H1 2009 Malware and Spam Review

MALWARE AND SPAM TRENDS

bitdefender

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

Matei-Răzvan STOICA, Communication Specialist – Vulnerabilities and Exploits

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

Dan VANDACHIEVICI, Spam Analyst

Table of Contents

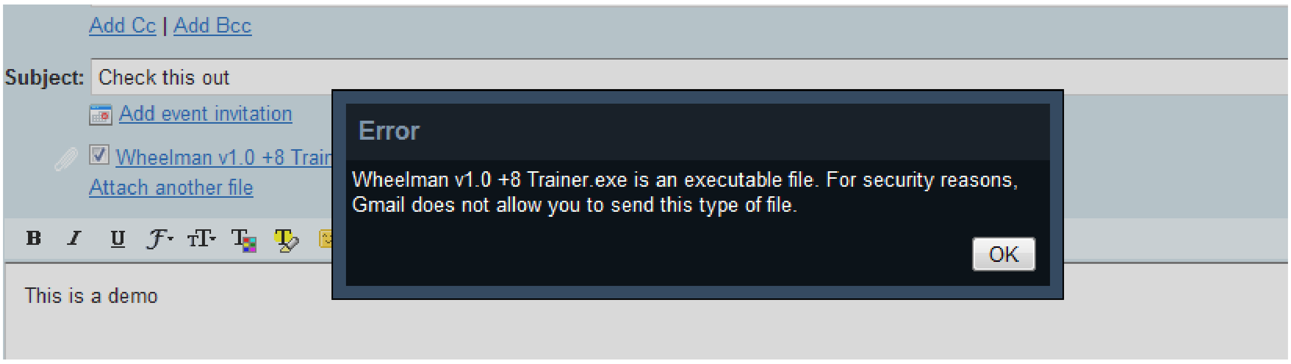
Overview

The Internet has undoubtedly become one of the most important means of communication, regardless whether it is used for business, academia or for past-time activities. However, the Internet is not only responsible for moving massive amounts of data, but is also an important vector for real money: e-banking services, stocks, electronic retail commerce and targeted advertising, all joined in one place and available at the user's fingertip.

Malware has long since ceased to be the source of pranks and innocent practical jokes exchanged between tech-savvy computer users. Writing malware has become a fully-fledged business shaped after corporate models, but run by cyber-criminals. Their sole purpose is to get between end-users and their financial assets or their intellectual property they manipulate / exchange or store via web services.

Contrary to popular belief, electronic threats are no longer exclusively related to Microsoft's Windows operating systems. While it may be true that attackers mostly focus on Windows boxes simply because they enjoy the largest market share, these cyber-criminals are also experimenting with Apple Mac OS X and mobile platforms such as the iPhone.

Most of the cyber-attacks are carried via web, rather than through e-mail messaging. Given the fact that Internet service providers and corporations have taken the appropriate measures to scan incoming and outgoing e-mail messages, as well as to restrict attachment formats to non-executable files only, malware authors are now mostly concerned with infecting trustworthy, high-traffic websites then wait for unwary users to take the bait.



Subject: Check this out

☑ Wheelman v1.0 +8 Trair

Error

Wheelman v1.0 +8 Trainer.exe is an executable file. For security reasons, Gmail does not allow you to send this type of file.

This is a demo

Malware Spotlights

- MS08-067 Worm — the Downadup / Conficker / Kido worm infected about 11 million computers worldwide during the first half of 2009. The infection is still in the wild, with hundreds of systems compromised on a daily basis.

- 88.3 percent of the worldwide electronic mail is spam. Image-based spam accounts for 3.9 percent, while the average size per message is 4.8 KB.

- Mac OS X platforms are still secure compared to Windows, but the number of phishing attempts, some flavors of scareware and the appearance of a fully-fledged Trojan horse pave the way to Mac OS X malware.

- Most of the worldwide spam is advertising prescription-based drugs with Canadian Pharmacy taking leadership as number one spammer.

- One of the most abused brands in spam is the WebMD online business, whose newsletters have been forged to display Canadian Pharmacy ads. Fake MSN newsletters ranks second in the brand abuse top.

- Phishing attacks witnessed a dramatic boost, with US-based money institutions in the hackers' crosshairs.

- ATM malware spotted in the wild: Trojan.Skimer.A targets automated teller machines from US manufacturer Diebold. The malicious application creates a virtual 'skimmer' which is capable of recording card details and personal identification numbers without the user's knowledge.

- Fake disinfection tools for the Downadup Internet worm: building on the pandemics triggered by the Downadup worm (about 11 million infections to date), malware authors released fake disinfection tools for the worm that actually would drop miscellaneous malicious files, especially rogue security software.

- Leaked copies of Microsoft's upcoming operating system, Windows 7, as well as a technical preview of the Microsoft Office 2010 suite have emerged on torrent websites. However, many of the distributed images have been modified to install miscellaneous variants of malware along with the genuine Microsoft files. Given their public appeal, many users have fallen victim to their curiosity.

- The first Windows 7 proof-of-concept rootkit (VBootkit) has been released under GPL license.

Malware Threats in Review

During the first six months of 2009, malware writers have continued their constant preoccupation to infecting users' systems to get either direct financial gains or to seize control over these machines. Trojan-type malware kept its ascending pace, accounting for more than 83 percent of the global malware detected in the wild.

Downadup and MS08-067

Although Trojans have been by far the most active family of e-threats, the largest damage caused to users this year was inflicted by an Internet worm - the notorious Downadup. The advent of this brand-new e-threat marked not only the comeback of worms in modern operating systems, but also shifted an entire philosophy. While most of the malware is being written for criminal purposes such as goods and assets theft (e-banking, online games and stock exchange) or for computing resources (the botnet approach), the Downadup worm actually had no payload. Shortly put, it did nothing.

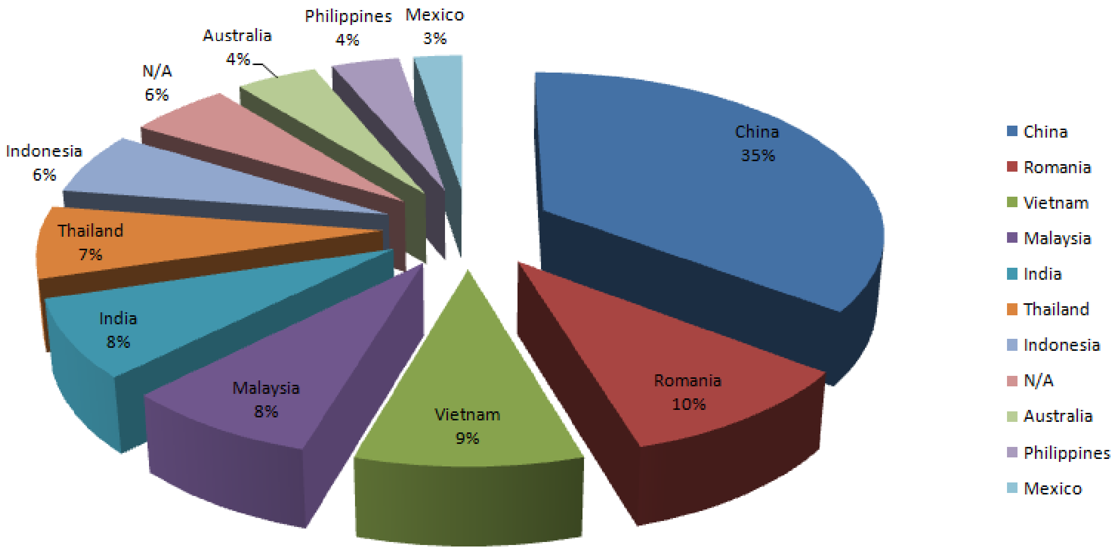


Figure 1: Downadup Infection - Breakdown by Country

Unlike other similar threats that caused havoc a couple of years ago (Code Red, Melissa and Nimda), the brand-new Downadup has been carefully crafted in order to deter detection and removal from the infected machine, Server-side polymorphism and Access Control List (ACL) modifications are only some of the novel features implemented by the group of professional cyber-criminals that wrote it.

