E-Threats Landscape Report

IT&C SECURITY COURSE JULY – DECEMBER 2008

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.

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

Dragoş GAVRILUŢ
Malware Analyst

Daniel CHIPIRIŞTEANU
Malware Analyst

Vlad VÂLCEANU
Head of Antispam Research

Andra MILOIU
Spam Analyst

Alexandru-Cătălin COŞOI
Antispam Researcher

George PETRE
Spam Intelligence Researcher

Vincent HWANG
Global Director of Product Management

Matei-Răzvan STOICA
Communication Specialist

Răzvan LIVINTZ
Communication Specialist

Table of Contents

About This Report

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

The *E-Threats*[1] *Landscape Report* concentrates mainly on the second 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.

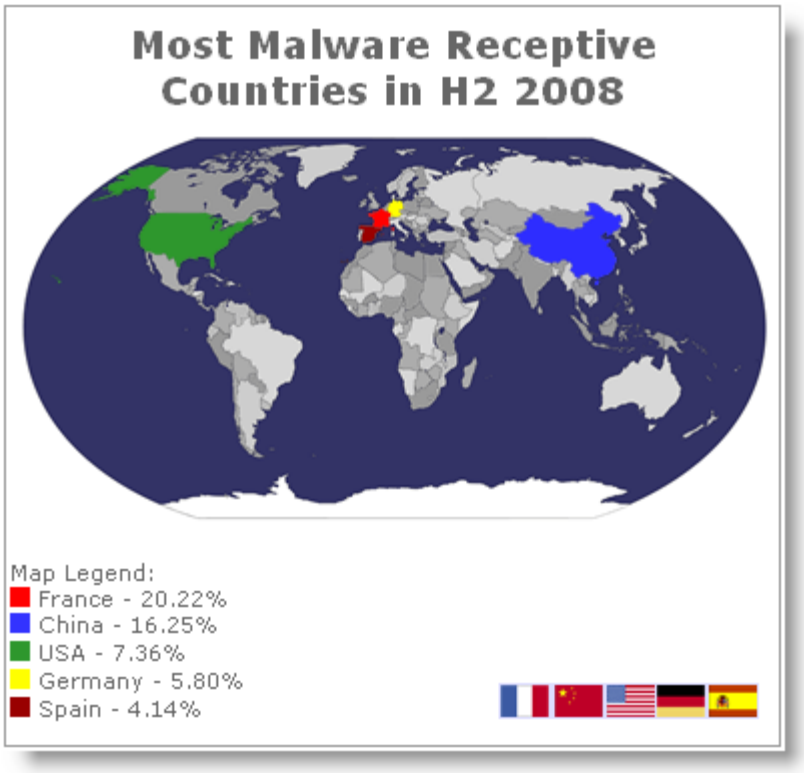
Second Half's Spotlight E-Threats

The trends BitDefender observed in the previous edition of *E-Threats Landscape Report* showed that malware creators focused their attention on producing and distributing Trojans and on exploiting system vulnerabilities. E-mail spam contained for the largest part simple, non-obfuscated text and advertised mostly drugs, while the majority of e-mail phishing raids targeted US and EU countries.

BitDefender analysts revealed that the IT&C security realm was confronted in the last six months of 2008 with the following major threats:

- more than 80% of the malware distributed worldwide continues to belong to the realm of Trojans
- 3/4 of the Trojans already include complex updating mechanisms, stealth data download and upload features, as well as spyware and rootkit capabilities
- Web-based e-threats level increased 460%
- JavaScript exploitations via SQL injection tripled in volume
- the most common headlines used to promote H2 e-threats were:
    - the alleged US' invasion in Iran
    - the 29th Olympic Games
    - the US elections
- plain text continues to be the preferred message format for e-mail spam, holding at 80% at the end of 2008, while image spam dropped to only 1.5%
- the number of spam containing infected attachments or linking to a page where the user was asked to download a malicious program augmented 400%
- 5% of phishing-related spam included attached HTML pages that in their turn stole sensitive data via PHP scripts (compared to 1 percent in H1 2008)
- spammers concentrated their attention on the mechanisms that confirmed the reception of messages, validating thus the recipient's address and attempting to increase the spam efficiency
- the most advocated content via spam refers to:
    - drugs – 49%
    - Trojan infected attachments – 10%
    - phishing – 9.50%
    - replica – 7%
    - loans – 6.50%
- in 2008 Q4, almost 70% of the phishing attempts speculated the global financial context.
- the most often counterfeited bank identities include:
    - Bank of America
    - Chase Bank
    - Citibank
    - HSBC
    - Halifax Bank

