

E-Threats Landscape Report

IT&C SECURITY COURSE JANUARY – JUNE 2008



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.

Copyright © 2008 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

Authors & Contributors

Sorin Victor DUDEA
Head of Antimalware Research

Viorel CANJA
Head of Antimalware Lab

Dragoș GAVRILUȚ
Malware Analyst

Daniel CHIPIRIȘTEANU
Malware Analyst

Vlad VĂLCEANU
Head of Antispam Research

Andra MILOIU
Spam Analyst

Alexandru-Cătălin COȘOI
Antispam Researcher

George PETRE
Antispam Intelligence Researcher

Mircea MITU
Senior Product Manager for Core Technologies

Alexandru BĂLAN
Product Manager

Matei-Răzvan STOICA
Communication Specialist

Răzvan LIVINTZ
Communication Specialist

Table of Contents

E-Threats Landscape Report.....	1
Disclaimer.....	2
Authors & Contributors.....	3
Table of Contents.....	4
About This Report.....	5
We Would Like to Hear from You	5
Predicting 2008’s E-Threats.....	6
First Half’s Spotlight E-Threats	7
<i>Malware</i>	7
<i>E-mail Spam</i>	12
<i>Phishing & ID Abuse</i>	14
BitDefender’s Keep You Safe Guidelines	15

About This Report

The purpose of this report is to provide a comprehensive investigation of the threats' landscape over the last six months, between January and June 2008. BitDefender®'s security experts thoroughly analyzed and examined the menaces of the first semester, focusing on software vulnerabilities and exploits, different types of malware, as well as countermeasures, cyber crime prevention and law enforcement.

The *E-Threats¹ Landscape Report* concentrates mainly on the first half of 2008, but it also contains facts, data and trends concerning the previously investigated periods, as well as several predictions related to the upcoming semester.

This document is primarily intended for IT&C System's Security Managers, System and Network Administrators, Security Technology Developers, Analysts, and Researchers, but it also addresses issues pertaining to a broader audience, like small organizations or individual users concerned about the safety and integrity of their networks and systems.

We Would Like to Hear from You

As the reader of this document, you are our most important critic and commentator. We value your opinion and want to know what you like about our work, what you dislike, what we could do better, what topics you would like to see us cover, but also any other comments and suggestions you wish to share with BitDefender's Team.

You can e-mail or write us directly to let us know what you did or did not find useful and interesting about this report, as well as what elements and details we should add to make our work stronger.

When you write, please be sure to include this document's title and author, as well as your name and phone or e-mail address. We will carefully review your comments and share them with the authors and contributors who worked on this document.

E-mail:

documentation@bitdefender.com

Mail:

BitDefender Headquarters

West Gate Park

24th, Preciziei Street

Building H2, Ground Floor

6th district, 062204, Bucharest

ROMANIA

¹ BitDefender defines *e-threats* as a general term that comprises, but is not limited to, any type of exploit, malware, virus, worm, bot and botnet, Trojan, backdoor, rootkit, spyware, adware, grayware, rogue security software, phishing, pharming, harvesting, e-mail spamming, etc.

Predicting 2008's E-Threats

As the very first days of 2008 were approaching, the IT&C Security Analysts around the world began to predict the key events to affect networks' and systems' safety. BitDefender's specialists proposed for the ongoing year the following top 10 threats to affect the users worldwide:

- 1. Individual workstation menaces** – most of the threats in 2008 will focus on system's vulnerabilities, seeking to illicitly gain access to personal and financial information, as well as substantial and relevant details about online transactions.
- 2. Unsolicited e-mail escalation** – 2008 will witness a major boost in terms of generation and distribution mechanisms. New creation and dissemination techniques are about to emerge, while the messages will focus most likely on major events, such as the US elections.
- 3. Mobile devices' vulnerability exploitation** – because of their numerous Internet connectivity opportunities, such as Wi-Fi, GPRS, WAP, Bluetooth, mobile computing and mobile communication gadgets are about to be heavily harassed this year.
- 4. Mobile spam & phishing amplification** – unwanted e-mail and phishing will converge more and more towards mobile phones, aiming especially the smart phones users. Nonetheless, the classic SMS will keep and augment its traditional share in terms of spam and financial lottery scams. Phishing rate is about to expand too, especially through WAP-PUSH technology proliferation, since this enables random unsolicited mobile content downloading.
- 5. Mobile technology viral blast** – smart phones and other intelligent business top tier devices with permanent Internet access are about to be targeted by the new mobile virus generations. A special attention will be paid to the browsers' vulnerabilities, which are about to be even more exploited in the near future.
- 6. Botnets ascending trend** – following 2007's incredible worldwide rise of the Storm Trojan horse, this year will experience similar dynamics related to the botnet general evolution. Most likely, the new and improved backdoor Trojan horse Zlob will be, in effect, one of the most dangerous malware specimens.
- 7. Victims of phishing's and ID abuse's increment** – web and e-mail-based phishing will have their regular casualties among the unprotected or unaware users; moreover, the number of victims is expected to increment due to SSL encryption the web-based phishing employs and to complex filter-evasive maneuvers and techniques comprised by the e-mail-based phishing. Banks and other social and financial institutions will be among the most appealing targets.
- 8. Adware and spyware still active** – 2008 will maintain, probably, the same level of adware and spyware, although their supremacy over other malware releases is now a simple history chapter. Still, the unprotected systems will be easily cozened.
- 9. File viruses' creation and distribution quite abundant** – average unprotected home users and file sharing regular customers will continue to be the default recipients of these viral solutions. Business sector will be just a col-

lateral casualty, as long as its security solutions and internal policies are not strong enough or improperly designed and deployed.

- 10. Mass-mailers' pace diminished** – unlike past year, 2008 will offer a significant reduced backdrop of this type of malware. Nevertheless, the unprotected systems and networks will be flooded without difficulty, whether we refer to individual, home or corporate users.

Six months after this initial forecast, the threats landscape confirmed most of our analysts' early predictions, but also offered several surprises, proving once again cybercriminals' mischievous creativity.

First Half's Spotlight E-Threats

To summarize, the IT&C security realm confronted in the first six months of 2008 with the following threats and dangers:

- 80% of the malware distributed worldwide consists of Trojans
- 1/3 of global malware exploits OS's and applications' vulnerabilities
- text-based spam took over the leadership again, holding 70% of the total unsolicited e-mails
- image spam continued its decline and dropped to 3%
- drugs represent the most advocated content via e-mail spam, with 51 percents of the entire spam volume, while the formerly widely advertised stock spam decreased under 10%
- 50% of the total phishing attempts forged identification elements pertaining to US financial organizations
- phishers also focused their attention on potential victims from EU states.

For a comprehensive description of the 2008's first semester, see the following sections:

- [Malware](#)
- [E-mail Spam](#)
- [Phishing & ID Abuse](#)