In order to spread across networks, the worm exploits the MS08-067 vulnerability in the Windows Server service, but it is also able to spread via infected USB drives using an autorun feature. Once it has successfully infected a system, the worm attempts to crack local passwords to access network shares. Most importantly, if an administrative account is compromised, Downadup uses the Windows Task Scheduler service[1] to spread itself to other systems on the network. Although Microsoft had issued an out-of-cycle patch for the vulnerability, the worm keeps infecting systems even today.

[1] Administrative Scheduled Tasks are automatically run without any prompt, which allows the worm to copy and execute itself on clean systems.

In order to prevent the user from accessing disinfection tools offered by antimalware solutions vendors, the worm denies access to their homepage and also blocks files containing specific names. BitDefender was the first to offer a working disinfection tool, available for free from www.bdtools.net[2].

World's Top 10 Malware

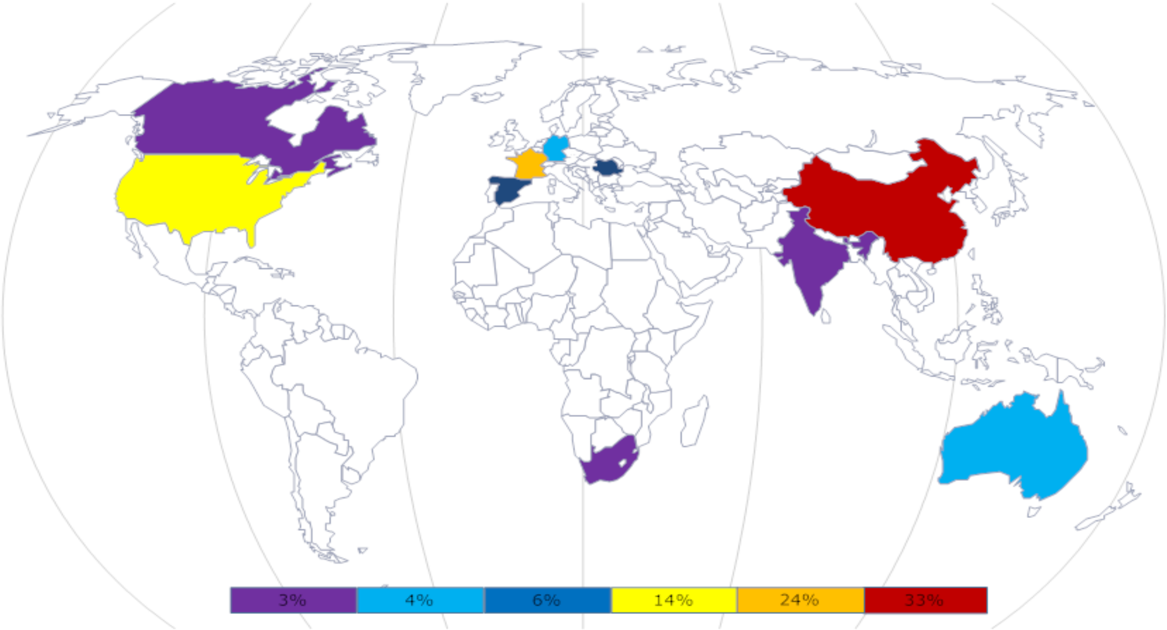


Figure 2: Malware breakdown by country

During the last six months the most active countries in terms of malware propagation were China, France and the United States, followed by Romania, Spain and Australia.

January – June 2009				
01.	Trojan.AutorunINF.Gen			31%
02.	Win32.Worm.Downadup.Gen			13%
03.	Trojan.Wimad.Gen.1			13%
04.	Trojan.Skimtrim.HTML.A			11%
05.	Trojan.Agent.AKXM			10%
06.	Trojan.Autorun.AET			7%
07.	Worm.Autorun.VHG			5%
08.	Packer.Malware.NSAnti.1			4%
09.	Trojan.Spy.Agent.NXS	3%	0.00	0.00
10.	Trojan.JS.PZB	3%	0.00	0.00

[2] At that time, www.bdtools.net was not blocked by Downadup. On April 08, an updated version of Downadup started blocking access to the website and BitDefender started offering free removal tools via the website set up at www.disinfecttools.net.

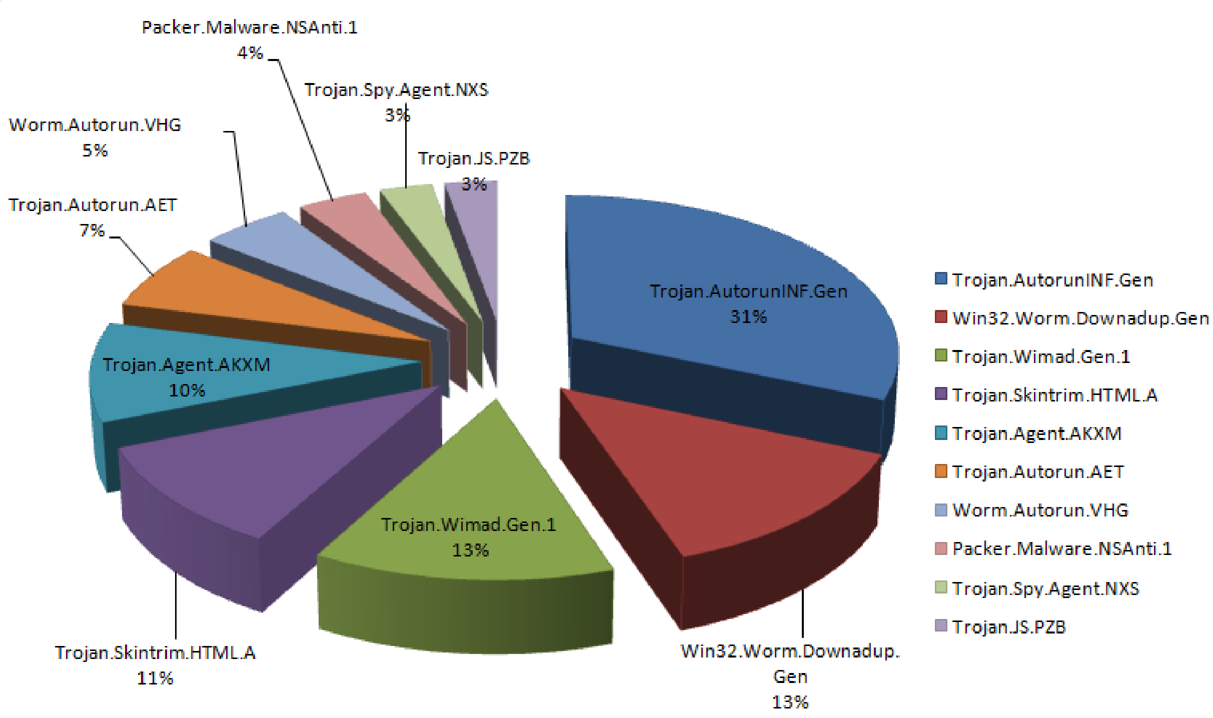


Figure 3: Top 10 malware threats for H1 2009

1. Trojan.Autorun.Inf

Ranking first in the H1 malware top, Trojan.Autorun.Inf is accountable for 31 percent of the total number of infections globally. However, the extremely large number of infections is not the result of global pandemics, but is rather due to the fact that the technique is being used by multiple malware families[3] to propagate via removable media.

Introduced back in Windows 95 in order to facilitate application installation for non-technical staff by opening the “right” file among others on a removable medium, the AutoRun feature has been successfully used by malware authors ever since.

One of the most important malware vectors, the autorun feature automatically executes a binary file once a removable medium is plugged into the PC. Before Windows Vista’s arrival, Windows-based operating systems would follow any autorun.inf file instructions

Despite the fact that it is extremely useful, Microsoft decided to disable it by default in its upcoming Windows 7 operating system.

2. Win32.Worm.Downadup

As stated above, Win32.Worm.Downadup needs no introduction: during the last six months it managed to infect an unprecedented number of worldwide computers and made the headlines of about any computer magazine.

The Downadup worm can compromise computers using three distinct approaches:

[3] The most important families of malware using the autorun feature are Win32.Worm.Downadup, Trojan.PWS.OnlineGames and Trojan.TDss.