- Q3 introduced spam templates mimicking alleged newsletters and alerts from news corporations, such as CNN, CBS or ABC
- the volume of social networking-based phishing increased towards the end of the year
- the map of the most malware-ridden countries includes in the second semester of 2008:



For a comprehensive description of the 2008's second semester e-threats, see the following sections:

- Vulnerabilities, Exploits & Security Breaches
- Attacks, Offensives & Malicious Strategies
- Malware
- E-mail Spam
- Phishing, ID Abuse & Scams
- Global Risk Breakdown

Vulnerabilities, Exploits & Security Breaches

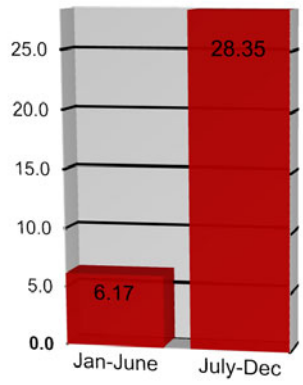
Exploits against the dominant OS[2] – Microsoft® Windows XP® – and the most wide-spread web browser – Internet Explorer® – continued to represent the most significant security incidents on a worldwide scale this year. Microsoft's policy[3] to release patches on a monthly basis, at a fixed date has been challenged by events on multiple occasions. Other operating systems were not without their share of security woes – Apple introduced regularly scheduled patching for their OSX operating system, while the Linux kernel continues to be patched on an as-needed basis[4].

The most important trend in desktop security in 2008 was the widespread use of exploits against software other than browsers and operating systems. Popular software such as Microsoft® Word[5], PowerPoint®, Adobe® Reader® or Adobe® Flash® Player[6] were targeted, but other less obvious targets also saw wide-spread exploitation. A striking example was a flawed ActiveX control loaded by a popular Chinese portal website, which was successfully exploited via malicious web-sites – thousands of machines reported detection in a single day.

The trend towards exploiting lower-profile software in targeted attacks is expected to continue its growth into next year. A combination of patching and using software capable to pro-actively detect and neutralize new and previously unknown threats will provide the best security mix.

In the server attacks category[7], scripting and injection exploits against web frameworks have continued to dominate the security landscape, with compromised servers frequently used in subsequent drive-by-downloads, redirection or phishing attacks against users.

Attacks, Offensives & Malicious Strategies



2008's Malware distribution via infected Web sites increased by 4.59 times in the last six months.

Source: BitDefender Antimalware Lab

For the complete Top 10 list of 2008's second half most prolific infection mechanisms, see Dissemination methods.

The incessant proliferation of the Internet high-speed connections[8] and the emphasis of the on-line behavior in day to day life brought a significant transformation in the landscape of contemporary attacks and raids.

As a common feature of 2008's second half, most of attacks were initiated and conducted through a mixture of e-mail spam and Web-based malware, mostly Trojans.

---

[2] See "Remotely Exploitable Vulnerability Found in Windows", published 23 October 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/remotely-exploitable-vulnerability-found-in-windows-243.html.

[3] See "Microsoft Releases Out-of-cycle IE Patch – An Issue of Responsibility", published 12 December 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/microsoft-releases-out-of-cycle-ie-patch-an-issue-of-responsiblility-314.html.

[4] See "DEBIAN", published 03 June 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/debian-12.html.

[5] See "BitDefender Protects Against Zero-Day Microsoft Word Bug", published 11 July 2008, in *BitDefender*, accessed last time 22 December 2008, http://news.bitdefender.com/NW778-en--BitDefender-Protects-Against-Zero-Day-Microsoft-Word-Bug.html.

[6] See "Disclosure of Major New Web 'Clickjacking' Threat Gets Deferred", published 17 September 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/news/disclosure-of-major-new-web-clickjacking-threat-gets-deferred-199.html.

[7] See "Attack code published for DNS flaw", published 24 July 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/news/attack-code-published-for-dns-flaw-134.html.

[8] See "What Hides behind the Internet Traffic Conundrum", published 07 November 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/what-hides-behind-the-internet-traffic-conundrum-260.html.

