed to be used for financial gain by stealing online credentials such as online banking, email, FTP and other passwords, although it is also capable of taking complete control of a compromised computer. Zeus was first used in 2007 to steal information from the United States Department of Transportation, but has evolved over time. The ease of use of Zeus has made it an ideal tool for even novice hackers to easily steal banking-related information from an individual, or customer-related data from a server. Being freely traded in underground forums, it has become widely prevalent and is now being distributed by multiple, unrelated parties.

Zeus reached record numbers in May 2009 with more than 5,000 variants. It has essentially earned the ‘bestseller’ status among malware with such wide variants. The Zeus malware alone is estimated to have caused damages worth US\$100 million since its inception. Actual figures may be much higher since currently no government entity tracks and reports on the number of victim organizations and the amounts lost. Trend Micro recently reported discovering a new Zeus variant targeting major consumer banks in Italy, England, Germany and France.

<sup>1</sup> Source: “2009 Internet Crime Report” released by the Internet CrimeComplaints Center (iC3)

<sup>2</sup> Survey conducted by the Ponemon Institute and Guardian Analytics

<sup>3</sup> Source: “New card and banking fraud figures” released by the UK Cards association

## Impact of Zeus

### Financial Damage

According to security company Trusteer, Zeus alone accounts for 44% of all banking malware infections. Many cases involve SMBs (see box below) who have had huge amounts transferred out of their accounts without their knowledge.

Little & King LLC, a small promotions company based out of Merrick, N.Y. lost \$164,000 in fraudulent wire transfers in Feb 2010, after one of its computers was infected by the Zeus malware. The firm now faces bankruptcy since it has run out of funds for working capital.

Cyber criminals based in Ukraine stole \$415,000 in July 2009 from the coffers of Bullitt County, Kentucky by unauthorized wire transfers, using Zeus and the victim's own Internet connection.

Smile Zone, a Springfield, Missouri based dental practice, lost \$205,000 in March 2010 after being affected by Zeus.

In most cases of financial loss due to malware, banks try to reverse the fraudulent transfers and are at least able to partially recover the funds (see box below), but the chances of that succeeding diminish rapidly after the first 24 hours following unauthorized activity. Businesses do not enjoy the same protections afforded to consumers hit by online fraud, as banks do not offer insurance against fraud to business customers.

Port Austin, Michigan-based United Shortline Insurance Service Inc fell victim to the Zeus trojan and lost nearly \$150,000 in March 2010. Luckily its bank, the Bay Port State Bank, was able to recover about half the money.

Eskola LLC, a Tennessee-based roofing firm and Orange Family Physicians, a medical practice in Virginia, lost \$130,000 and \$46,000 respectively to Zeus in January 2010. While Eskola's bank recovered around \$100,000, Orange Physicians' bank could recover only \$6000.

The cases detected so far are probably just the tip of the iceberg; most victims are unwilling to disclose their identity or the full extent of their financial losses, fearing implications for their businesses.

<sup>4</sup> Source: Report by RSA' FraudAction Anti-Trojan division

### Damage to Goodwill

The recent months have seen a flurry of malware-related lawsuits. Victims of online fraud are now suing their banks to recover some of their losses (see box).

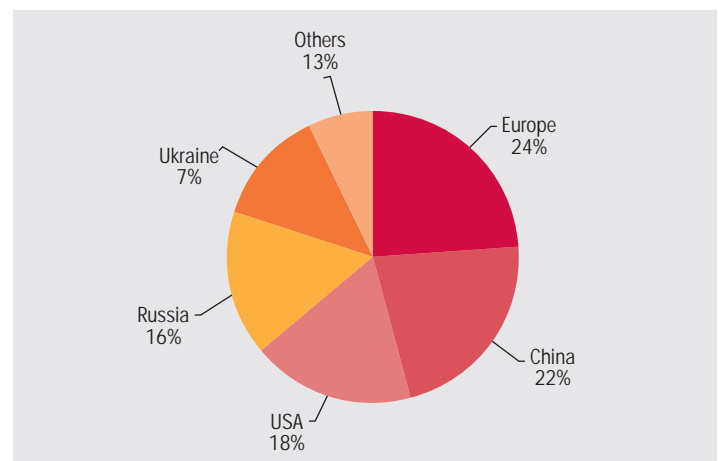
In Illinois, a couple whose bank account was robbed of US\$26,500 has been allowed to sue their bank, Citizens Financial Bank, for its alleged failure to implement the latest security measures designed to prevent such compromises. The outcome of these cases is still awaited.