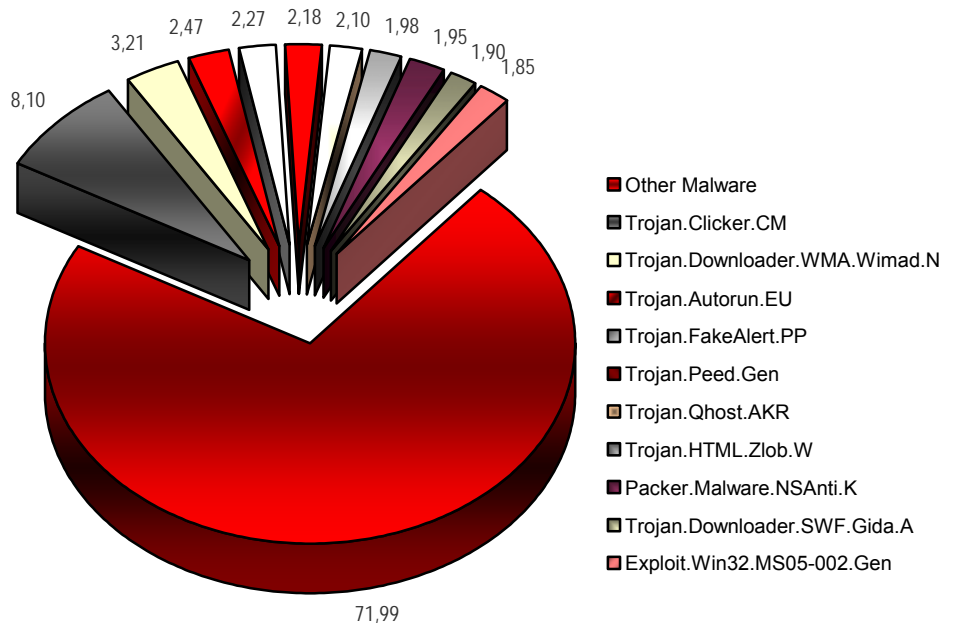
Malware

The first six months of 2008 revealed that malware creators have concentrated their efforts on exploiting systems' vulnerabilities via threats mimicking legitimate applications. Thus, 80 percents of the global malware chart is populated by Trojans.

"2008's malware continues to revolve around profit, mainly financial. To ensure gains, cybercriminals need a way to compromise a large number of systems where to deploy as many bots, adware and spyware as possible, with less or no costs at all. Thus, the most difficult task (or not, if we take a look at the e-threats chart's "inhabitants") is not the malware's dissemination, but the system's infiltration and exposure to other threats. This explains the Trojan horses' heavy mass production we encountered the last six months." said Sorin Dudea, Head of BitDefender Antimalware Research.

The Top 10 list for the first half of 2008's most effective malware comprises:

World's Top 10 Malware January – June 2008		
RANK	MALWARE	PERCENTAGE
01.	Trojan.Clicker.CM	8.10
02.	Trojan.Downloader.WMA.Wimad.N	3.21
03.	Trojan.Autorun.EU	2.47
04.	Trojan.FakeAlert.PP	2.27
05.	Trojan.Peed.Gen	2.18
06.	Trojan.Qhost.AKR	2.10
07.	Trojan.HTML.Zlob.W	1.98
08.	Packer.Malware.NSAnti.K	1.95
09.	Trojan.Downloader.SWF.Gida.A	1.90
10.	Exploit.Win32.MS05-002.Gen	1.85
11.	Other Malware	71.99

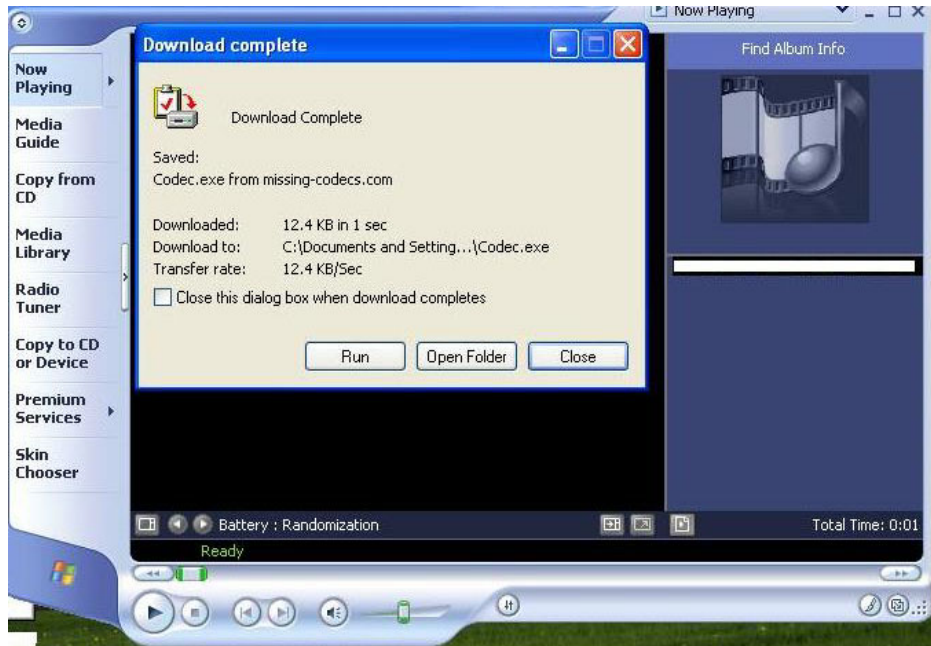


Source: BitDefender Labs

First position belongs to [Trojan.Clicker.CM](#), which holds 8.10 percents of the infected computers worldwide. This Trojan displays a significant number of commercial pop-up windows in the current Web browser's background instance, trying to determine the user to click and thus generate profit for advertisements registered within a pay-per-click system.

