H2 2009 E-Threats Landscape Report

MALWARE AND SPAM TRENDS

Disclaimer

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post -release information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide.

Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Author

Bogdan BOTEZATU, Communication Specialist

Contributors

Răzvan LIVINTZ, Communication Specialist – WEB 2.0 Threats

Daniel CHIPIRIŞTEANU, Malware Analyst
Alexandru MAXIMCIUC, Malware Analyst
Dragoş GAVRILUŢ, Malware Analyst
Ştefan – Cătălin HANU, Malware Analyst
Marius VANŢĂ – Malware Analyst

Alexandru Dan BERBECE - Database Administrator

Adrian MIRON - Spam Analyst
Irina RANCEA – Spam Analyst

Table of Contents

Overview

Year 2009 witnessed a wide range of security threats aiming at both end-users and at corporate networks. The Downadup worm (also known as Conficker or Kido) took a dramatic surge and managed to stay one of the top three global e–threats during 2009. Although not entirely dangerous (as variants A, B and C had no malicious payload), its spreading mechanisms and its resistance to detection may be regarded as the cornerstone of the upcoming breeds of highly-destructive malware.

During the past six months since the release of our previous report, malware authors have preserved their focus to web-based attacks, but at the same time, they have been actively looking for new methods of disseminating their products. Large social networks and ephemeral web pages boosted by intense BlackSEO strategies have also become the favorite hotspots for drive-by downloads and worm distributions.

The extremely popular iPhone mobile phone from Apple has earned enough market share to become a viable target. Its market grip, combined with most users' choice of "jailbreaking" the device allowed malware authors to successfully exploit the default password used by the SSH (secure shell) Unix utility in order to gather sensitive e-banking credentials and add the device to a botnet.

Distributed Denial-Of-Service attacks witnessed an increase in terms of both violence and amount of damage done to the affected companies. Early August saw such attacks on multiple high-profile web services such as Youtube, Blogger, Twitter and Facebook, and unconfirmed reports from inside the targeted companies claimed that these thoroughly coordinated attacks were not blackmailing attempts, but rather focused on political reasons.

If these allegations were true, then warfare has moved to the cyberspace. If not, this means that cyber-criminals have reached such a level of organization and logistics that they are becoming unimaginable threats for both service providers and end-users. Either way, the war against cyber-crime has become much harder.

During the second half of 2009, malware authors have focused their efforts on boosting their revenue. Complex adware, banker Trojans and a wide range of rogue antivirus software have constantly targeted the average computer user.

Spam has also kept an ascending pace to a new threshold of 88.9 percent, 0.3 percent up from the first half of 2009. Health spam and phishing have been the most lucrative fields of activity, while education and OEM software unsolicited mail are also catching up.

Win32.Worm.Downadup has mostly disappeared from the collective memory after April 1st, but it is still one of the top three global e-threats. The BitDefender labs estimate that the number of computers infected with all variants of Downadup easily surpasses 7 million. The worm's persistence reveals the fact that most users still refuse to apply security fixes, even if they have been available for free.

Malware Spotlights

- International events such as Michael Jackson's death and the advent of the Swine Flu have been exploited to their full extent by malware authors in order to launch new infections.

- Trojan.Clicker.CM holds as number one e-threat for the second half of the year. It is used to force advertisements inside the users' browsers when visiting grey area websites (such as porn websites or services offering "warez" software. The alarming infection rate reveals the fact that malware authors are driven by profit and pay-per-click fraud is enough of a motivation to cyber-criminals.

- Distributed Denial-Of-Service attacks are becoming a trend among botnet masters, who now target both financial institutions and popular web services such as Blogger, Youtube, Facebook and Twitter. More importantly, the battle between cyber-criminals and legitimate service providers seems to have replaced its financial interests with political ones.

- Social networking platforms and instant messaging services, along with peer-to-peer networks are the favorite vectors for disseminating worms. The second half of 2009 saw the advent of Worm.P2p.Palevo.B, Trojan.Agent.Delf.RHO, Win32.Worm.Rimecud.C, as well as Win32.Worm.Koobface.ALX.

- Rogue antivirus software is on the rise, propelled by intense Black Hat SEO and taking advantage of users' lack of technical knowledge. During the second half of the year, rogue AV creators have pushed the legal boundaries even further by rigging their creations with a minimum amount of utility in order to avoid any consequences in the event of a lawsuit.

- Phishing messages have maintained their ascending pace foreseen in H1 2009, and is now ranking second right after medicine spam. Once again, attackers have focused on the spam areas that bring the best revenue in the shortest timeframe.

- Multiple system vulnerabilities have been discovered in Microsoft's products. The Redmond company has published six security bulletins, ranging from MS09-029 to MS09-035, and detailing flaws affecting Internet Explorer that could allow remote code to run on computers when users visited a specially crafted Web page. Strikingly enough, one of the vulnerabilities has been documented in 2008, but Microsoft failed to issue a fix.

- Adobe has also published no less than 12 vulnerabilities that could allow arbitrary code execution. These exploits mostly affected the Adobe Flash Player versions 9 and 10, as well as the Adobe Acrobat Reader.

- One of the most critical vulnerabilities discovered this year is the SMB 2.0 bug that affects all operating systems newer than Vista, except for Windows 7 RTM and Windows Server 2008 R2. However, the RC version of Windows 7 is.

Malware Threats in Review

Along with the already "traditional" Trojan.Clicker.CM infections, Win32.Worm.Downadup has been one of the most notorious e-threats for the past six months. Malware authors' choice of disseminating their e-threats remains the web, but Autorun-based techniques have rapidly gained ground. By default, every removable storage device features an autorun.ini script that instructs the computer which file to execute when the medium is plugged in, but malware authors frequently tamper with the file to make it launch miscellaneous malicious applications. Although extremely useful for non-technical computer users, the feature has been completely discarded in Windows Vista SP2 and Windows 7[1] in order to prevent infections.

World's Top 10 Malware

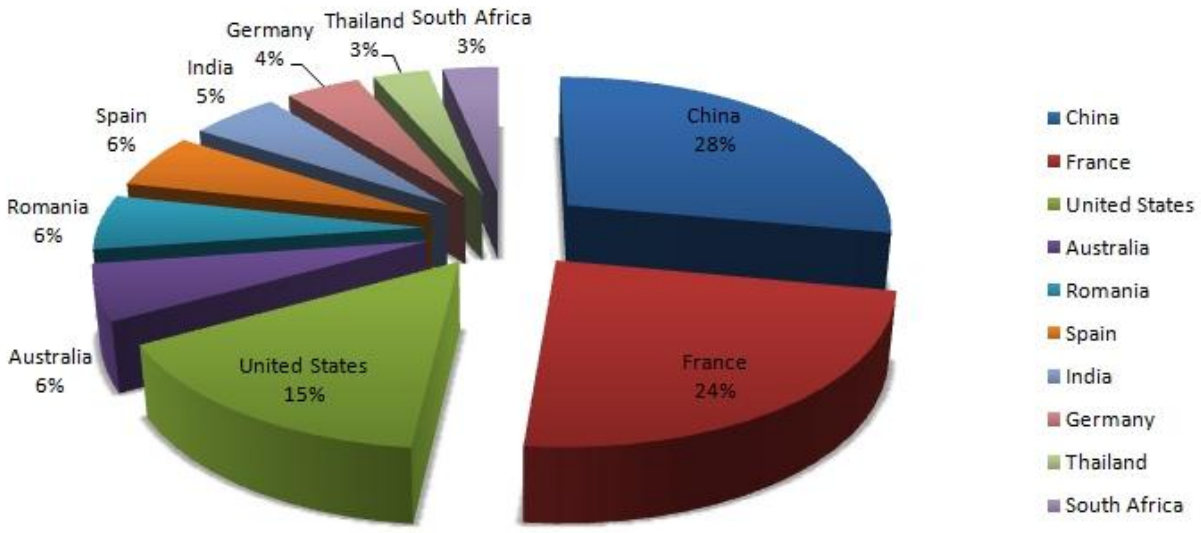


Figure 1: Malware breakdown by country

During the last six months the most active countries in terms of malware propagation were China, France and the United States, followed by Australia (up one place from H1 2009), Romania (also up one place) and Spain (down one place).