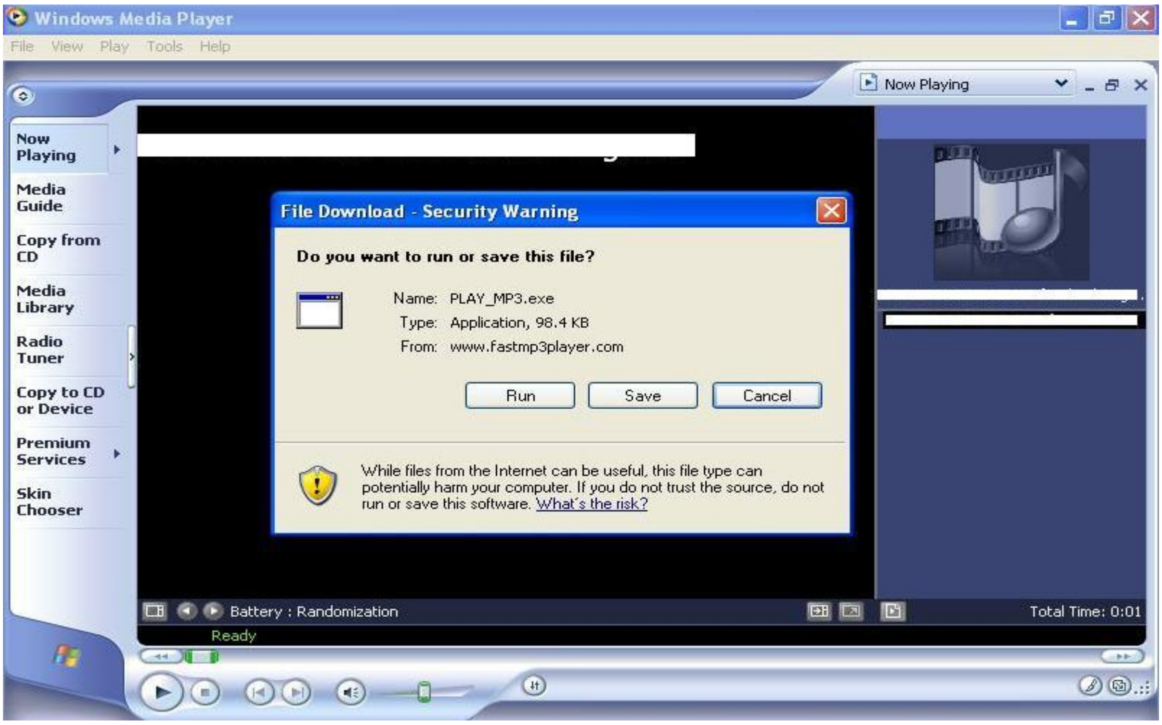
- If the target system has not been patched against the MS08-067 vulnerability, the worm can send itself from a computer on the network that had already been infected.
- Once it has infected a system that is part of a network, the worm would locate clean systems and would launch a brute-force attack on the remote administrative account in order to gain access to the user's file shares.
- If the worm has been copied onto a removable medium (CD-R, DVD-R, flash drive or a mapped network-attached storage device), it would take advantage of the **Autoplay** feature (if enabled) to automatically transfer itself to the clean computer.

The worm has obviously been engineered by a team of professional cyber-criminals, given the fact that it uses less-known Windows APIs and is extremely resilient to disinfection. For instance, the worm protects itself from deletion by removing all NTFS file permissions to all system users, except for the execute and directory traversal ones[4].

3. Trojan.Wimad

Ranking third in the H1 2009 malware top, Trojan.Wimad takes advantage of a less-known feature implemented by Microsoft in order to store coordinated digital media data. The Trojan affects ASF files, an extensible file format that supports data delivery over a wide variety of networks and is extremely easy to play back locally. The ASF format is actually a container for storing data in either WMA (Windows Media Audio) or WMV (Windows Media Video) formats.

What's particularly important in the ASF format specifications is the fact that it supports a feature in the Command Type Name known as **URLANDEXIT**. This feature allows the file to automatically download the appropriate video codec if it is missing from the system. However, the mechanism can easily be hijacked by malware authors in order for the file to download Trojans or to lead the user to a booby-trapped webpage.



File Download - Security Warning

Do you want to run or save this file?

Name: PLAY_MP3.exe
Type: Application, 98.4 KB
From: www.fastmp3player.com

Run | Save | Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Battery : Randomization
Ready
Total Time: 0:01

Figure 4: Infected video file trying to download a malicious binary

[4] For more information on the Downadup worm, as well as for our free disinfection tool, please visit http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html

4. Trojan.SkimTrim.HTML.A

Trojan.SkimTrim.HTML.A is part of the NaviPromo adware family. Known especially for its aggressive popups, resilience to detection and disinfection, this piece of adware uses advanced rootkit techniques to hide its files both on disk and memory, thus concealing its presence from both operating system and antivirus scanners.

NaviPromo is usually bundled with other pieces of software available on the web. It installs without users' consent, and then injects its code into explorer.exe. As the user surfs the web, NaviPromo monitors their surfing habits, collects and sends personal information, used for building commercial profiles. When profiling is done, the user starts receiving pop-up ads related to the website content the user is currently reading.

5. Trojan.Agent.AKXM

While autorun.inf files are not malicious by themselves, they are used by malware authors to automatically launch miscellaneous pieces of malware when an infected medium is mounted. Trojant.Agent.AKXM is a particular piece of malware using the autorun feature. The file is obfuscated and packed with garbage text to prevent detection. Whenever the infected drive is accessed, the inf file would automaticall make rundll32.exe to load a dll file located at *RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\.* Analysis revealed that the launched dll file is in fact a copy of Win32.Worm.Downadup.

6. Trojan.Autorun.AET

Trojan.Autorun.AET is a piece of malware that spreads through the Windows shared folders, as well as via removable media (network attached storage devices or mapped drives). The Trojan exploits the Autorun feature implemented in Windows operating systems to automatically execute itself when an infected device is being plugged in. For more info on how the Autorun feature can impact on your computer's security, please check the discussion regarding Trojan.Autorun.Inf.

7. Worm.Autorun.WHG

Worm.Autorun.WHG is yet another version of the Trojan.Agent.AKXM, an autorun.inf file used by Win32.Worm.Downadup to spread via infected removable media.

8. Packer.Malware.NSAnti.1

This class unites different families of malware packed / protected with the NSAnti protection scheme. More to the point, NSAnti is a technology developed by cyber-criminals in order to allow them to hide malware contents from antivirus scanners.

One of the most important features of the NSAnti packer is the fact that the contained files can be executed on the fly, rather than written to the file system, where the antivirus could pick them up. NSAnti is making heavy use of polymorphism (the capacity to modify its code to deter signature-based detection) and is extremely resilient to emulation (its code has the ability to crash virtual machine). The NSAnti code is also subject to frequent changes in order to avoid detection by antivirus products.

9. Trojan.Spy.Agent.NXS

The ninth place in the malware top for the first half of 2009 is taken by Trojan.Spy.Agent.NXS, a piece of malware that can execute shell commands. Although the piece of malware does not maintain a permanent UDP or TCP connection, the bot can serve as a backdoor for remote intruders.