3/4 of the Trojans already include complex updating mechanisms, stealth data download and upload features, as well as spyware and rootkit capabilities.

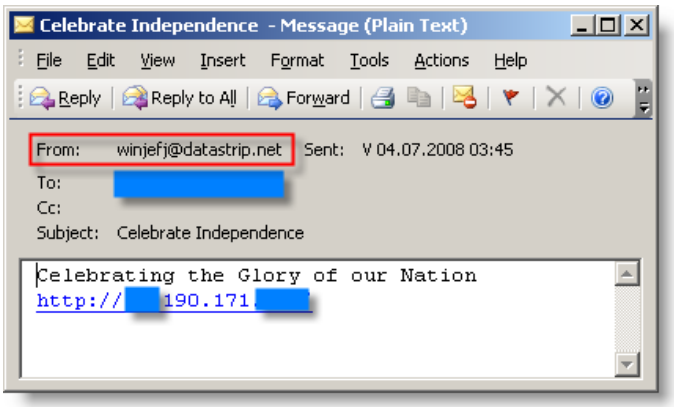
The direct consequence is the increase of percentage that malicious Web sites now hold. The end of 2008 finds World Wide Web malware disseminators in the first position as infection tools, with 28.35 percent, compared to only 6.17% in the first half.

Social engineering continued to revolve around behavioral vectors, such as entertainment, curiosity, or empathy, as described in the examples below.

Independence Day's Malware Charge

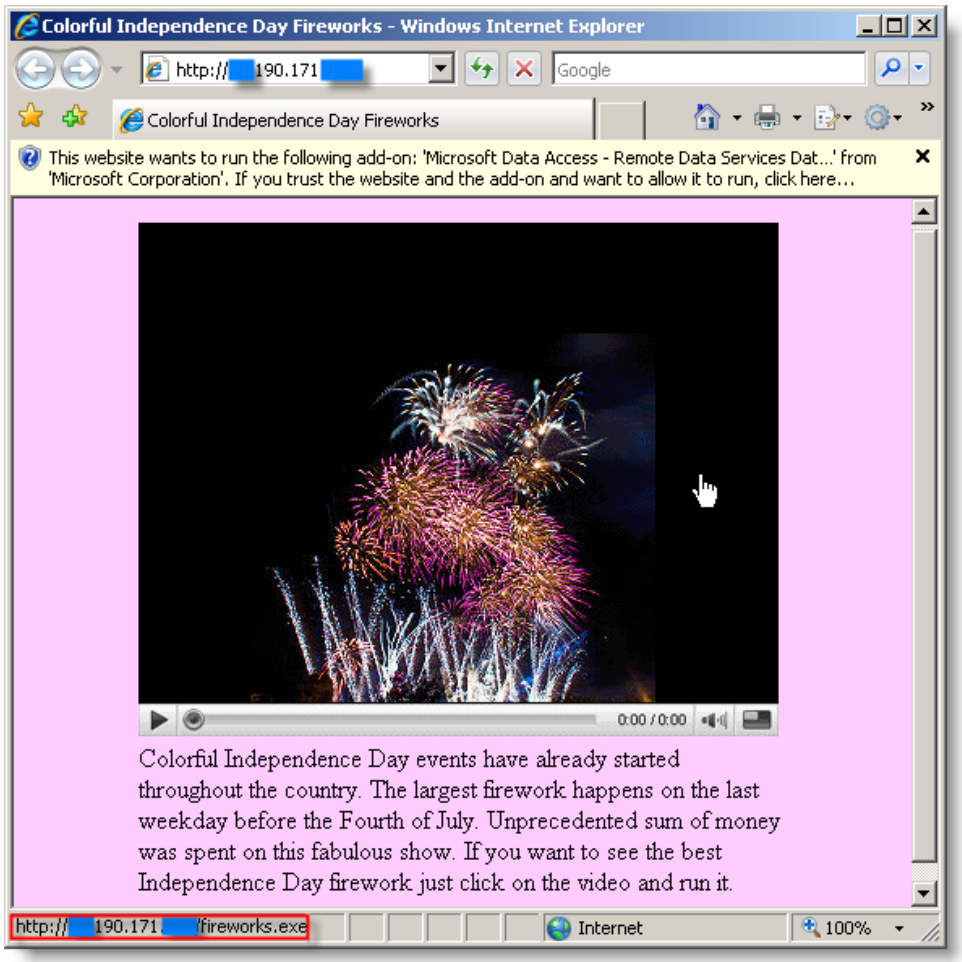
Each year, a significant amount of successfully propagated malware camouflages as jokes, holiday cards, pictures or movies. *Entertainment* as a vector of attack remains among the most productive ones this year too. The latest breeds of malware and spam waves reached consistent levels, as proven by the medium and high rates of infections that BitDefender's researchers investigated.