[1] In Windows 7 and Windows Server 2008 R2, only drives of type DRIVE_CDROM read and use the autorun.inf file. Moreover, users cannot override these policy settings via Registry tweaks.

July – December 2009		
01.	TROJAN.CLICKER.CM	8,97%
02.	Trojan.AutorunINF.Gen	8,41%
03.	TROJAN.WIMAD.GEN.1	4,41%
04.	Win32.Worm.Downadup.Gen	4,13%
05.	EXPLOIT.PDF-JS.GEN	3,39%
06.	Win32.Sality.OG	2,60%
07.	TROJAN.AUTORUN.AET	1,97%
08.	Worm.Autorun.VHG	1,59%
09.	TROJAN.JS.PYV	1,50%
10.	Exploit.SWF.Gen	1,47%
11.	Others	61,57%

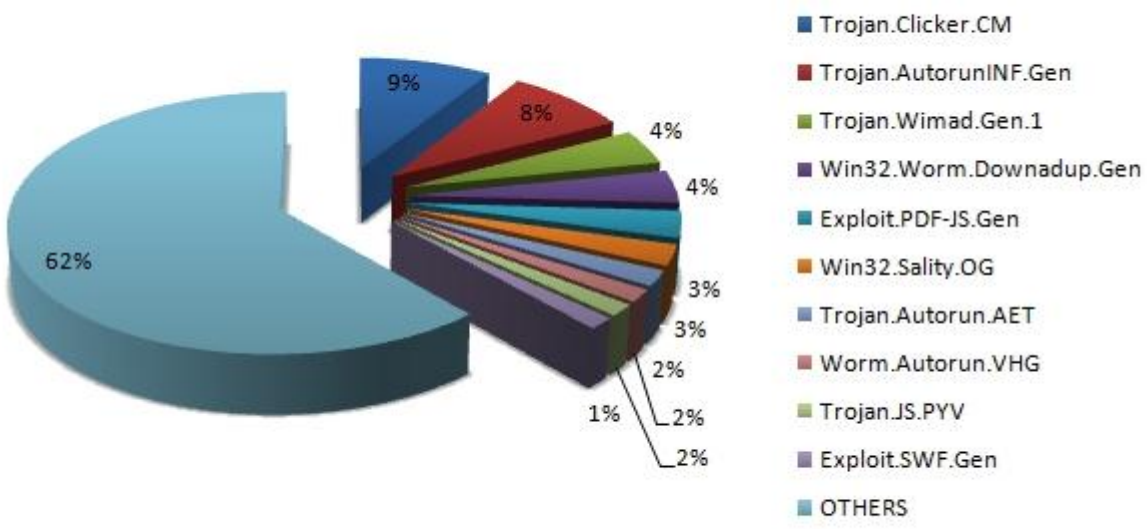


Figure 2: Top 10 malware threats for H1 2009

1. Trojan.Clicker.CM

The top e-threat on BitDefender's Top Ten list for the second half of 2009 is **Trojan.Clicker.CM**, which is mostly present on websites hosting illegal applications such as cracks, keygens and serial numbers for popular commercial software applications. It is mostly used to force advertisements inside the browser. Trojan.Clicker made up 8,97 percent of infected files.

2. Trojan.AutorunInf.Gen

Ranking second in the global infections top for H2 2009, **Trojan.AutorunInf.Gen** is a generic mechanism to spread malware via removable devices such as flash drives, memory cards or external

hard-disk drives. **Win32.Worm.Downadup** and **Win32.TDSS** are two of the most famous families of malware to use this approach to trigger newer infections.

3. Trojan.Wimad.Gen.1

Trojan.Wimad.Gen.1 takes the third place with 4,41 percent of the global infections triggered during the second half of the year. It mostly exploits the capability of ASF files to automatically download the appropriate codec from a remote location in order to deploy infected binary files on the host system. The ASF format is actually a container for storing data in either WMA (Windows Media Audio) or WMV (Windows Media Video) formats. Such WMV files are mostly distributed via illegal shares on Torrent websites. Malware distributors usually take advantage of the media hype around box-office move titles that haven't been released yet in order to rig their torrents with Trojan.Wimad. When played locally, the specially-crafted WMV file would allegedly attempt to download a "special codec", which is in fact a malicious binary hosted on a third-party website.

Figure 3: Torrent containing an infected WMV file. As of the date of writing, the Avatar movie hasn't been released yet.

4. Win32.Worm.Downadup

Ranking fourth in BitDefender's E-threat Landscape Report, **Win32.Worm.Downadup.Gen** is responsible for 4,13 percent of the global infections. The worm relies on the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (MS08-67) in order to spread on other computers in the local network and restricts users' access to Windows Update and security vendors' web pages. Newer variants of the worm also install rogue antivirus applications[2], among others.

5. Exploit.PDF-JS.Gen

Exploit.PDF-JS.Gen is a generic detection for specially crafted PDF files which exploit different vulnerabilities found in Adobe PDF Reader's Javascript engine in order to execute malicious code on user's computer. Upon opening an infected PDF file, a specially crafted Javascript code triggers the download of malicious binaries from remote locations. The threat ranks fifth with 3.39 percent of the global infections.

[2] For a full report on Win32.Worm.Downadup and its evolution during 2009, please visit BitDefender's special whitepaper at http://www.bitdefender.com/files/Main/file/Conficker_-_One_Year_After_-_Whitepaper.pdf

6. Win32.Sality.OG

This family of polymorphic file-infectors ranks sixth in the E-threats report for H2 2009 with more than 2.60 percent of the global infections. In order to spread itself, the virus appends its encrypted code to executable files (.exe and .scr binaries). The virus also features a rootkit component that is subsequently deployed on the infected machine to conceal the infection. What's particularly important about Win32.Sality.OG is the fact that it uses a list of keywords to find and stop processes and services associated with antivirus or monitoring applications.

7. Trojan.Autorun.AET

The seventh place goes to **Trojan.Autorun.AET**, a malicious code spreading via the Windows shared folders, as well as through removable storage devices. The Trojan exploits the Autorun feature implemented in Windows for automatically launching applications when an infected storage device is plugged in. The e-threat is accountable for 1.97 percent of the global infections.

8. Worm.Autorun.VHG

Worm.Autorun.VHG is an Internet /network worm that exploits the Windows MS08-067 vulnerability in order to execute itself remotely using a specially crafted RPC (remote procedure call) package (an approach also used by **Win32.Worm.Downadup**). The worm ranks eight with 1,59 percent of the global infections.

9. Trojan.JS.PYV

The ninth place in the malware top for the first half of 2009 is taken by **Trojan. JS.PYV**, a malicious script affecting users who are browsing malware-distributing websites, or legitimate websites which had been compromised by attackers. Infected websites feature an invisible iframe window able to execute code from a remote location. Its presence in the Top 10 international e-threats reveals the fact that a large number of legitimate websites have been compromised without webmasters even realizing it.