10. Trojan.JS.PZB

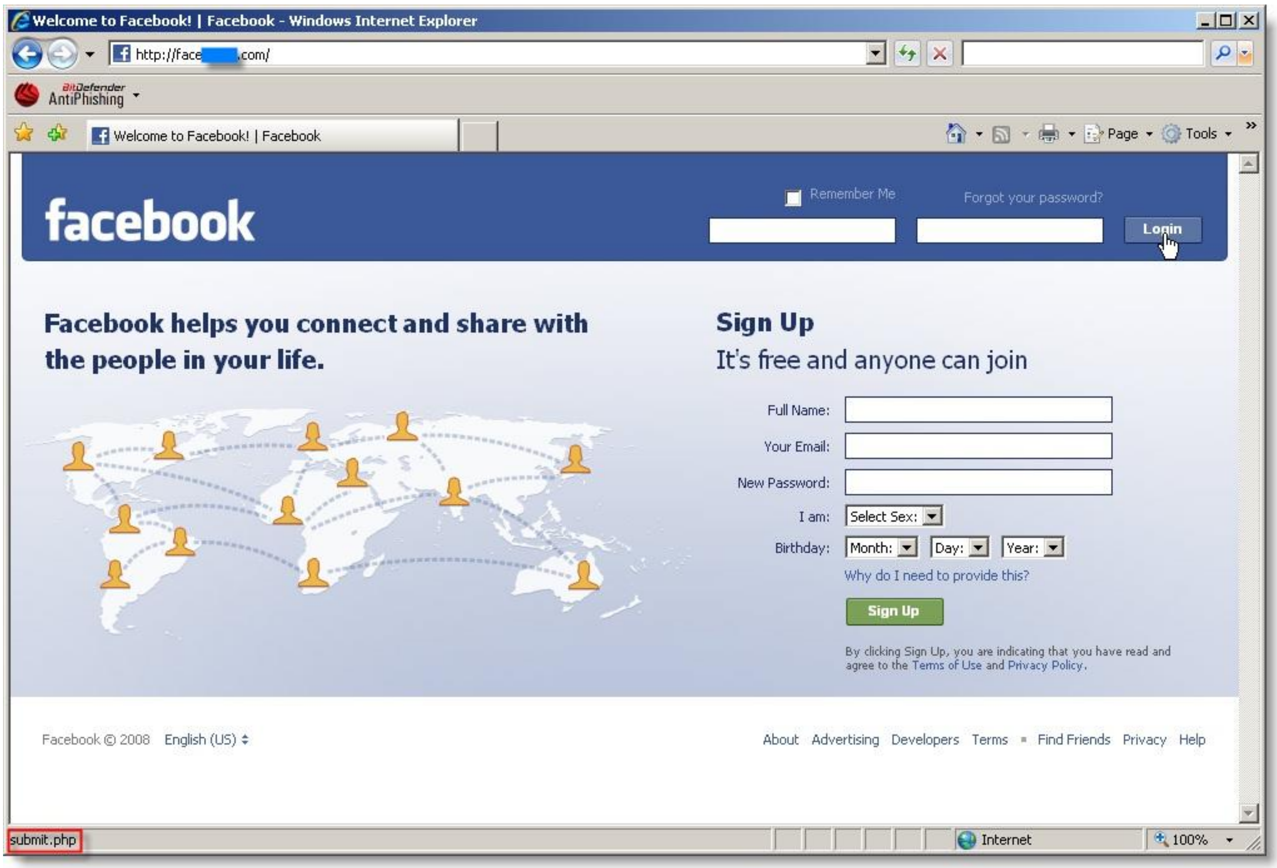
Ranking last in the H1 malware top, Trojan.JS.PZB uses iFrame techniques to inject malicious content into legitimate websites.Shortly put, a legitimate website can be compromised to host an invisible “window” to a third-party, malicious URL. Each time the user visits the infected webpage, they may trigger a drive-by malware download.

Web 2.0 Malware

The increased popularity of Web 2.0 services such as social-networking sites, blogs, and wiki platforms has made it easier for attackers to reach their malicious goals. Given the fact that most of these web 2.0 services ask for extra personal info as compared to a classical online community or blog, the user may get exposed should this info fall into the wrong hands.

Spam and phishing

Social network user accounts are key elements for carrying out subsequent attacks to other network users. However, since respectable service providers have tightened security in order to protect their users’ personal info, attackers have set up fake login pages in an attempt to get genuine user login credentials.



Welcome to Facebook! | Facebook - Windows Internet Explorer

http://face[redacted].com/

Facebook helps you connect and share with the people in your life.

Sign Up

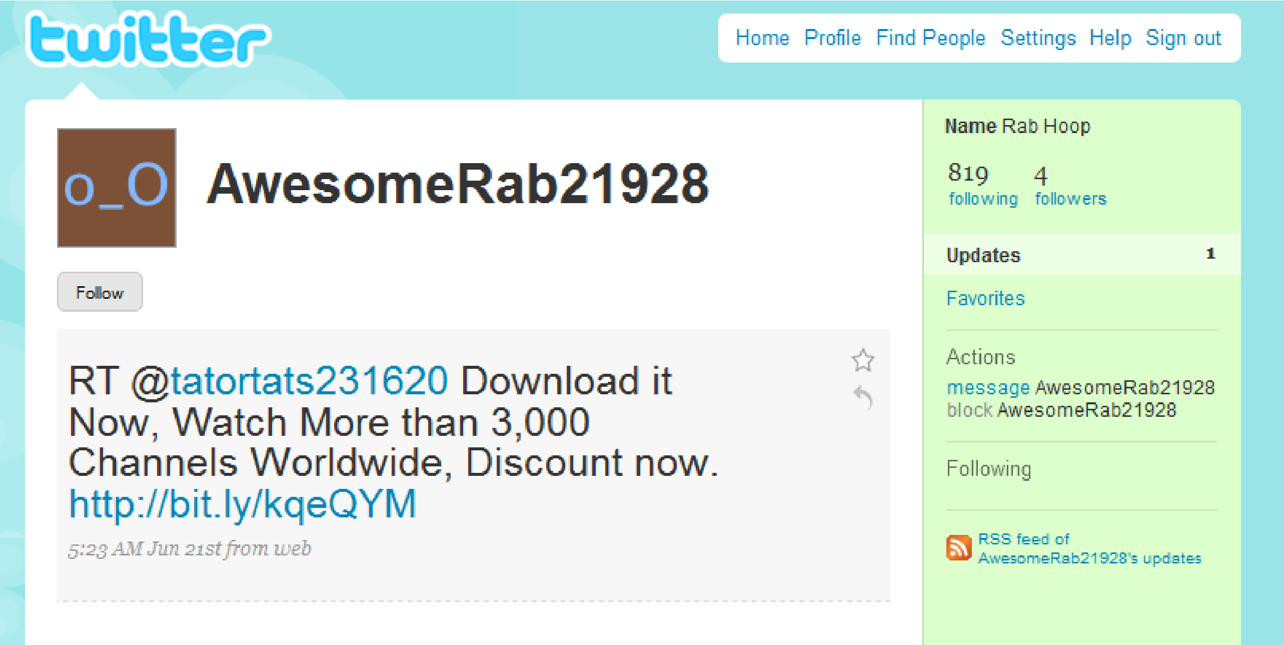
It's free and anyone can join

By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.

Facebook © 2008

Figure 5: Facebook phishing page

Social networks also enjoy heavy traffic and are the perfect spot to display own advertisements. Spammers set up dedicated accounts with the sole purpose of displaying links to websites advertising products or to malicious files.


twitter
Home Profile Find People Settings Help Sign out
o_O
Follow
Name Rab Hoop
819 following 4 followers
Updates 1
Favorites
Actions
Following
RSS feed of AwesomeRab21928's updates

AwesomeRab21928

RT @tatortats231620 Download it Now, Watch More than 3,000 Channels Worldwide, Discount now. http://bit.ly/kqeQYM

5:23 AM Jun 21st from web

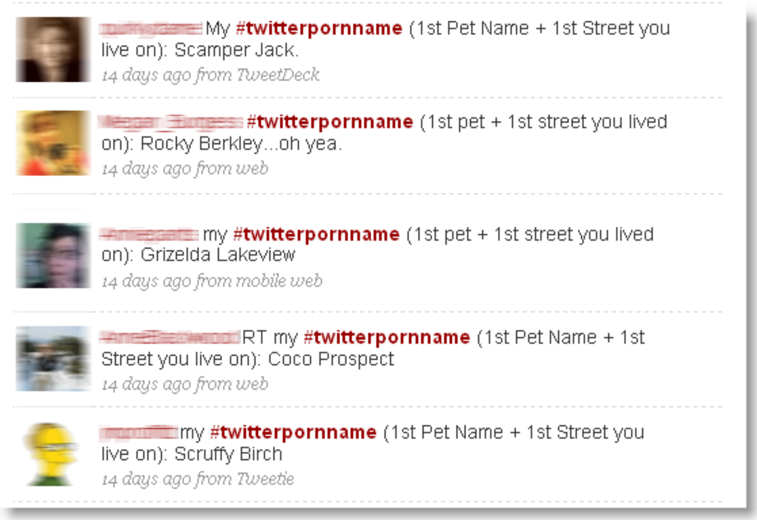
message AwesomeRab21928
block AwesomeRab21928

Figure 6: Single-post Twitter profile advertising satellite dishes

Spam and phishing are the most prominent threats related to Web 2.0 services, but they are not the only dangers the social networking user is exposed to. Web 2.0 communities have also become an important vector for spreading malware, especially Trojan horses and rogue AV utilities.