Banks are currently under no legal obligation to reimburse business customers for losses suffered due to malware. Such incidents, however, cause a huge loss of reputation and bad publicity for the bank, in addition to loss of confidence among customers who transfer their accounts to other banks. Since trust is fundamental to banking institutions, such incidents lead to decreased growth for the affected banks. Customers also begin to migrate away from the cost-effective online banking channels, leading to increased costs for the bank.

### Scale of Infection

Though it is difficult to trace exactly how many systems have been affected by Zeus, it is estimated that around 3.6 million PCs are infected in the US alone. Research indicates that as of April 2010, 88% of Fortune 500 companies have been affected by this malware.<sup>4</sup>

The most recently detected large Zeus botnet is the so-called Kneber botnet. In February 2010, the US-based corporate security company NetWitness reported the detection of Zeus-infected computers in 2,500 organizations in 196 countries worldwide. A total of 76,000 infected computers were detected.

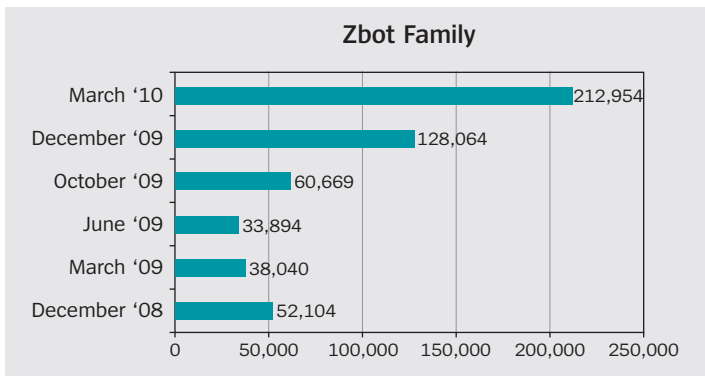


As of October 28, 2009 Zeus had also sent out over 1.5 million phishing messages on Facebook. From November 2009, Zeus spread via e-mails purporting to be from Verizon Wireless. A total of nine million of these phishing e-mails were sent.

Per the Microsoft Malware Protection Center, the number of Zeus infections has increased when compared to last year. The figure below illustrates the same:

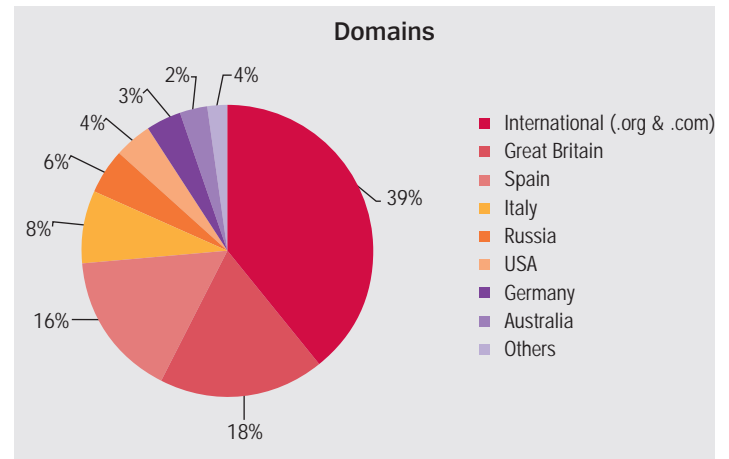
Out of the 11 international domains that Zeus targets, 8 are banks offering internet banking services to its clients and the other 3 are commercial internet service providers.

Running Zeus from any location is exceedingly possible. More often or not, malicious users place their servers with European, Chinese, North American and Russian providers as they offer well developed hosting services. Zeus records the location of the host when the bot checks into the command and control server.