10. Exploit.SWF.Gen

Ranking last in the H2 malware top, Exploit.SWF.Gen is a generic detection for a family of specially-crafted Adobe Flash files that allow the execution of a remote file by exploiting a vulnerability in the Adobe Flash Player. By using a malformed SWF record value, the attacker can force the application into a buffer overflow condition (a download and execute shellcode). This exploit usually downloads and installs password-stealing Trojans.

The Rise of Botnets

Botnets (also called “Zombie Networks”) are networks of compromised personal computers that can be controlled remotely to act as one, extremely powerful, system. In order to gain control over a machine, the attacker has to trick the user into installing a remote access tool (usually a Trojan horse with backdoor capabilities). After a successful infection, cyber-criminals are able to remotely access and control the infected computer, without users’ consent or interaction.

Botnets can be put to a variety of illegal uses, ranging from sending spam to performing distributed denial-of-service or even massive data theft. Since their lucrative potential is practically unlimited, they are regarded as assets and treated accordingly: botnets can be sold, lent or even used as tools for “in-house” projects.

As described in the chart below, the most active families of bots are Rustock, Ozdok[3] and Kobcka, all three equipped with rootkit functionality to allow them run undetected. They are mainly responsible for the huge amount of pharmacy spam, among others.

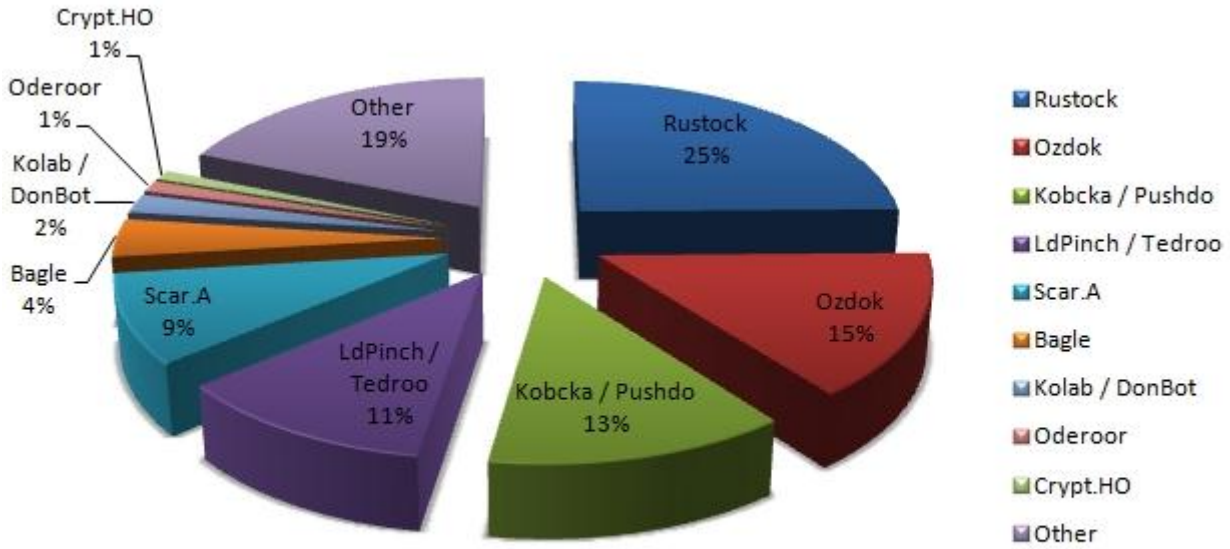


Figure 4: Botnet activity by bot family

[3] The Ozdok botnet managed to surpass the Storm zombie network, but a coordinated effort involving law-enforcement authorities and ISPs put an end to it as of early November.

Web 2.0 Malware

Because of their wide popularity among computer users and the amount of personal information stored, social networking platforms have become the favorite hunting place for malware authors. As of the moment of writing, Facebook has just celebrated 350 million accounts, each of them containing personal information, or at least the groundwork for initiating a spear-phishing attack. Instant messaging platforms have also become one of the favorite vectors of disseminating malware: multiple families of worms rely on users' unawareness to trick them into following links to infected applications.

Spam and phishing

As one of the largest social networks connecting people around the globe, Facebook has been successfully used to lure users into disclosing their credentials for a long time. The phishing mechanism is simple, yet efficient: the victims usually receive a spam message announcing updates in Facebook's Terms of Use or even an alleged account lockdown due to suspicious activity. In order to re-activate their account, the user has to follow an embedded link and log-in to the platform. As soon as they press the Login button, their authentication credentials are sent to an unauthorized third party via a PHP script. The collected accounts will be used to trigger worm infections or to collect data for other phishing attempts.

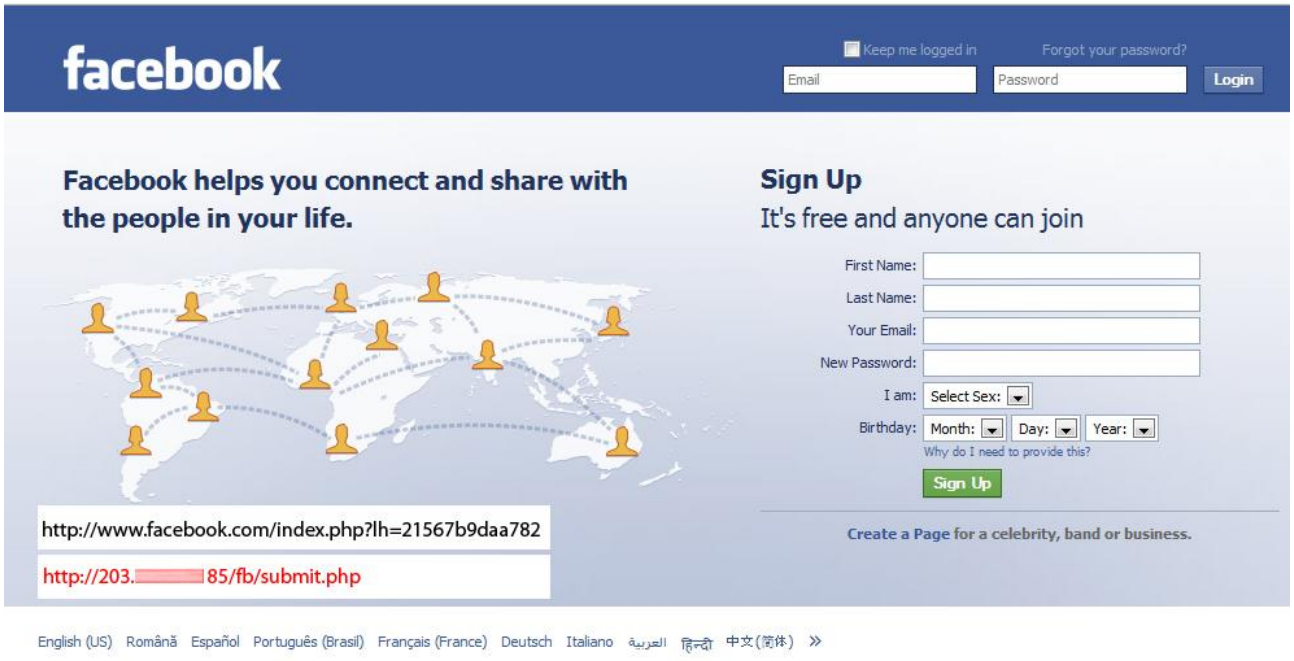


Figure 5: Facebook phishing page

Spamming is also a common practice among social networking service users. While Twitter and Facebook have imposed strict policies on spamming, some other social network services have barely taken into account this possibility. For instance professional network LinkedIn has become the favorite playground for people and organizations offering miscellaneous services. Spammers attempt to join users' professional networks and then bomb them with messages advertising their products or services. The message below depicts a job offering from a communication agency. It is written in Romanian and can be considered spam because it tries to sell communication services to employees of multiple Romanian companies, despite the fact that LinkedIn specifically asks its users not to contact people who they do not know, either directly or indirectly. During the past six months, BitDefender has identified multiple variations of LinkedIn spam - a warning sign showing that the precarious state of the global economy pushes more and more providers into abusively marketing their services via social networks.