It is worth to mention that most endeavours concentrated particularly on stealing log in credentials, as well as other data that could facilitate their access to Twitter and similar platforms, such as e-mail, blogging or e-commerce accounts. Gaining such access translates into a wide range of e-crime opportunities, from further spam and phishing attempts (employing the list of followers/friends/contacts) to identity and commercial data theft or blackmail and extortion.

Most of these phishing attempts relied on social engineering schemes and speculated the user’s naïveté. The Twitter Porn Name scam is a good example. Users were invited to reveal their first pet name, as well as the first street they live. These names are usually employed as backup/security questions for the previously mentioned applications. An e-crook possessing one’s username and these “clues” can easily retrieve a “forgotten” password that he or she can later employ to access the account and send spam, access transactions or make whatever profit (including demanding a ransom for releasing the hijacked account).



[redacted] My **#twitterpornname** (1st Pet Name + 1st Street you live on): Scamper Jack.
14 days ago from TweetDeck

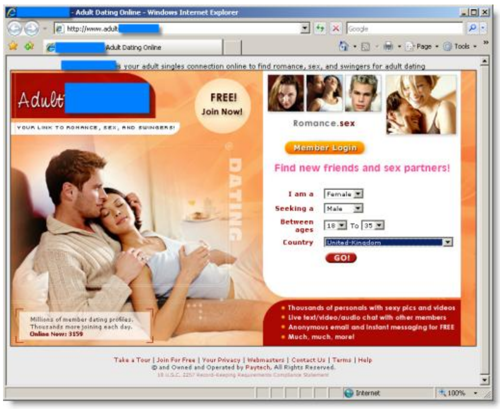
[redacted] **#twitterpornname** (1st pet + 1st street you lived on): Rocky Berkley...oh yea.
14 days ago from web

[redacted] my **#twitterpornname** (1st pet + 1st street you lived on): Grizelda Lakeview
14 days ago from mobile web

[redacted] RT my **#twitterpornname** (1st Pet Name + 1st Street you live on): Coco Prospect
14 days ago from web

[redacted] my **#twitterpornname** (1st Pet Name + 1st Street you live on): Scruffy Birch
14 days ago from Tweetie

Other schemes involved typosquatted Web sites, such as tvvitter.com (currently unavailable), that harvested the log in credentials and automatically added some unwanted followers. The links displayed on these (possibly bogus or hijacked) profiles redirected the users toward a dating site, probably in some pay-per-click or ranking fraud.



[redacted] - Adult Dating Online - Windows Internet Explorer

http://www.adult[redacted]

[redacted] Adult Dating Online

[redacted]s your adult singles connection online to find romance, sex, and swingers for adult dating

Find new friends and sex partners!

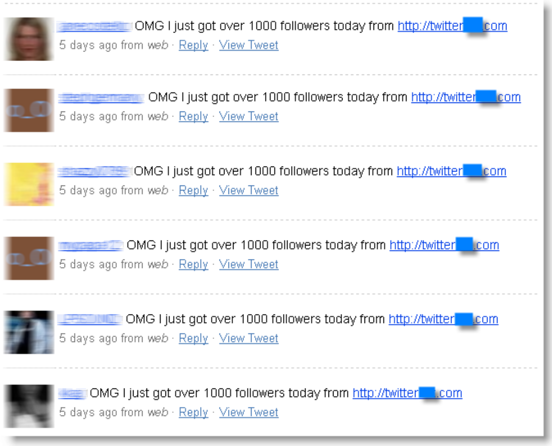
I am a: Female
Seeking a: Male
Between ages: 18 To 35
Country: United-Kingdom
GO!

- Thousands of personals with sexy pics and videos
- Live text/video/audio chat with other members
- Anonymous email and instant messaging for FREE
- Much, much, more!

Millions of member dating profiles. Thousands more joining each day. **Online Now: 3159**

Take a Tour | Join For Free | Your Privacy | Webmasters | Contact Us | Terms | Help
© and Owned and Operated by Paytech. All Rights Reserved.
18 U.S.C. 2257 Record-Keeping Requirements Compliance Statement

Another phishing scheme involved an alleged third party Web site that sent messages about the opportunity to rapidly increase the number of Twitter followers. To complete the process, the Web site demanded the Twitter username and password. When provided, the unwary user's list of followers was automatically spammed with the same message.



[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

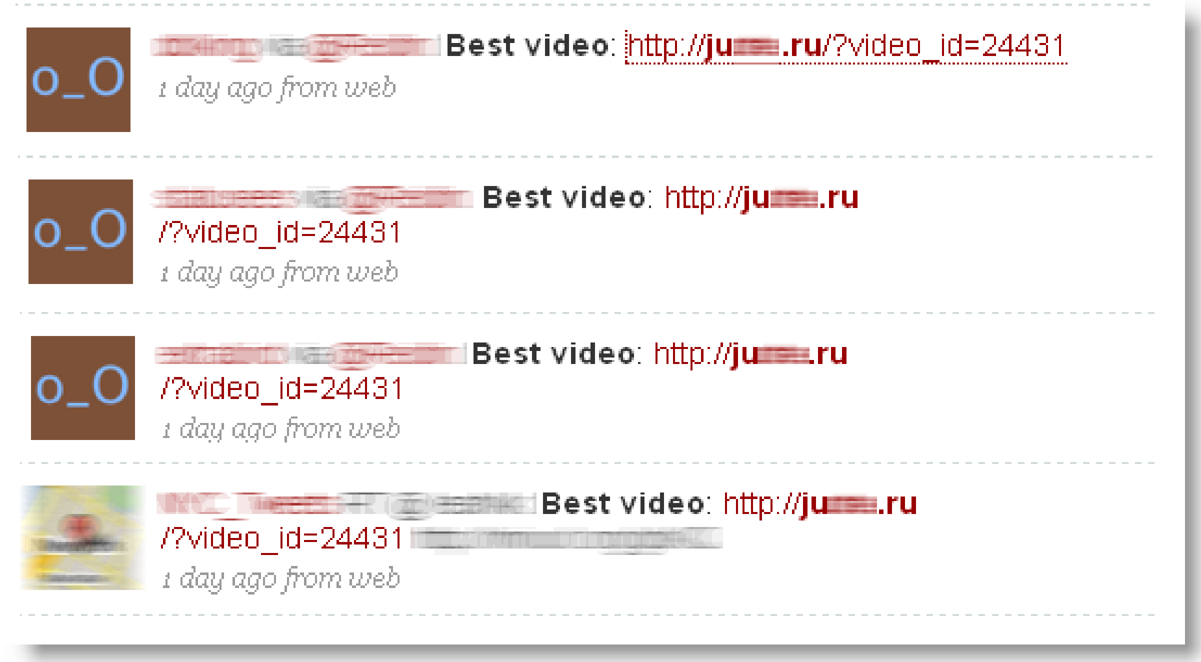
[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

[redacted] OMG I just got over 1000 followers today from http://twitter[redacted].com
5 days ago from web · Reply · View Tweet

Last but not least, one of the recent attacks relied on a combination of spam disseminated via different accounts and a maliciously crafted PDF that downloaded via an iFrame exploit when the user clicked a link purporting to display the “Best video”.