Second position goes to [Trojan.Downloader.WMA.Wimad.N](#), responsible for the infliction of 3.21% systems around the globe. Usually distributed via e-mail spam campaigns as a 3.5 MB .wma attachment (and bearing the name of some popular artist), the disguised Trojan automatically opens the Web

browser in order to retrieve the “appropriate” codec, which is, in effect, another piece of adware – [Adware.PlayMp3z.A](#).



[Trojan.Autorun.EU](#) ranks the third, with 2.47 percents. This Trojan regularly inhabits the root of fixed and removable disk drives and helps the execution of other malware (mostly worms) on systems that have autorun function enabled.

[Trojan.FakeAlert.PP](#) places the fourth, 0.20% below the previous position. This malware issues a warning about a viral infection and request the installation of another malware – [Adware.XPantivirus.A](#), a fake antivirus.



[Trojan.Peed.Gen](#), also known as the (in)famous Storm, came out the fifth, with 2.18%. A spectacular malware with an unusual longevity, Peed has several

mischievous consequences related to the compromised system's resource drainage. Peed creates and randomly names infected copies of the executable files it finds. Concurrently, each 4 seconds scans the system and closes any window whose name pertains to an antimalware product.

On the sixth position resides [Trojan.Qhost.AKR](#), with 2.10 percents. Qhost poses as a BitDefender patch for 2008's security suite. Its purpose is to block any updates BitDefender's applications should receive on an hourly basis.

The seventh place goes to [Trojan.HTML.Zlob.W](#), and its 1.98 percents of all infected systems. This variant of the widely spread Trojan is part of a Web page requesting the user to download and install a specific ActiveX component or codec. After installation, Zlob copies itself in the root folder and injects malevolent code into other processes, such as "explorer.exe", "winlogon.exe", "svchost.exe", etc. Once installed, it reconfigures the Internet Explorer's start page and attempts to download and execute other malware.

[Packer.Malware.NSAnti.K](#), scoring 0.03% less than the previous e-threat, ranks the eighth. This malware acts as a malign shield that bypasses the installed security solution and conceals other malware. NSAnti is, in effect, a packer accountable for archiving executable files which can be stealthy loaded and run directly into the system's memory.

The ninth position is taken by [Trojan.Downloader.SWF.Gida.A](#), with 1.90%. The Trojan consists of an Adobe® Flash® ActiveScript which injects JavaScript and HTML code into the Web pages the user accesses. Subsequently, it initiates other malware downloads, while also displays several commercial pop-up windows for rogue antimalware products.