Figure 6: LinkedIn contact request to offer services

Worms and Bots

While spam and phishing sum up almost 80 percent of the e-threats related to social networks, worms exploiting large platforms have rapidly escalated. During the last six months of 2009, numerous families of worms have been pestering the most important social networks such as Twitter, MySpace and Facebook.

Initially spotted on August 2008, the Koobface worm has been one of the most active and destructive e-threats affecting social networking platforms. The cyber-criminal team behind the worm has released multiple variants of it in order to extend their reach with multiple social networking services[4].

The viral infections took most of the platforms by surprise and the damage inflicted to users was beyond imagination[5]. The infection technique was simple yet efficient: the worm used compromised accounts to lure friends into clicking the infected links.

[4] The worm has been initially designed for Facebook, but subsequent variants of Win32.Worm.Facebook.A also targeted MySpace and Twitter accounts. BitDefender was the first security vendor to alert and issue protection for all variants of Koobface. For further details on Win32.Worm.Koobface.A, please visit the worm's description at http://www.bitdefender.com/VIRUS-1000362-en--Win32.Worm.KoobFace.A.html

[5] Win32.Worm.Koobface.ALX features a rootkit component that can disable some of the commercially-available antivirus utilities and could export sensitive data (e-banking credentials and IM passwords) to a remote location.

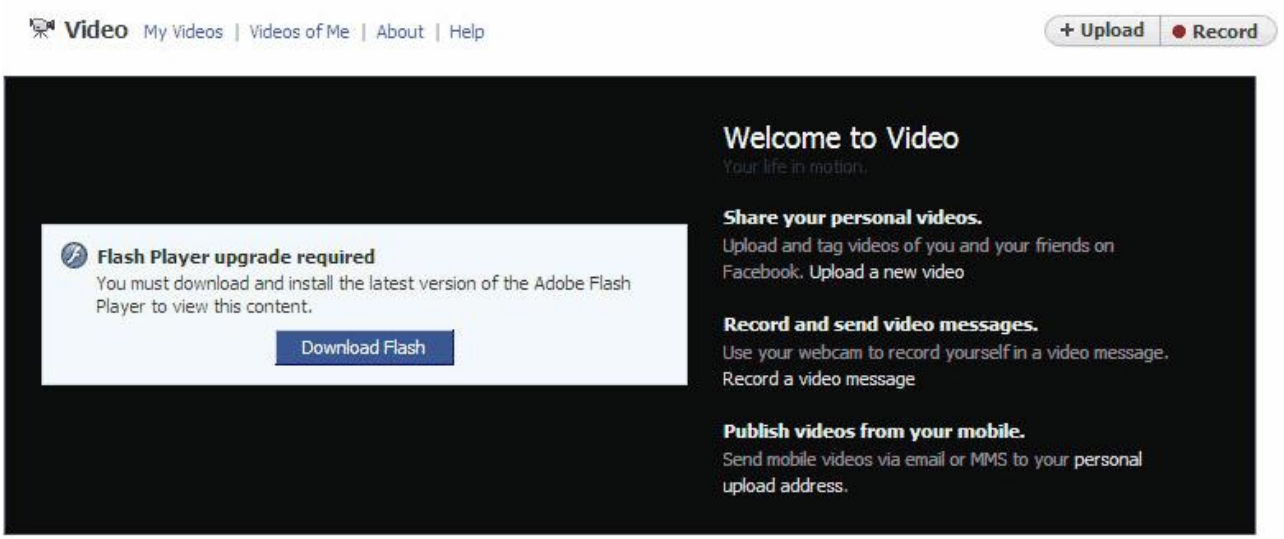


Figure 7: The Koobface worm impersonating a Flash Player update

Other Facebook worms blend social engineering with highly-advanced URL manipulations resulting in a cross-site request forgery in order to submit their message every time the user clicks on an infected link. These specific Cross-Site-Request Forgery attacks (also known as XSRF) are based on iframes running third-party scripts to manipulate Facebook into behaving as if the account user had sent a wall post.

Fortunately, the worm had no malicious payload and did not affect unwary users other than the obvious embarrassment caused by the picture below.

Figure 8: Cross-Site Request Forgery worm on Facebook

Instant Messaging services have also been thoroughly exploited by malware authors due to their popularity with computer users. Skype may have had its rough times with IM worms since early 2008, but, as of the moment of writing, the targeted IM services are now Yahoo Messenger and MSN Messenger.

Initially spotted in late June this year, Worm.P2P.Palevo.B is an extremely aggressive e-threat primarily aiming at peer-to-peer service users. One of the first symptoms of infection is increased network activity on UDP ports originating from explorer.exe and the presence of a hidden file called sysdate.exe inside the "%systemdrive%\RECYCLER\S-1-5-21-[random groups of digits]" folder.

The worm has been designed in a manner to allow it to spread via multiple channels. It can add its code to the list of P2P shares on popular file-sharing applications such as Ares, BearShare, iMesh, Shareza, Kazaa, DC++, eMule and LimeWire, but it would also infect any removable USB device plugged into an already-infected machine or even network drives mapped locally.

Worm.P2P.Palevo.B is also able to send links to infected websites if it detects the presence of MSN Messenger on the compromised system, thus luring unwary contacts into installing the worm from a remote location.

The worm does not limit its destructive habits to infecting other hosts and leaving the user with a barely usable system because of its increased activity. It is also able to intercept passwords and other sensitive data entered in Mozilla Firefox and Microsoft Internet Explorer web browsers, which makes it extremely risky to users relying on e-banking or online shopping services.

Worm.P2P.Palevo.B features a backdoor component that allows remote attackers to seize control over the infected machine and manipulate it according to their own needs (for instance, to install additional software, to export locally saved documents, to manipulate online voting from various IPs, or even to launch TCP/UDP flood attacks against Internet servers).

Another aggressive Trojan horse exploiting Yahoo Messenger is Trojan.Agent.Delf.RHO, a piece of malware that spreads via links sent as instant messages on the behalf of other infected users. In order to trick the user into accessing the malicious links, the Trojan places them in a valid context. For instance, some messages warn the victim that he / she is infected and should immediately download a cleaning utility via the provided link, while others advertise an invisible / ignore contact scanner. Trojan.Agent.Delf.RHO seems to have its roots in Romania, since the messages it sends are written in Romanian.

The link takes the user to a web site or blog containing an embedded movie that requests the user to download a codec, which turns to be the Trojan itself. Upon execution, the setup file installs the following files: *%WINDIR%\system32\yahooui.exe, %WINDIR%\system32\yahooauth2.dll, %WINDIR%\system32\ssleay32.dll, and %WINDIR%\system32\libeay32.dll.*

The Trojan would wait for the user to sign into their account and then would start sending spam messages to the contacts in the user's list.

Trojan.Agent.Delf.RHO is more than meets the eye: apart from being annoying, it also invites other friends to its party, such as the extremely dangerous **Trojan.Spy.Banker.ACFQ**, which tries to trick the user into accessing phishing sites targeting e-banking services.