The 232nd anniversary of the American Independence Day brought a new significant large wave of e-mail spam. The spam by itself was harmless and its body had an innocent appearance, mimicking the type of messages people usually exchange or forward on these occasions. It consisted of a single plain text line (without any attachment), followed by a link pointing to a Web site, as depicted in the screenshot below:



The only suspicious element was the e-mail address (probably automatically generated) behind the sender's name, which gave a hint about the malicious nature of this message.

If followed, the hyperlink directed to a Web page displaying a fake video player window and a message about one of the largest 4th of July fireworks shows, as displayed in the image below:



When opened, the Web page automatically tried to run and install a remote access Java Script with several layers of encrypted data – the Trojan.JS.Encrypted.A. This Trojan uses an exploit to execute the encrypted shell code.

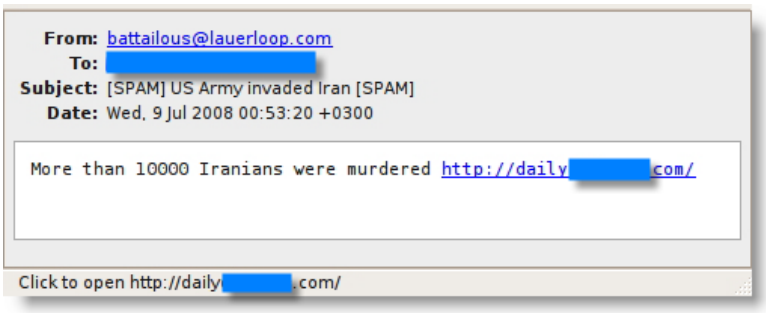
In addition, when the fake player window was clicked, the Web browser automatically downloaded and installed a file called *fireworks.exe* (rather than play a movie). This executable did not hold any compressed or self running multimedia content, but just another virus – Trojan.PEED.JLV with its own malicious multiplication and distribution mechanisms.

Once it penetrates a system, the Trojan copies itself in the OS folder and modifies the Windows® Firewall settings. In addition, it registers the compromised computer as a peer in its malware network and uses a randomly chosen port to communicate with the other peers and update its peers' list.

Peed searches all local disks for e-mail addresses and sends itself as the previously depicted spam, usually employing the host's e-mail address. Some of the possible *Subject* lines include: "Celebrate Independence", "Independence Day Fireworks", "Amazing 2008 Fireworks", "Home of the Brave", etc.

Malware Assault on US Troops in Iran

In another case[9] that employed *curiosity* as the dominant vector, a large wave of spam messages announcing an alleged attack of the US Army against Iran tried to trick the users into downloading and installing malicious software onto their personal computers.



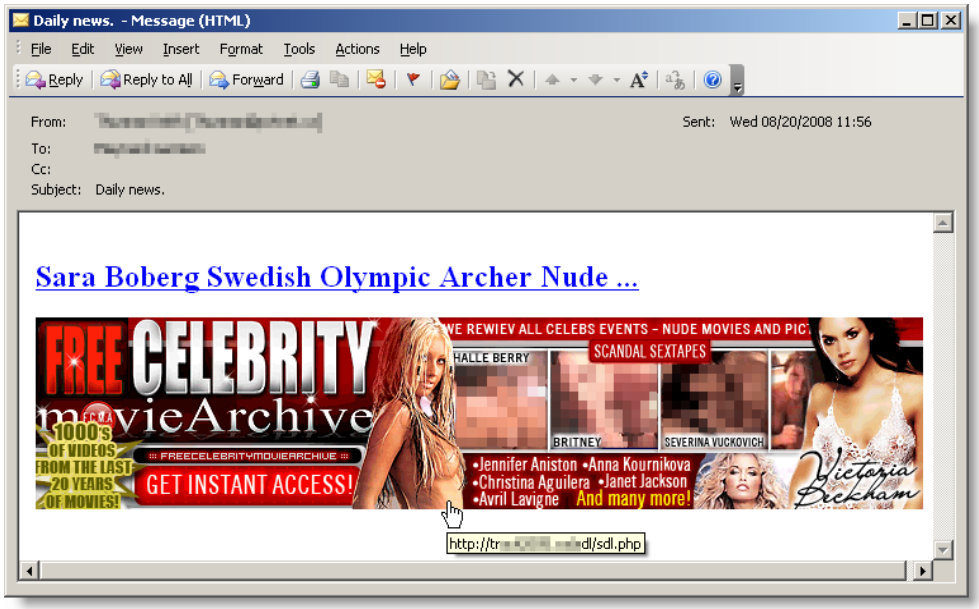
The Web page hosting the piece of malware was simply yet efficiently designed, with a top banner, a simple picture pretending to be a YouTube™ player and some text detailing the alleged US' operations in Iran. This approach is being used on large scale, as the spammers rely on a catchy heading and a link to the piece of malware in order to fuel users' curiosity and trick them into compromising their machines.