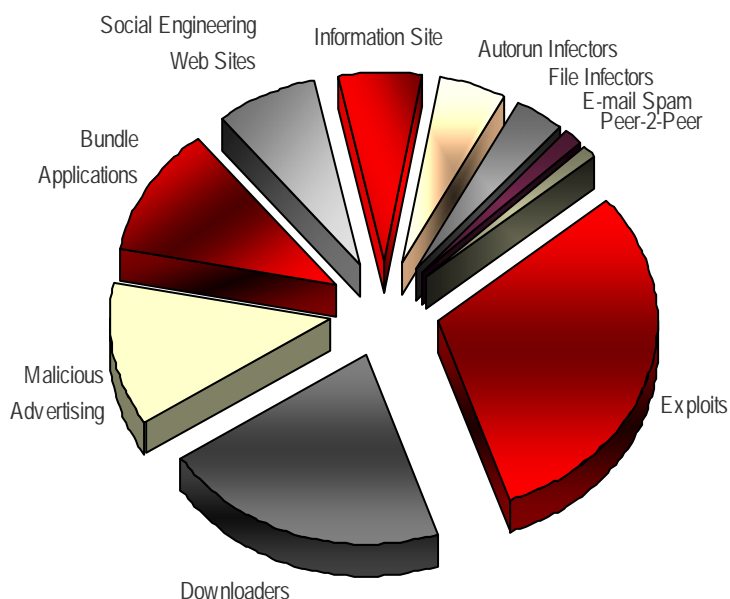
"We expect to see the figure of Adobe® Flash® ActiveScript exploitations increasing in the following months. Apparently innocent and harmless, the popular multimedia Flash® Player which is included or required by plenty of the current OSs and common applications offers an unexpected opportunity for malware creators. The end of May already brought numerous attempts seeking to take advantage of the [Exploit.SWF.Gen](#) that led to remote code execution via Web browsers, e-mail clients, as well as other applications on the systems worldwide." said Mircea Mitu, BitDefender Senior Product Manager for Core Technologies.

The last place goes to [Exploit.Win32.MS05-002.Gen](#), holding 1.85 percents. This e-threat resides on Microsoft® Windows® vulnerability in cursor and icon format handling which can allow remote code execution or cause Denial of Service on unprotected systems. Thus, a cybercriminal using a Web site that employs mischievously engineered icons and cursors could drop and execute arbitrary code.

"Probably an intriguing surprise for the 2008's list of most prolific e-threats, the already «classic» [Exploit.Win32.MS05-002.Gen](#), publicly disclosed in the second half of 2004, confirms our previous forecasts. On one hand, its presence in this malware chart shows clearly that many users either still employ a large number of outdated Microsoft® Windows® editions or pirated (and thus not patched) versions. On the other hand, it reflects a trend which is currently the dominant vector of the malware distribution methods. Almost certainly, the months to come will make hay of the systems' vulnerabilities exploitation." said Sorin Dudea, Head of BitDefender Antimalware Research.

The Top 10 list for the first half of 2008's most prolific dissemination methods holds:

World's Top 10 Malware Distribution Methods January – June 2008		
RANK	METHOD	PERCENTAGE
01.	Exploits	30.86
02.	Downloaders	20.98
03.	Malicious Advertising	12.34
04.	Bundle Applications	11.11
05.	Social Engineering Web Sites	7.40
06.	Information Sites	6.17
07.	Autorun Infectors	4.93
08.	File Infectors	3.70
09.	E-mail Spam	1.23
10.	Peer-2-Peer	1.23