Spam Threats in Review

During the second half of 2009, the spam landscape has remained relatively unchanged, with Canadian Pharmacy positioned as top worldwide spammer. Most of the messages advertised sexual enhancement products such as alternative replacements for Cialis, Viagra and Levitra. This is an extremely lucrative field of spam, mostly because the products ordered via Canadian Pharmacy webshops never make it to the customer, which is often too ashamed to report these issues to the authorities. More than that, these online payments are extremely risky, since the spammer has access to the used credit card details and can draw any amount of money at will.

Spam Distribution by Territory

The most active countries in terms of spam are presented in the chart below.

Spam distribution by point of origin
July – December 2009

	Spam Percentage
United States	27
Vietnam	9.63
Korea	5.77
China	5.28
Brazil	4.91
Colombia	4.1
Russia	3.9
Argentina	3
Spain	2.7
Poland	0.5
Others	33.21

While the United States of America and Vietnam account for one third of the worldwide-distributed messages, Argentina, Spain and Poland rank last with almost 6 percent. Russia has witnessed a minor decrease as compared to the first half of the year (from 4.2 to 3.9 percent), probably because of the ISPs initiatives' of containing the botnet activities and shutting down the illegal mail servers activation on inside their territory.

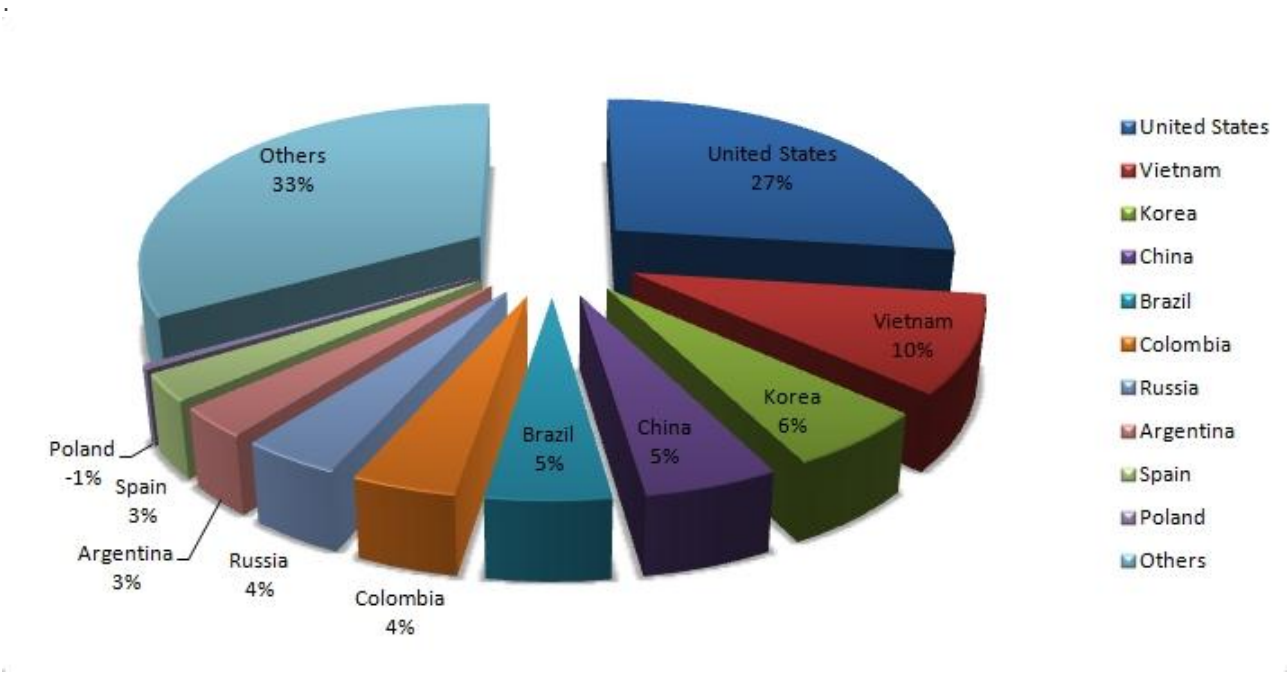
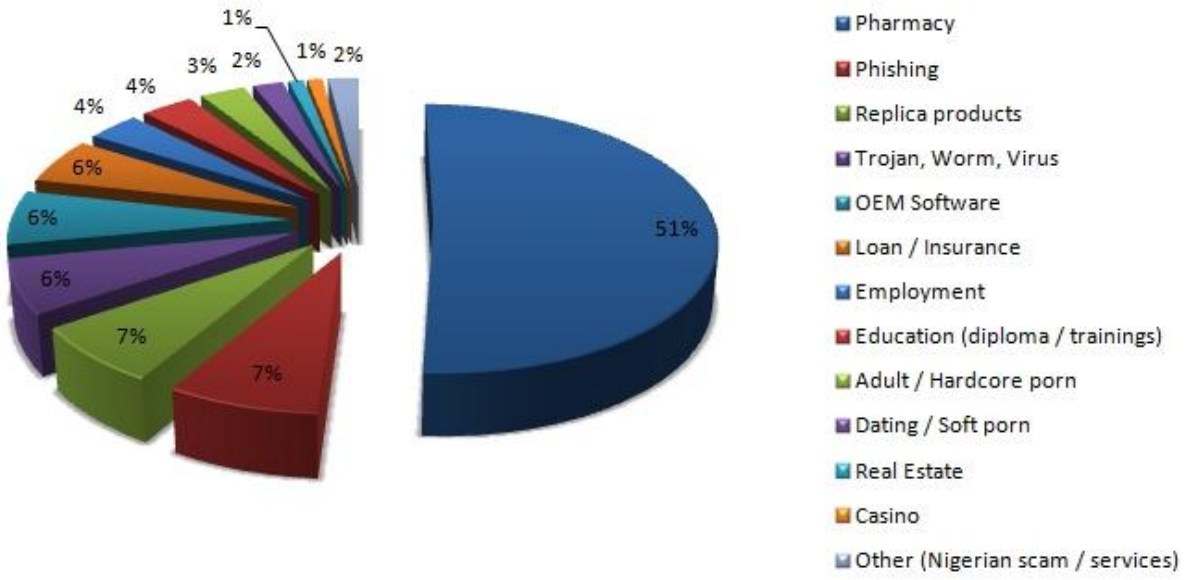


Figure 9: Spam distribution by territory

Spam Breakdown by Type

The BitDefender Antispam labs estimate that the most advertised products during the past six months of 2009 are Canadian Pharmacy offerings with a total of 51 percent of the worldwide sent spam. Phishing attempts sent via email have kept the same trend seen in the first part of the year, although the targeted institutions have slightly changed.



Replica products rank third for the six-month period, but the amount of messages advertising knock-off products rapidly escalates around holidays, when users are more likely to purchase them as presents.

Malware-attached spam accounts for 6 percent of the total amount of unsolicited mail. While figures have remained the same as in H1 2009, the attachments sent during H2 2009 have dramatically changed, as described in the next chapter.

Spam Trends

Spam messages account for 88.9 percent of the total amount of electronic messages sent worldwide. Text-based messages are the most frequently encountered form of spam, while image-based spam is extremely rare, with only 2.3 – 2.5 percent. The average size of a spam message is 3.5 Kb, although their size usually varies from 2 Kb to 9 Kb, depending on the approach.

During this semester, spammers have especially exploited international or national media events to lure their victims into opening the messages. One of the most important spam campaigns was launched after the controversial death of pop-star Michael Jackson. Back in July, BitDefender identified multiple spam waves allegedly offering more info on Michael Jackson's unknown killer, but actually carrying sexual enhancement drug ads and malware[6].