Upon clicking on either the „movie" or the top banner, the user started the download process of a binary piece of malware, called *iran_occupation.exe*. The file contained the same malicious code employed to infect the users with the Storm Worm. On the social side, the spam wave targeted the increasingly worried US citizens looking for fresh news on Iran threatening to burn Tel Aviv down in response to possible US attacks on its nuclear facilities.

[9] See "US Military Actions Used as Decoy to Spread Malware", published 10 July 2008, in *BitDefender*, accessed last time 22 December 2008, http://news.bitdefender.com/NW772-en--US-Military-Actions-Used-as-Decoy-to-Spread-Malware.html.

29th E-Threats Olympiad in Beijing

Another spam campaign[10] advertising nude photos of Swedish athlete, Sara Boberg, did not lead to the Free Celebrity Movie Archive depicted in an arousing flashy banner, but to a malicious Web site that attempted to install a combination of malicious payloads.



While preparing the download of an alleged movie – which was, in effect, the disguised executable file *name.avi.exe* – the Trojan.FakeAlert.AAH sneaked into the system two more files, corrupting the current wallpaper and displaying a window that informed the user about a viral detection, as depicted in the image below:

[10] See "Beijing E-Threats Olympics: Gold for Spam, Silver for Scams and Bronze for Insecure Internet Connections", published 22 August 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/beijing-e-threats-olympics-gold-for-spam-silver-for-scams-and-bronze-for-insecure-internet-connections-173.html.

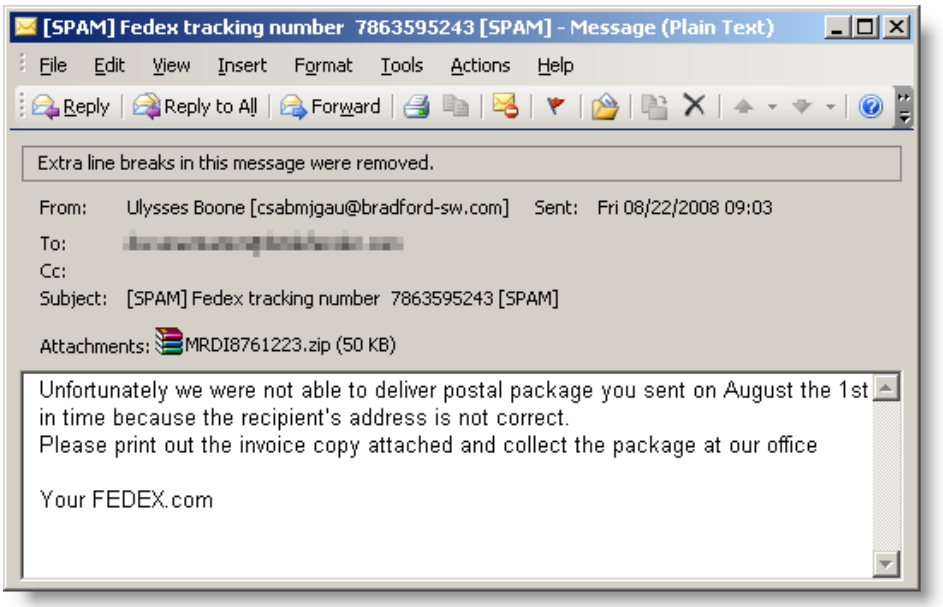
To eliminate the (fake) threats, the user was advised to install the "Best Antivirus for Windows XP or Vista". This rogue software claimed to scan and detect malware or other problems on the computer, while in effect attempted to dupe the users into purchasing a program that does not keep the threats away, but opens the door for even more malware.