Zeus targets certain top level domains; the most commonly targeted domains are international domains (.org and .com) which belong to large multinationals.

The following chart clearly depicts the top domains that are targeted by Zeus:



Top 5 victim countries affected by Zeus are:

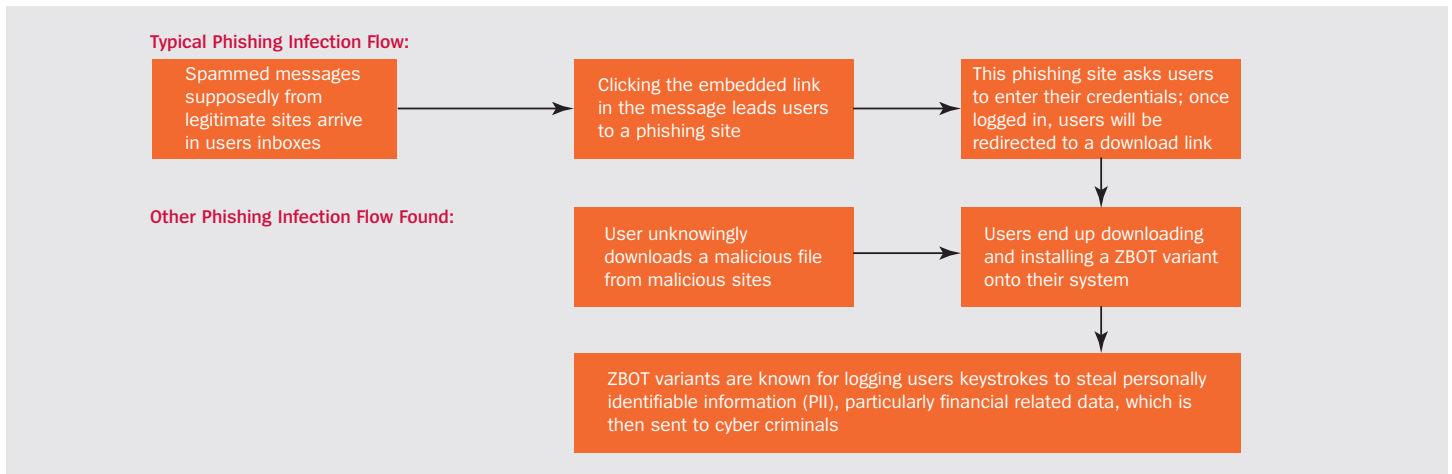
Country Name	% Machines Infected
Egypt	19%
Mexico	15%
Saudi Arabia	13%
Turkey	12%
United States	11%

## How Zeus Works

The primary purpose of Zeus is to steal online

Malware is designed to infiltrate a computer system without the owner's informed consent. While malware was initially written for pranks, experiments or vandalism, it is now primarily used to perpetrate online fraud. Zeus is a specific kind of malware known as a 'botnet'. A botnet is a collection of software agents designed to run autonomously and automatically. Malware writers are now increasingly using botnets to affect as many machines as possible and use a 'bot master' to control the group remotely, if required. Other notable botnets apart from Zeus are Storm, Conficker, Mega-D, Pushdo and Srizbi.

Zeus is likely to have originated in Russia or Eastern Europe and has now entered the underground cybercriminal community as a commodity. Zeus is also known as ZBot, PRG, Wsnpoem, Gorhax and Kneber.



Zeus primarily targets machines running Microsoft Windows XP (SP2/SP3). Windows Vista machines have also been found to be infected. The primary purpose of Zeus is to steal online credentials. This is done by techniques such as keystroke logging, capturing screenshots, or advanced methods such as HTML injection into web pages and exploiting browser vulnerabilities. Zeus gathers a variety of system information along with passwords and encryption certificates and sends this to a command-and-control server. The server can also send a configuration file to the bot,, specifying a list of actions to be performed.