Figure 10: Malware-bundled spam message exploiting the death of Michael Jackson

In this case, the attached file is a variant of Trojan.Spy.Zbot.UI, which, once installed, adds the compromised computer to the Zeus Botnet, and then transforms it into a spam relay, sending hundreds of messages without the users' knowledge or consent and eating up valuable computing resources.

[6] For more info on how Michael Jackson's death was exploited by malware authors and spammers, please visit http://www.malwarecity.com/blog/michael-jacksons-unknown-killer-481.html.

Samantha Geimer's abuse and Roman Polanski's arrest in September was yet another opportunity for e-crooks to spam their products and to push rogue antivirus in the spotlight. In order to lure users into visiting their malicious websites, spammers have not only sent millions of mail messages, but they have also used thoroughly optimized (BlackSEO) websites to disseminate rogue AV software.

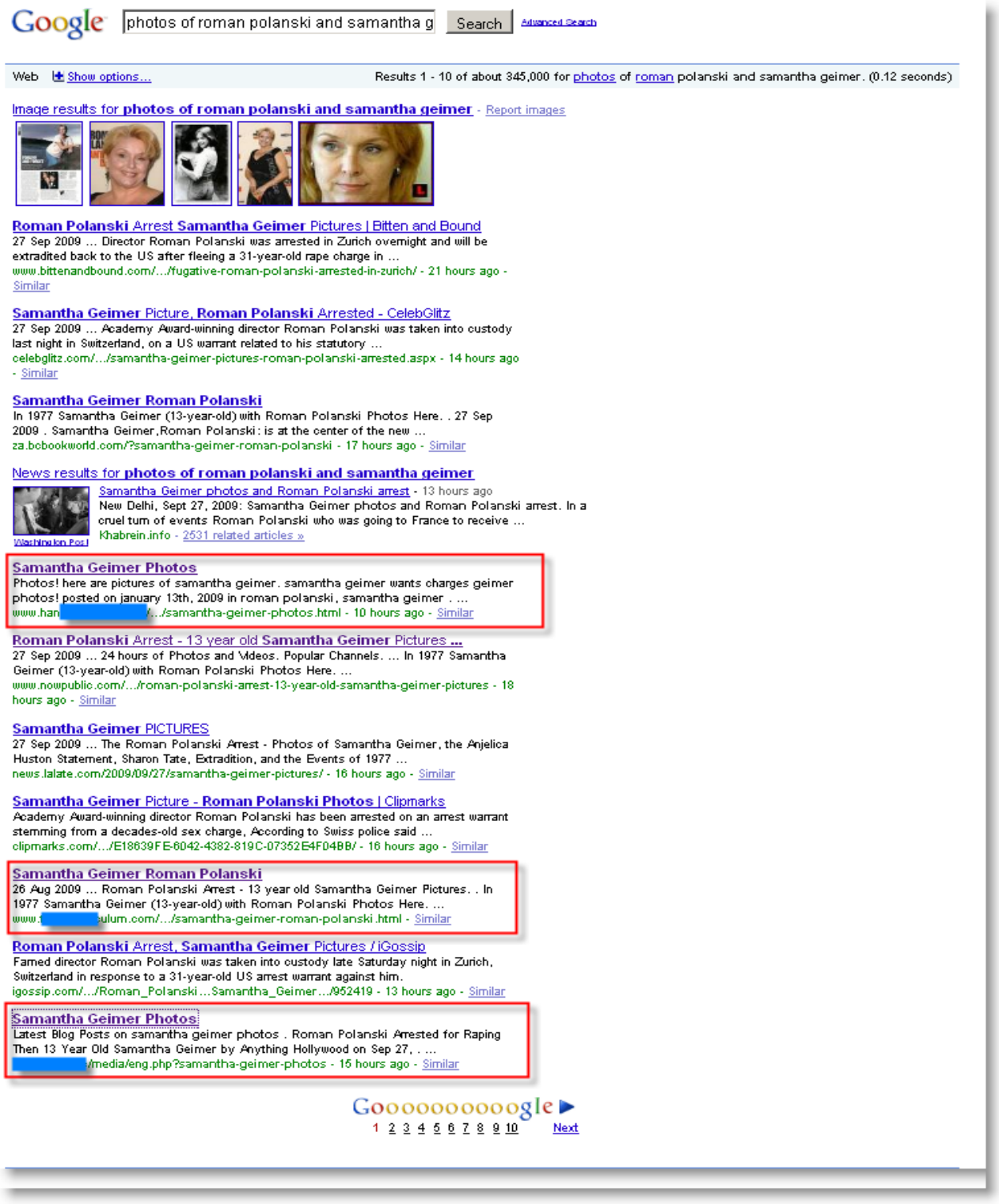


Figure 11Malicious web pages optimized for these keywords

When clicked, the links automatically redirect the browser towards several Web sites registered on .cn domains holding the newest member of the rogue family - **Total Security Rogue**, detected by BitDefender as Trojan.FakeAV.SQ.

Phishing and Identity Theft

Compared to the first half of 2009, the amount of phishing messages has remained relatively unchanged, although phishers have switched their focus to institutions that could bring them the most of profit in the shortest timeframe.

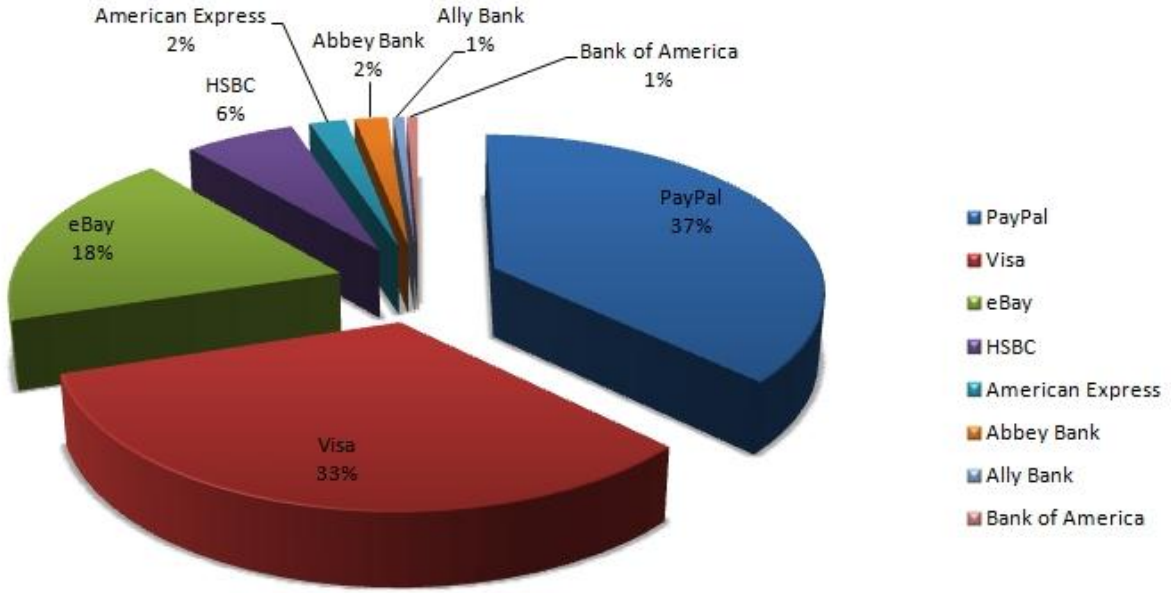


Figure 12: Top phished institutions during H2 2009

As seen in the image above, phishers' primary targets are PayPal, Visa and eBay, followed by HSBC, America Express and Abbey Bank. Ally Bank and Bank of America rank last with a little over one percent of the total amount of phishing messages.

These messages mostly target English-speaking computer users who are using the services of at least one of the institutions mentioned in the top.