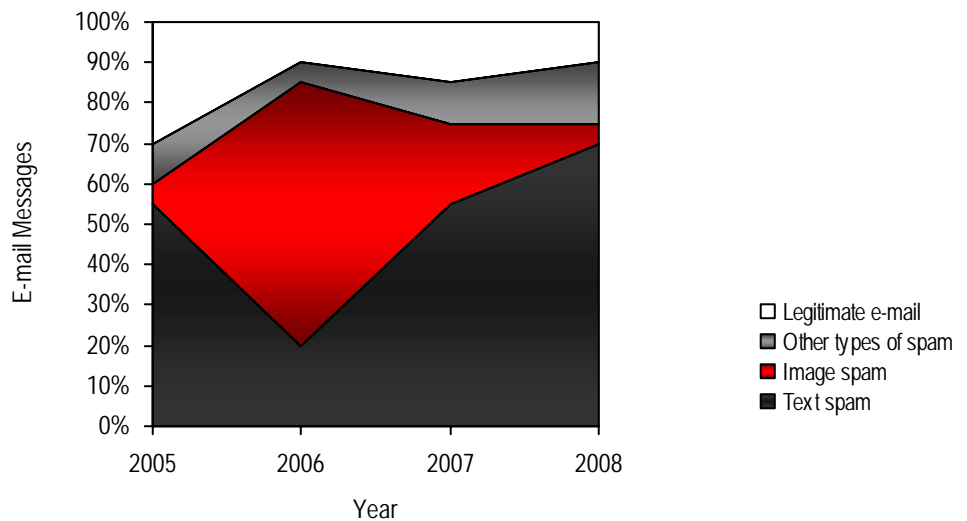
Source: BitDefender Labs

“The current malware chart proves once again several alarming aspects. First of all, it demonstrates that many Web surfers around the globe are not protected by a reliable security solution. Second, the computer users worldwide do not possess the basic information for preventing and protecting their systems against malware. Third, it reveals that the average home and business users are not aware of the intricate dangers which eventually may inflict their work. Last but not least, it shows that the software security industry should also pay more attention to user's e-threats culture and antimalware education, by improving and increasing their defense knowledge.” affirmed Viorel Canja, Head of BitDefender Antimalware Lab.

E-mail Spam

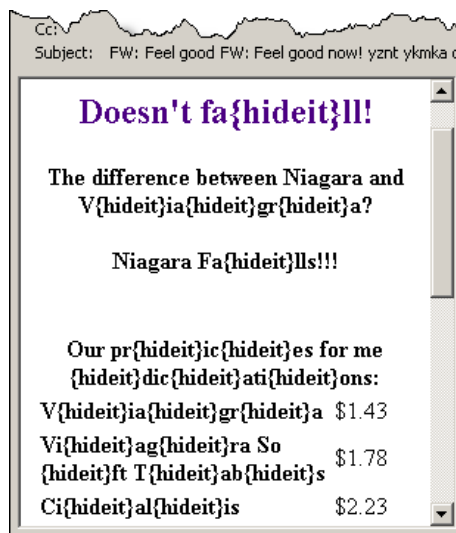
In terms of spam media and techniques, the most notable trend that BitDefender's analysts noticed in the first semester of 2008 concerns the revival of the text-based spam which reached this year 70% (compared to 20% in the same period of 2007). Image spam continued its decline and stopped this month to 3% (compared to 60% last year).

Spam Evolution



Source: BitDefender Labs

“Plain text continues to be the most prolific medium for e-mail spam distribution, especially due to its simplicity, reduced size and extreme versatility.” said Vlad Vâlceanu, Head of BitDefender Antispam Research Lab.

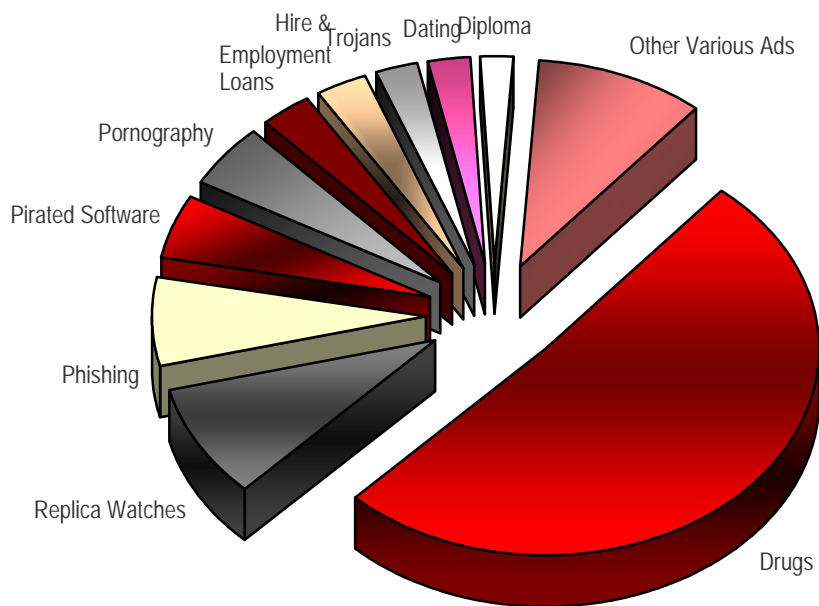


Text-based spam still appeals to automated scripts for word scrambling, rephrasing or (synonymic) substitution, while image spam usually employs obfuscated content. Other types of spam, such as e-mails bearing attached PDF, audio, video files, etc., became less and less popular and disappeared. Their take of 10-15% was replaced with a combination of plain text and HTML formatted messages.