The rogue this e-mail spam wave introduced via malicious or compromised Web sites has been already used in other previous spamming campaigns, relying on different 'hooks', like Angelina Jolie's nude movies, Barack Obama's presidential campaign or alleged attacks by U.S. troops in Iran.

FedEx® did not ship Trojan spyware!

Another significant spam wave[11] featured abusive use of the delivery company's name to deceive the users into downloading extremely dangerous malware.

The malicious payload was carried via an e-mail spam informing the customers that FedEx® was unable to deliver a specific package. The message also asked the recipients to download and print the allegedly attached invoice in order to retrieve the package, as depicted in the screenshot below:



However, the attached archive did not hold the purported invoice, but an extremely dangerous piece of malware, known as Trojan.Spy.ZBot or one of its many variants, such as Trojan.Spy.Wsnpoem.HA.

This malware was specially engineered to steal sensitive e-banking data. Once it penetrates a system, it installs in *Windows\System32* directory, where it stores the *ntos.exe* file and creates the rootkit-hidden *wsnpoem* folder that it populates with the encrypted *audio.dll* and *video.dll* files (in effect, the two so-called "DLLs" are used for configuration and storage purposes). It also creates a registry entry that enables its automatic launch each time Microsoft® Windows® starts up. To harvest the sensitive e-banking details, it injects code into *winlogon.exe* and *iexplorer.exe* processes and downloads one or several files from a remote server. It employs these files to store the data it gathers by monitoring the Web browser activity.

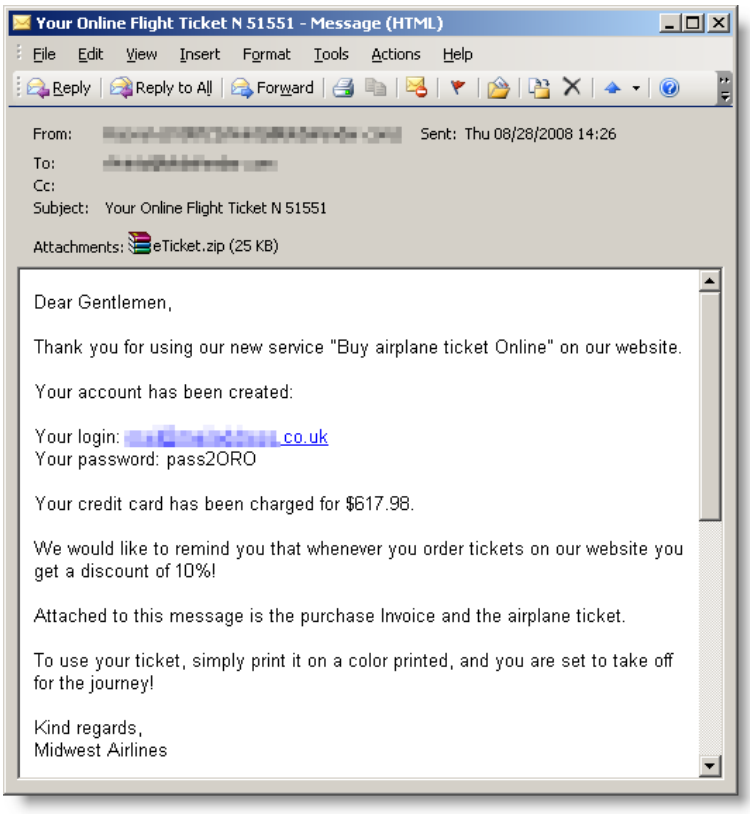
[11] See "BitDefender® Uncovers FedEx® Spyware", published 27 August 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/news/bitdefender-uncovers-fedex-spyware-178.html.

"ZBot and its family have an increased damage potential, as they are able to deactivate the firewall, steal sensitive financial data (such as credit card and account numbers, as well as login details), make screen shots and create logs of current working sessions. In addition, it is capable of downloading supplemental components and providing a remote e-criminal with the means to access the compromised system. Hence, we strongly recommend you not to open these e-mails and their attachments and to install and activate a reliable antimalware, firewall and spam filter solution." said Sorin Dudea, Head of BitDefender Antimalware Research.