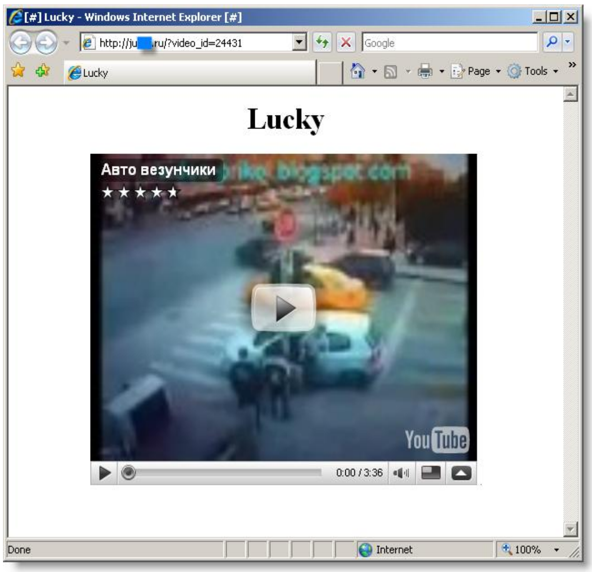
o_O [redacted] Best video: http://ju[redacted].ru/?video_id=24431
1 day ago from web

o_O [redacted] Best video: http://ju[redacted].ru/?video_id=24431
1 day ago from web

o_O [redacted] Best video: http://ju[redacted].ru/?video_id=24431
1 day ago from web

[redacted] Best video: http://ju[redacted].ru/?video_id=24431 [redacted]
1 day ago from web

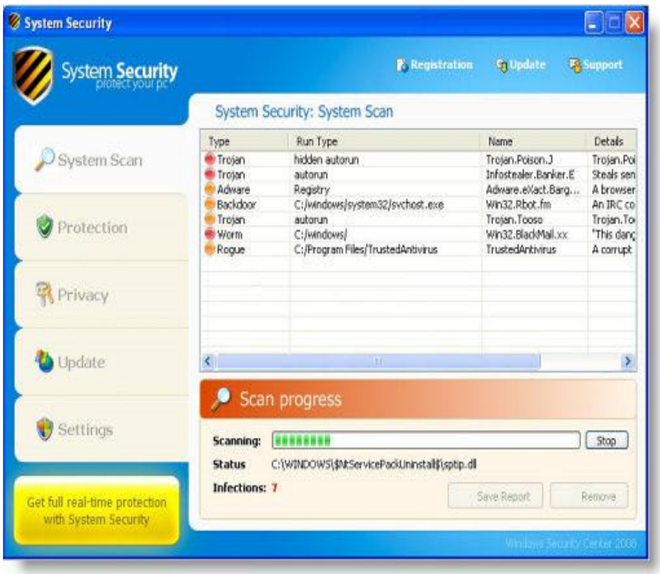
Besides the clip, the page hosted in Russia also delivered System Security 2009 rogue software.



[#] Lucky - Windows Internet Explorer [#]

http://ju[redacted].ru/?video_id=24431

Lucky



System Security

System Security: System Scan

Type	Run Type	Name	Details
Trojan	hidden autorun	Trojan.Poison.J	Trojan.Poi
Trojan	autorun	Infostealer.Banker.E	Steals sen
Adware	Registry	Adware.eXact.Barg...	A browser
Backdoor	C:/windows/system32/svchost.exe	Win32.Rbot.fm	An IRC co
Trojan	autorun	Trojan.Tooso	Trojan.To
Worm	C:/windows/	Win32.BlackMail.xx	"This danc
Rogue	C:/Program Files/TrustedAntivirus	TrustedAntivirus	A corrupt

Scan progress

Scanning:

Status C:\WINDOWS\$NtServicePackUninstall$\sptip.dll

Infections: 7

On April 30, Microsoft’s Technet service has been flooded by malicious links inserted in users’ profiles. Disguised as video players promoting adult scenes with miscellaneous celebrities (Rihanna and Angelina Jolie are only a few of the Hollywood names used), these profile signatures would require the user to download and install Mediacodec_v3.7.exe, a 1.93-Megabyte binary file that actually installs a rogue utility known as **Privacy Center**.

Spam Threats in Review

During the first half of 2009, spam messages impersonating newsletters has witnessed a sharp rise. These messages are HTML templates to which the spammer usually adds a spam image (Cialis, Viagra and Levitra advertisements) linked to a Chinese domain name.

Spam Distribution by Territory

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

Spam distribution by point of origin

January – June 2009

	Spam Index
Brazil	13.6
United States	10.1
India	5
Russia	4.2
China	3.3
Argentina	2.8
Spain	2.7
Colombia	2.6

Canada, Egypt, Morocco and Korea conclude the top with less than 0.5 percent of the global spam

.

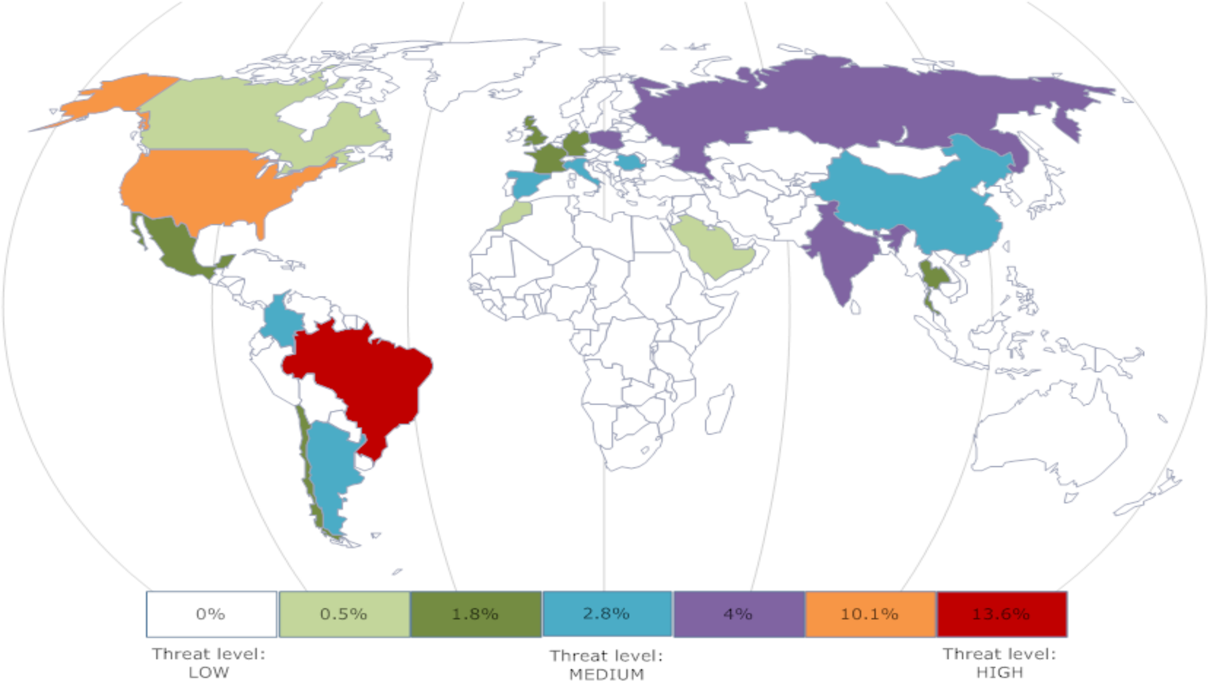
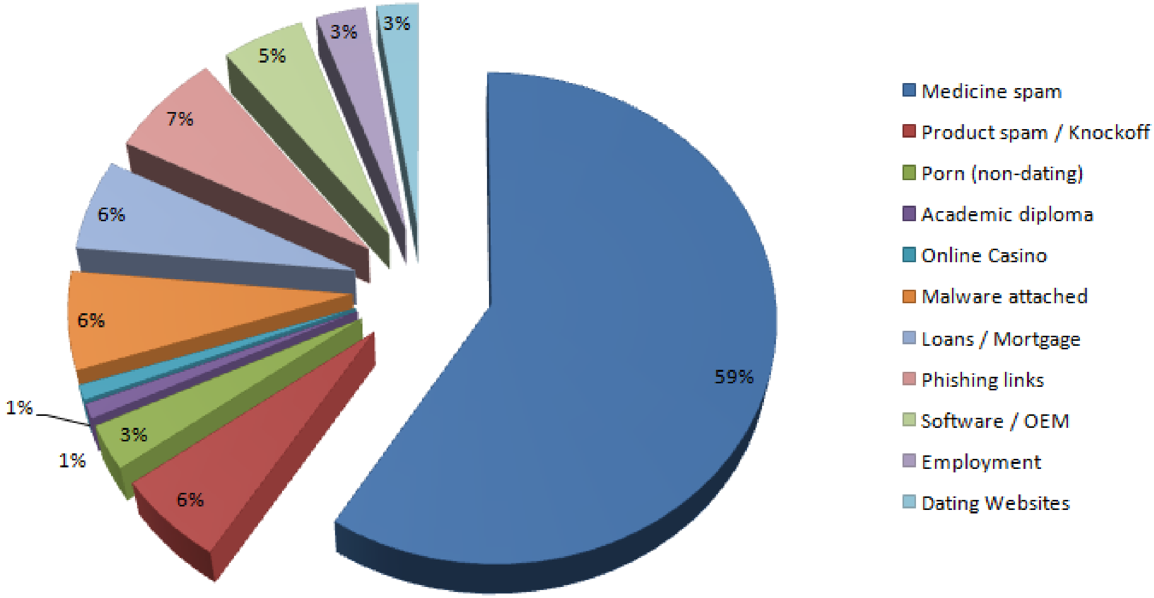