E-mail spam’s content lost its emphasis on stock options. In addition and related to the spam media changes, if the last half of 2007 was dominated by the various image formats and .mp3 audio files, the first six months of 2008 brought back the non-obfuscated and identical text-based message templates.

The Top 10 list for the first half of 2008’s most advocated content through e-mail spam includes:

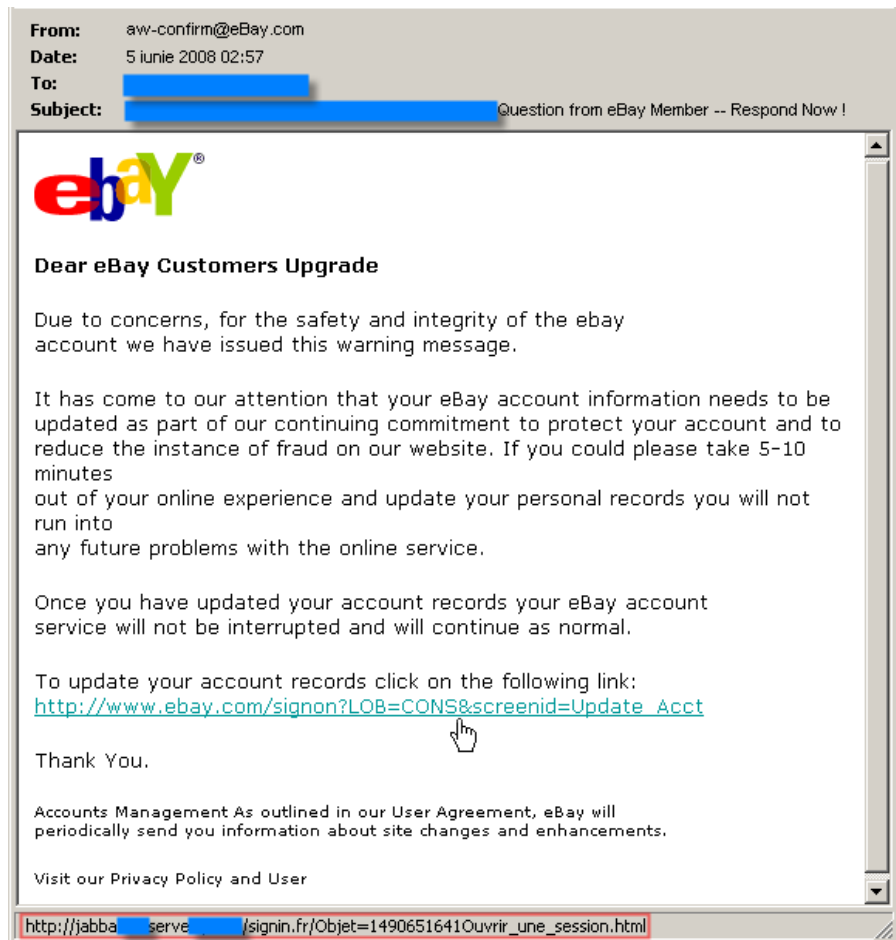
E-mail Spam’s Featured Content January – June 2008		
RANK	CONTENT TYPE	PERCENTAGE
01.	Drugs	51
02.	Replica Watches	9
03.	Phishing (tool for)	7
04.	Pirated Software	5
05.	Pornography	5
06.	Loans	3
07.	Hire & Employment	3
08.	Trojans’ Spread (tool for)	2.5
09.	Dating	2.5
10.	Diploma	2
11.	Other Various Ads	10



Source: BitDefender Labs

Phishing & ID Abuse

Phishing trends for the first half of 2008 indicate a variation and growth of the spoofed institutions and targeted clients. Primarily forged elements belong to the US financial organizations, while the possible victims are now the English native speakers who reside in US, UK or Canada, although last weeks BitDefender's researchers received several notifications about ongoing attacks from Spain, Italy and France. Most arguments invoked in the illegitimate e-mails are still negative, such as account blocking or expiration and account details update for security reasons.