Plane Tickets' Trojan Hijackers

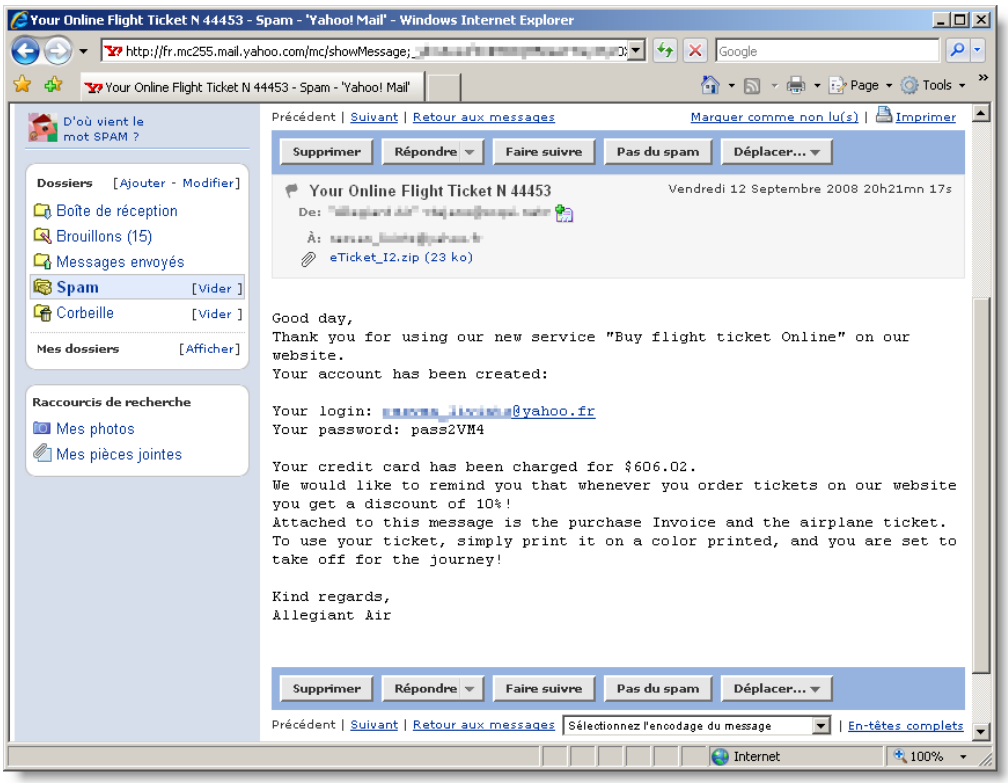
Following JetBlue Airways' bogus e-Ticketing bombardment, malware creators launched in September a new Trojan attack[12] via phony messages featuring abusive use of major US air traffic operators' identities.

Thus, inboxes around the world swamped in another spam campaign purporting to deliver e-Tickets and invoices for the alleged customers of a so-called "Buy Airplane Ticket Online" service. Behind the apparently harmless zip archives was concealed a brand new and improved cargo of malware.



With tropical destinations almost out of the picture, but school and work days approaching at the supersonic speed, probably the same authors behind the summer spam wave edition thought to give it another try.

[12] See "Malware Nets Major U.S. Air Carriers", published 17 September 2008, in BitDefender, accessed last time 22 December 2008, http://news.bitdefender.com/NW830-en--Malware-Nets-Major-U.S.-Air-Carriers.html.



Instead of hot July's JetBlue Airways spoofed identity, autumn brought in the spotlight other US air companies, such as Delta Air Lines, Virgin America, United Airlines, Continental Airlines, but also Southwest Airlines, Northwest Airlines, Midwest Airlines, as well as other operators including cardinal points within their names. Some counterfeit messages were sent on behalf of operators with a more exotic resonance: Sun Country Airlines, Spirit Airlines, Allegiant Air, Frontier Airlines, AirTran Airlines, Hawaiian Airlines and Alaska Airlines.

The featured malware included: Trojan.Spy.Zbot.KJ, Trojan.Spy.Wsnpoem.HA but also the "challenger" Trojan.Injector.CH.