For instance, eBay customers were face with a medium-sized phishing campaign that asked them to fill in a new mandatory "confirmation form", by clicking the link provided in the spam message. Unwary users following these links were presented with a form that had nothing to do with eBay, but instead collected sensitive personal and financial information that could be used for credit-card fraud or even identity theft.

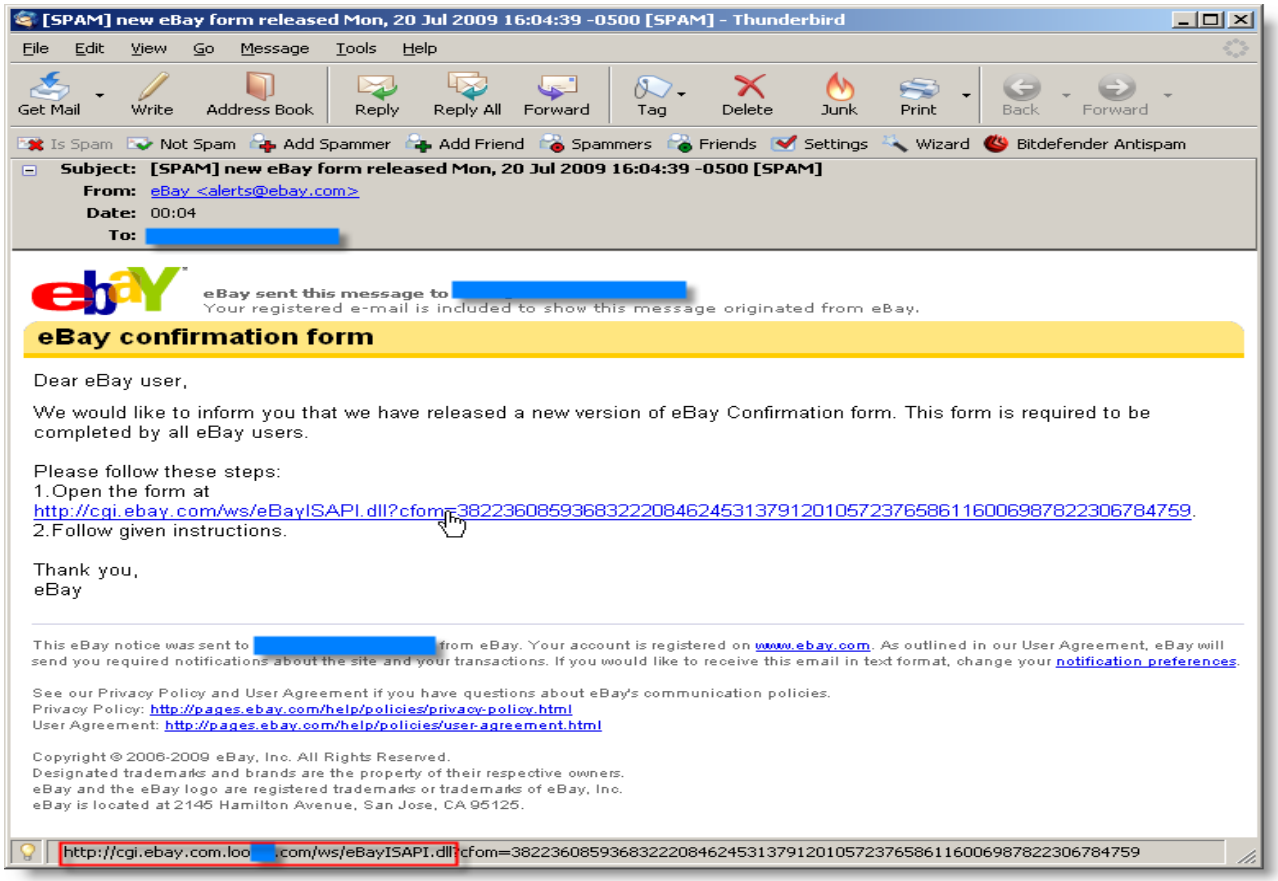
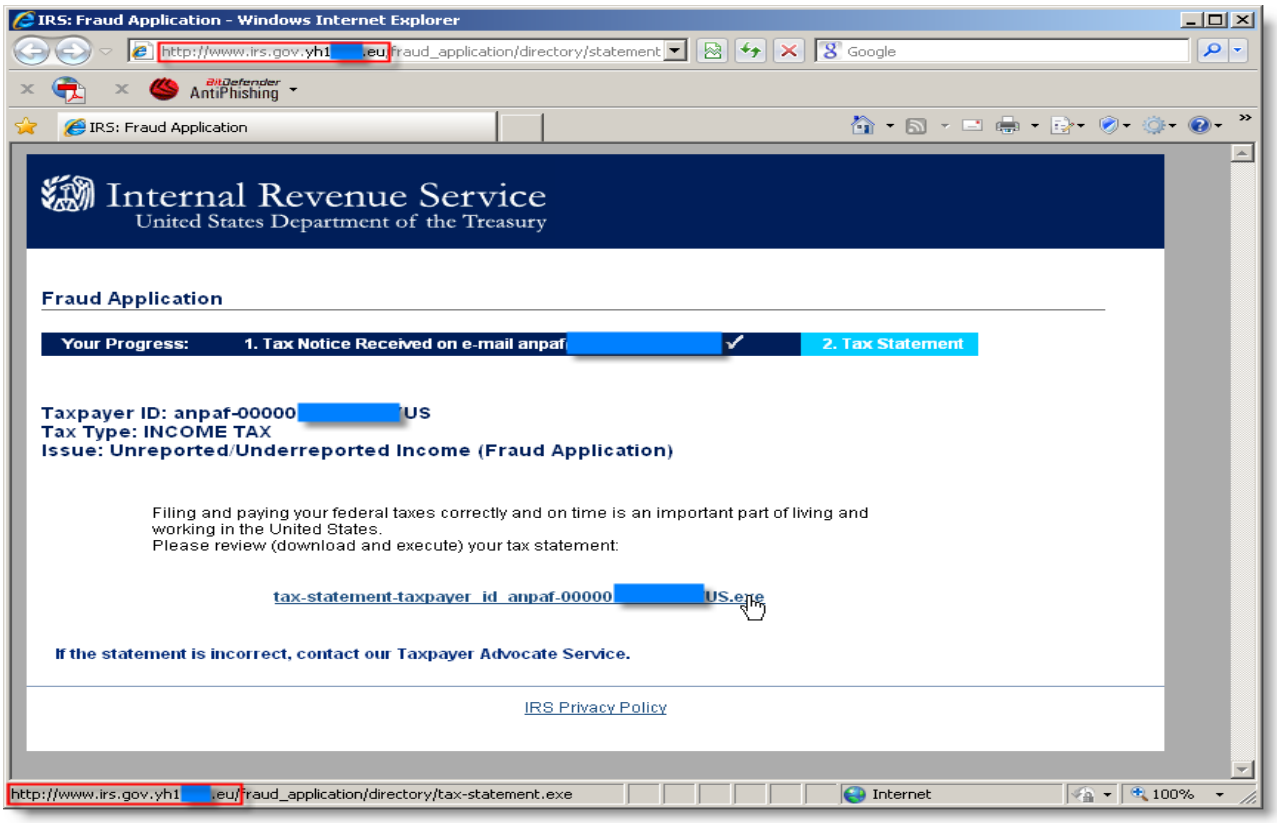


Figure 13: Phishing message targeting eBay users

September 15th was another highly-anticipated event by spammers, given the fact that US taxpayers were supposed to file their 2008 tax return. The spam message used as bait requires the taxpayers to review their unreported or underreported income statement, providing them with an alleged customized link towards the IRS Web site.