The Top 10 list of counterfeit business identities in the first half of 2008 includes:

1. eBay
2. Paypal
3. Bank of America
4. Wachovia
5. Fifth Third Bank
6. NatWest
7. Poste Italiane
8. Sparkasse
9. Regions Bank
10. Volksbank

“Spammers and phishers continue to improve their skills in replicating and forging legitimate messages’ characteristics. However, the simple text e-mails proved their efficiency as well, rounding up the total figure of ID theft victims to 50,000 each month.” said Vlad Vâlceanu, Head of BitDefender Antispam Research Lab.

BitDefender’s Keep You Safe Guidelines

The trends BitDefender observed in the first half of 2008 show that malware creators focused their attention on Trojans production and distribution, as well as system vulnerabilities’ exploitation. E-mail spam based the largest part of its content on simple, non-obfuscated text and advertised mostly drugs, while the majority of phishing raids targeted US and EU countries.

For the second half of 2008, BitDefender expects cybercriminals to concentrate their efforts on make hay of Adobe® Flash® Player vulnerabilities, Web browsers’ and other Internet-related applications’ breaches, office document flaws, as well as social networks weaknesses.

You can secure your system and keep these e-threats away by following the recommendations below:

- install and activate a reliable antimalware, firewall solution and spam filter.
- update your antimalware, firewall and spam filter as frequent as possible, with the latest virus definitions and suspicious applications/files signatures.
- install and activate an Internet browser pop-up blocker.
- scan your system frequently.
- check on a regular basis with your operating system provider – download and install the latest securities updates, malware and malicious removal tools, as well as other patches or fixes.
- do not install any program or application that might require resource sharing without the permission of your system and/or network administrator.
- do not open or copy on your computer any file, even if it comes from a trusted source, before running a complete antimalware scan.
- do not open e-mails and e-mail attachments from senders you do not know.
- do not open e-mails with odd entries in Subject line.
- do not respond by submitting any personal information (such as user names and passwords, social security number, bank account or credit card numbers) to e-mail requests from social, financial or commercial institutions requiring you to update your profile. Most of these organizations usually do not send general e-mails (addressed to a *Dear customer*), but customized printed notification forms (including your full name, as well as other unique identification details) through a regular postal service. If you have any doubt about an e-mail you received from such organization contact them immediately.
- do not click any links indicated in the spam e-mails, including the “unsubscribe” ones; you might trigger other malware and compromise your system’s security.
- do not click the links provided by unwanted pop-up windows.
- always delete the spam messages; if you accidentally open them, display the attached images or click links within their corpus you simply indicate the spam-

mers your e-mail account is active and available to receive more spam or you may trigger and install other malware.

- do not unsubscribe, opt-out or reply to any spam message; you might confirm your e-mail address is active and available for receiving even more unwanted messages.
- when browsing the Internet, do not submit your e-mail address and personal information when requested by suspicious web pages.
- when purchasing goods and services online, refrain from signing up for any additional service or promotion, as well as other online subscriptions, advertised on the seller's website unless you really need them.
- avoid placing your e-mail address on websites, guest books, newsgroups, contact lists, shopping or gift lists.
- when publishing your e-mail address, use a "munged" (intended alteration of) e-mail address, such as *myaddress[at]domainname[dot]com*, instead of using the @ and . signs.
- use at least two e-mail addresses. Create one e-mail account and use it for your correspondence with people you know and a second e-mail account for the websites forms requiring an e-mail address to allow content access.
- avoid typing sensitive personal information (such as user names and passwords, social security number, bank account or credit card numbers) from a computer outside a secured network (like a public Internet Café) or not protected by a reliable security solution.

BitDefender® is the creator of one of the industry's fastest and most effective lines of internationally [certified security software](#). Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe – giving them the peace of mind of knowing that their digital experiences are secure. BitDefender solutions are distributed by a global network of value added distribution and reseller partners in more than 100 countries worldwide. For more details about BitDefender's security solutions, please check www.bitdefender.com.