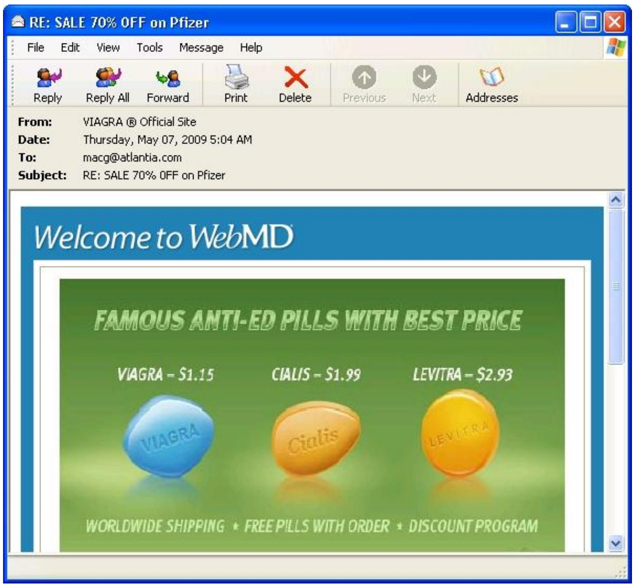
Figure 7: Spam distribution by territory

Spam Breakdown by Type

Spam messages advertising pirated / OEM software products also increased dramatically as compared to the same period last year. According to the statistics provided by the BitDefender Antispam labs, software spam accounts for about 3 percent of the worldwide spam. By June this year, unsolicited mail related to software products has become one of the top 5 spam threats and accounted for 5 percent of the total spam sent worldwide.



Spam Trends



From: VIAGRA ® Official Site
Date: Thursday, May 07, 2009 5:04 AM
To: macg@atlantia.com
Subject: RE: SALE 70% OFF on Pfizer

Welcome to WebMD
FAMOUS ANTI-ED PILLS WITH BEST PRICE
VIAGRA – $1.15
CIALIS – $1.99
LEVITRA – $2.93
WORLDWIDE SHIPPING • FREE PILLS WITH ORDER • DISCOUNT PROGRAM

Just like in the previous semester, spammers still rely on plain text messages for unsolicited mail. According to the Antispam researchers, plain-text spam accounts for over 80% of the worldwide spam. Image-based spam has also increased considerably as compared to H1 2008 up to 150%.

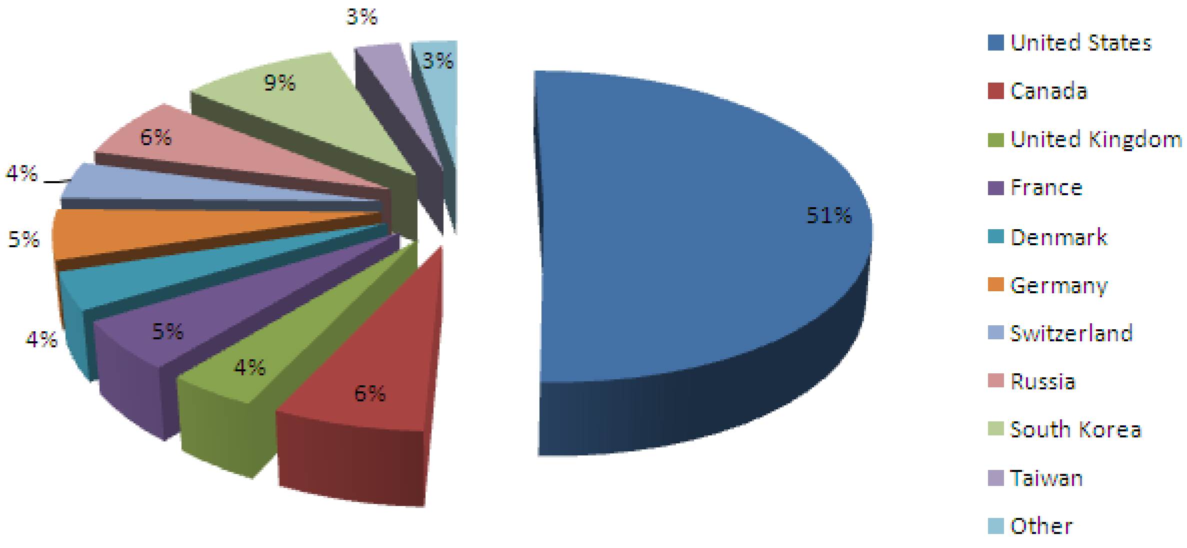
Medicine spam – the most popular segment of unsolicited mail – now features suggestive images inserted in legitimate newsletters (especially the HTML mail updates sent by WebMD).

This strategy allows spammers to trick users into accepting the image if it is blocked by the email client and, at the same time, to bypass spam filters by slightly modifying the image's color palette.

Phishing and Identity Theft

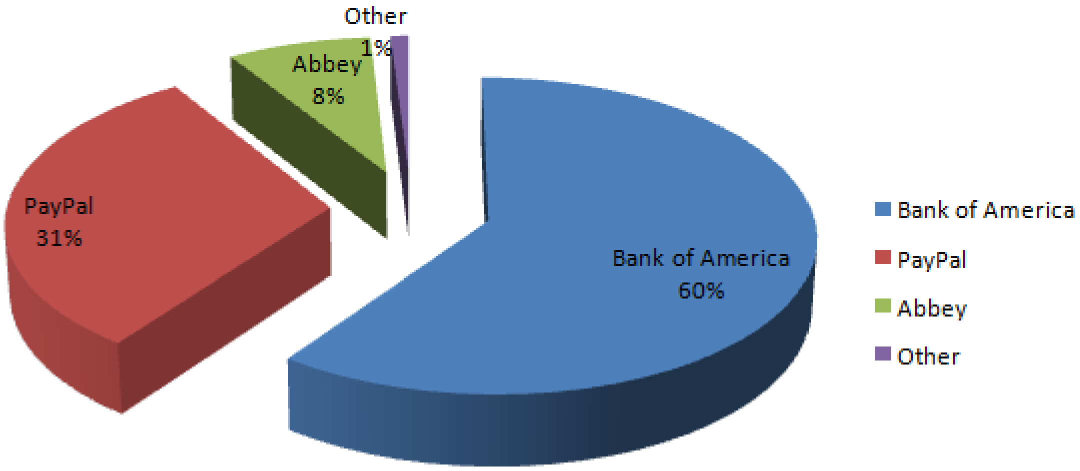
One of the most important threats for the average email user, phishing attempts witnessed a dramatic rise over the past six months. Primarily targeting English-speaking and less tech-savvy web surfers, phishing attempts can dramatically impact on users' banking balance.

Given the fact that more and more phishing attempts target banks and are as dangerous as malware infections, BitDefender is constantly monitoring phishing trends by analyzing messages collected through its global network of honeypots.



During the last 6 months, phishing messages reached an alarming threshold of 7 percent of the spam messages sent worldwide. As expected, the most receptive countries in terms of phishing are the United States, Canada and the United Kingdom - three English-speaking countries. However, Russia is another significant source of phishing messages, mostly because of its lax legislation regarding cyber-crime, as well as of the current unemployment rates.