The link does not lead to the agency portal, but to a Web page (registered on an .eu domain) that mimics an on-line form, employing several visual identification components of the original IRS Web site (namely the logo and the general formatting elements).

The page also provides a link of a purported tax statement that the user should download and execute. However, upon clicking the user does not download an e-form, but receives a malicious payload that BitDefender detects as Trojan.Generic.2436384, which is, in effect, another variant of the infamous ZBot.



Vulnerabilities, Exploits & Security Breaches

Although they are not the main vector for disseminating malware, vulnerabilities and exploits play a significant role in successfully compromising IT infrastructure for financial gains. During the first half of 2009, the most important e-threats were related to the emergence and proliferation of the Downadup worm, which exploited the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (MS08-67) in order to spread on other computers in the local network. The successful demonstration of MD5 collision attacks in early January has also raised multiple questions on the data security and methods of authentication on the web.

SSL Vulnerabilities and Website Impersonation

In early July, two independent researchers have uncovered a serious set of vulnerabilities in the implementation of the SSL protocol that would allow an attacker to impersonate any SSL-protected website and successfully carry out the perfect phishing attack.

According to the researchers' findings, the vulnerability occurs in the way the SSL technology has been implemented in all the commercially-available browsers on the market. These certificates sometime are the ultimate security element that ensures the user they have landed on the right webpage. They are available for purchase through Certificate Authorities (CAs) such as VeriSign and Thawte. Upon requesting a SSL certificate for a top-level domain, the Certificate Authority contacts back the domain owner at the specified e-mail address in the Whois database in order to confirm ownership.

However, if an attacker successfully registers a domain and then asks for a certificate, he could subsequently apply for a certificate for a subdomain of his or her site, such as bankofamerica\0.somesite.com, by simply using the null character '\0'. Given the fact that he legitimately owns the root domain, the CA will issue the certificate even if the subdomain contains trademark names such as BankOfAmerica.

The newly-found vulnerability in the SSL implementation within commercial browsers documents the fact that they would read the attacker's certificate as if it were issued for BankOfAmerica. This condition occurs as browsers would automatically stop reading the characters that follow the special null-char ('\0') in the name.

Other Software Vulnerabilities

During July, software vendor Microsoft has published no less than six security bulletins, ranging from MS09-029 to MS09-035, and detailing flaws affecting Internet Explorer that could allow remote code to run on computers when users visited a specially crafted Web page. Given the severity of the bug, Microsoft has published two subsequent updates, namely the MS09-34 and MS09-035 to take care of the vulnerabilities in the Active Template Library.

July also saw vulnerabilities in multiple software applications from other vendors. For instance, Adobe released a security bulletin addressing no less than 12 remotely exploitable vulnerabilities in software applications such as Adobe Flash Player versions 9 and 10, as well as Adobe Reader.

One month later, in August, Java's Virtual Machine was slammed with the CVE- 2009-2675 vulnerability that allowed remote code execution from a specially-crafted malicious website. August also brought more fixes for Adobe's Flash Player, many of which were dealing with arbitrary code execution. However, the most spectacular vulnerability is the SMB 2.0 bug that affects all operating systems newer than Vista, except for Windows 7 RTM and Windows Server 2008 R2. SMB 2.0 is the newest iteration of the protocol used for sharing files and printers across a network. Although Windows 7 is immune to the bug, the Release Candidate of the new operating system from Microsoft is.

Predicting Next Year's E-Threats

Year 2009 witnessed a wide range of security threats aiming at both end-users and at corporate networks. The Downadup worm (also known as Conficker or Kido) took a dramatic surge and managed to stay one of the top three global –threats during 2009. Although not entirely dangerous (as variants A, B and C had no malicious payload), its spreading mechanisms and its resistance to detection may be regarded as the cornerstone of the upcoming breeds of highly-destructive malware.

Botnet activity

Botnets are the core of most of the businesses involving malware. They are relatively easy to maintain and they provide a criminal organization with unimagined computing power for multiple purposes, such as sending spam, performing distributed denial-of-service attacks or pay-per-click revenue abuse.

- Spam sent by botnets will keep their ascending pace we witnessed in 2009
- Distributed denial-of-service attacks will also increase, as more and more Internet users switch from cable modems to high-speed Internet connections such as optical fibre or broadband wireless. The attackers will mostly focus on financial institutions, web-based casinos or large companies to force them pay amounts of money in exchange of "protection". Some of the upcoming DDOS attacks will only serve as a demonstration of power for potential botnet customers.

Malicious applications

The vast majority of malicious applications are oriented towards illicit financial gains. BitDefender estimates that the next year will bring an increased amount of malware, especially of adware applications and rogue antivirus software. More complex malware, such as rootkit-based file infectors and worms relying on multiple vectors of infection (e-mail, instant messaging and peer-to-peer protocols), are also expected.

Social networking

Building on their experience with Facebook and Twitter, malware authors are expected to extend their reach with the new Google Wave, as the search engine's instant messaging service gains popularity. Facebook and Twitter will also stay in attackers' crosshair, given the fact that Facebook has surpassed 350 million users. Spam and phishing attempts targeting social networking users are also expected to rise.

Apart from the fact that social networking websites are expected to become one of the most important vectors of infection, they are also likely to trigger other security incidents such as involuntary public disclosure of sensitive information.

Operating systems

Microsoft's newly-launched operating system Windows 7 has proved to be much safer than its predecessors. However, as users transition from XP and Vista to Windows 7, malware authors will focus on finding software vulnerabilities and security breaches in the operating system.

Apple Mac OS X users should also consider adopting an anti-malware suite in order to avoid trouble. Apart from the usual spam and phishing attempts that are platform-independent and target any computer user connected to the Internet, Apple's transition to the Intel hardware platform will unleash new opportunities for attackers that are currently writing malware for Windows.

Mobile operating systems

The latest iteration of iPhone (the 3GS family) dramatically increased the iPhone user-base, and many of them have decided to jail-break the operating system in order to install third-party applications. Jail-breaking involves activation of the SSH service with a default password and root access. BitDefender expects that 2010 will bring new e-threats focusing on the rapidly-growing mobile platform, especially worms and password-stealing Trojans.

On the contrary, Android and Maemo users will be spared. Given the fact that their market share is still insignificant as compared to Windows Mobile, Symbian and iPhone OS, malware authors will not focus their efforts on finding vulnerabilities, but rather strengthen their efforts on social engineering attacks.

Enterprise threats

Microsoft's Windows Server 2008 R2 Hyper-V and the VMWare vSphere virtualization technologies have opened new opportunities for small and medium businesses. Accommodating multiple servers to a single machine with virtualization will dramatically contribute to cutting down on costs. During 2010, remote attackers are expected to look for vulnerabilities in software that would allow them to seize control over the hypervisor and, implicitly, on all the virtual machines deployed on the system.

Cloud computing services are also living their heyday. No matter whether they are used for e-mailing (such as Google' Gmail service) or for data storage and backup, the cloud technologies hold and process significant amounts of sensitive data. It is just a matter of time until attackers shift their focus on these infrastructures to seize control over or limit access to these cloud resources.

Netbooks and PDAs will slowly become security risks in corporate environments as their adoption ramps off. These intelligent devices are extremely small; in fact, they are so small that can be easily lost or snatched by a thief. If their physical value is sometimes negligible, the data stored on the local solid-state drive is priceless. Since netbooks do not come with Trusted Platform Modules or other types of hardware / software encryption and cannot be managed remotely (in order to wipe the storage medium clean in case of loss/theft), sensitive information may land into the wrong hands.

Table of Figures