The Zeus crimeware kit can be purchased for as low as US\$700 and provides a ready-to-deploy package for hackers to distribute their own botnet. The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command - and -control server. ZBot is a generic back door that allows full control by an unauthorized remote user. However it is primarily observed to be used for financial gain by stealing online credentials such as online banking, email, FTP and other passwords.

## Latest Developments in Zeus

- Zeus is now exploiting features in Adobe Reader to launch malicious attacks.
- Zeus 1.6, which is the latest version of Zeus in market, is targeting Firefox browser
- With the explosion of social networking across the globe, Zeus is now using social networking sites to send out its phishing messages to users; for instance, last year it sent out close to 1.5 million messages to Facebook users. If a user opened that message there would be a Trojan that would be installed on their system

## The Traditional Malware Control Approach vs. Zeus Malware

The results of the survey conducted by Trusteer, a security company, on close to 10, 000 machines are quite astonishing. Zeus is able to penetrate close to 55 percent of systems which have up-to-date antivirus. Up-to-date anti-virus programs are effective at blocking Zeus infections only 23 percent of the time.

The above table clearly shows that the traditional assumption that the system is free from any virus attack, if there is an antivirus installed on it, does not hold true in case of Zeus.

What is even more alarming is that Zeus is now reported to have successfully undermined the two-factor authentication put in place by many banks. Even the use of biometrics may not be helpful (see box below). This makes it clear that multiple-factor authentication simply cannot prevent fraudulent activity if the user is operating from a compromised environment in the first place.

A New Hampshire-based IT consulting firm, Cynxsure LLC, employed a fingerprint scanner for authentication to mitigate risks from password-stealing malware. However, Cynxsure still ended up losing nearly \$100,000 in February 2010. Zeus trojans include a feature called “form grabber” that effectively steals the fingerprint authentication data before the web browser can encrypt it.

It is now understood that, to reduce the risk associated with being exposed to powerful malwares such as Zeus, just installing and updating antivirus software may not be sufficient. Companies need to look at radical innovations in the security field and adopt new technologies to ensure that their machines never get compromised. This will go a long way to protecting them from any kind of online fraud, and help them maintain customer goodwill.

	General Population	Zeus Infected
No Antivirus found	23%	31%
Antivirus found but not up-to-date	6%	14%
Antivirus is up-to-date	71%	55%

## Conclusion

Zeus today has earned a reputation as the most dangerous malware for the banking industry. This is primarily because of the vast number of toolkit versions readily available, as well as the features it possesses, to thwart the traditional antivirus solutions. The ease of use that Zeus provides makes it ideal for even an amateur hacker to easily steal online banking and other credentials for financial gain. Zeus is now being used by cybercriminals to steal personal information and even people's identities.

With Zeus having infected almost 90 percent of Fortune 500 companies, and causing huge financial damages to around 2400 companies in 196 countries worldwide, it is unarguably among the top malwares that exist today. Though antivirus companies are struggling hard to provide the right solution for a Zeus free environment, the malware continues to evolve and thwart their efforts.

It is clear that the conventional methods of malware control have not succeeded against Zeus which has, therefore, managed to cause an estimated damage of more than US\$100 million since its inception. This is primarily because conventional methods are not fully effective if the user is operating from a compromised environment in the first place.

At Unisys, we assess, design, develop, and manage mission-critical solutions that secure resources and infrastructure for governments and businesses. Our approach integrates resource and infrastructure security, creating the most effective and efficient security environment possible and freeing our client to focus on best serving its citizens and customers. Keeping this in mind, Unisys has developed the Secure Virtual Terminal solution for the banking industry to address security risks such as Zeus. The Secure Virtual Terminal device simply needs to be plugged into the USB port of any laptop or desktop computer to transform it to a trusted online banking terminal. When the online banking session is completed, the device can be removed and the computer returns to normal. This simple and easy-to-use solution, based on Unisys' patent-pending Communities of Interest (CoI) technology, can go a long way towards eliminating the threat from Zeus and other malware. For more information, please contact your Unisys representative or visit us at [www.unisys.com](http://www.unisys.com).

**For more information, contact your Unisys representative.  
Or visit our website at: [www.unisys.com](http://www.unisys.com)**