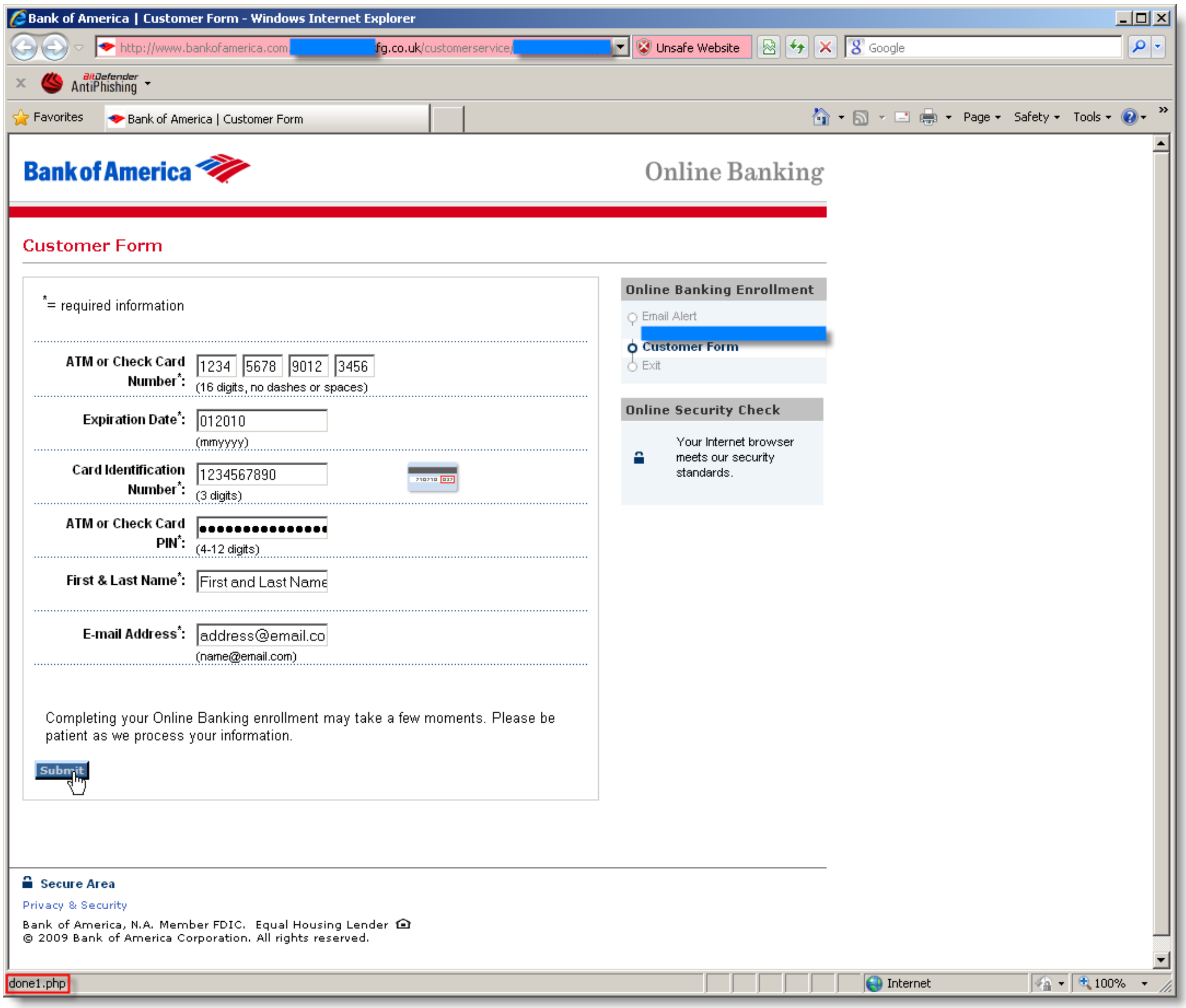
The phishing landscape is continuously evolving and morphing, but phishers' most favourite targets are constant. On average, the most abused identities are related to the financial sector, primarily banks and wire transfer institutions. On a side note, most of the phishing messages rely to social engineering and explain the user that their account has been either blocked or has expired and they need to re-enter their login credentials for re-activation. Other variants of phishing messages announce the recipients that their accounts have been emptied by unauthorized persons and they need to re-login to cancel the transaction.



BitDefender estimates that more than 55,000 users fall for phishing scams each month, which leads to an impressive number of 330,000 victims for H1 2009. Most importantly, unlike malware, **phishing and spam are universal e-threats** – they work on any computer, regardless of their operating systems and security patches. Extra caution and a highly-rated antimalware solution with antispam, antiphishing and antimalware modules are a must-have for the web surfer.

In order to succeed in deceiving their victims, phishers have to impersonate (spoof) the genuine page as accurately as possible. However, while replicating the original webpage is just a matter of copy-and-paste, the spam message usually contains misspelled words or negligent formatting.

This is not the case with most of the phishing raids targeting Bank of America. Not only that the text is impeccably laid out, but the phishing page has also been crafted with an unusual attention to details, which suggests that those behind the business are a highly organized gang of cyber-criminals.



Bank of America | Customer Form - Windows Internet Explorer

http://www.bankofamerica.com[redacted]fg.co.uk/customerservice/[redacted]

Bank of America

Online Banking

Customer Form

*= required information

ATM or Check Card Number*:	1234 5678 9012 3456 (16 digits, no dashes or spaces)
Expiration Date*:	012010 (mmyyyy)
Card Identification Number*:	1234567890 (3 digits)
ATM or Check Card PIN*:	●●●●●●●●●●●●●●● (4-12 digits)
First & Last Name*:	First and Last Name
E-mail Address*:	address@email.co (name@email.com)

Completing your Online Banking enrollment may take a few moments. Please be patient as we process your information.

Submit

Online Banking Enrollment

○ Email Alert
[redacted]
● Customer Form
○ Exit

Online Security Check

Your Internet browser meets our security standards.

Secure Area

Privacy & Security

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2009 Bank of America Corporation. All rights reserved.

The viral distribution of unsolicited messages is done via the Pushdo botnet, a zombie network of malware-infected computers that is also accountable for Canadian Pharmacy spam, along with other campaigns.

Vulnerabilities, Exploits & Security Breaches

While malware accounts for most of the security incidents that happen globally, vulnerabilities and exploits also play an important role in the e-threat landscape. Beyond headline-grabbing vulnerabilities such as those listed below, the first half of 2009 has been marked by continuing diversification of exploit targets – MacOS X, the Safari browser and associated technologies are beginning to get attention from security researchers and hackers alike as their market and mind share grows. Open source software such as Linux and the Firefox browser have continued to attract increasing attention for various bugs and vulnerabilities as well.

A third area of concern is related to Web 2.0 apps and services – the relative immaturity of the underlying technologies continues to give way to numerous security breaches. PHP-based web frameworks have been amongst the worst-hit, but other types of services and software are being heavily targeted as well.

MD5 Collision Attacks

The first major security incident in 2009 was reported in January with the discovery of a practical way to obtain collisions in the MD5 hashing algorithm. The MD5 format is widely used to encrypt passwords without the possibility of reversing, as well as to sign digital certificates.

The research team conducted by Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger demonstrated that virtually undetectable phishing attacks are possible by creating a rogue Certification Authority certificate. As soon as a CA certificate is successfully added, the browser would trust any digital signature emerging from the Certificate Authority (CA). This way, attackers can sign digital certificates that will be accepted by the compromised browsers.

A collision attack practically makes a file to pass as another. In order to hijack a Certificate Authority, researchers had to generate the same hash for two distinct data chunks. They relied on 200 PlayStation 3 gaming consoles stacked together, as their Cell processors are extremely optimized for this kind of operation.

Linux Sudo command makes way for security breaches

A critical vulnerability in the increasingly popular Ubuntu Linux distributions has been discovered in February. Labeled as CVE-2009-0034, the bug only affected versions 8.04 and 8.10 of Ubuntu and allowed non-administrative users to run applications as root or tamper with other users’ files.

By design, the Sudo command allows regular system users to escalate their privileges to the administrative level. In order to be able to install software or perform system-wide changes, these users have to be listed in a special file, called "sudoers". However, the same file can be configured to allow user accounts to run programs with the privileges of other user accounts (for instance, to allow remote users to perform print jobs as if they were local users. However, this specific configuration setup can pose serious privacy issues to other user accounts.

Conclusions

Malware development is a rapidly evolving business, both because this specific niche of software programmers are driven by illicit financial gains and because of technology's rapid evolution.

Most software companies run an extremely tight schedule from envisioning their products to actually delivering them to their users, in order to maximize sales. However, many times, such applications are not fully tested and proofed against various types of attacks or critical coding flaws.

Other vulnerable factors in malware distribution schemes are the very end-users – their lack of awareness on the latest trends in the malware landscape can dramatically impact on both their budget and privacy.

Voluntary disclosure of trivial information via Web 2.0 websites or blogging platforms can also help malicious third parties build personal profiles or gather additional data to be used in phishing attempts.

In order to enjoy a safe and pleasant experience while surfing the web, BitDefender recommends that you install, activate and update a complete anti-malware protection solution.

Table of Figures