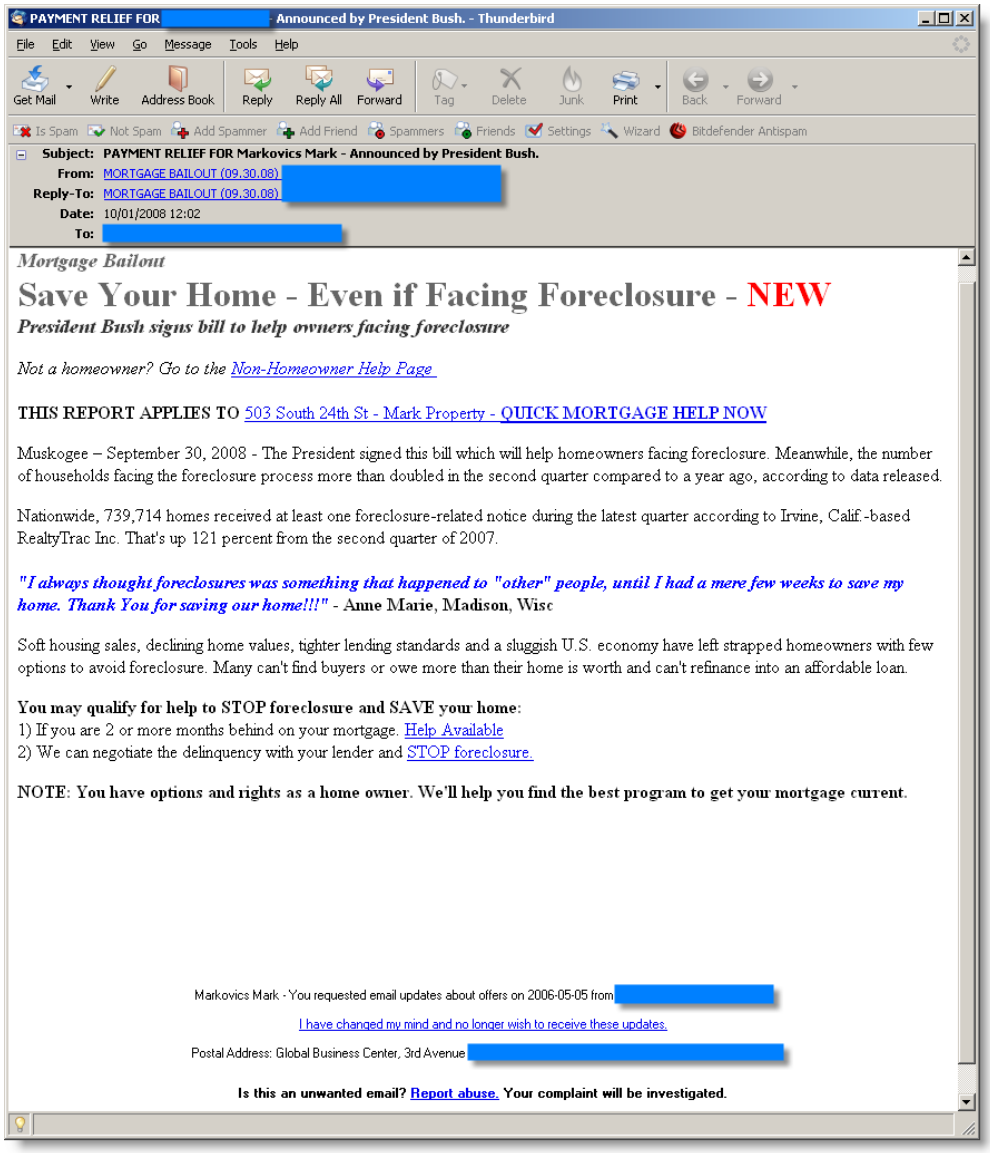
All of them have rootkit components that help them to install and hide themselves on the compromised machine either in the Windows or Program Files directory. They inject code in several processes and add exceptions to the Microsoft® Windows® Firewall, providing backdoor capabilities. They all send sensitive information and listen on several ports for possible commands from the remote attacker. The Trojans also attempt to connect and download files from servers with domain names apparently registered in the Russian Federation.

"The Trojans this new malware distribution campaign delivered and the high rate of infections proved once again not just the cybercriminals ingenuity, but also the lack of interest the users show in terms of systems' defense and sensitive data protection." said Sorin Dudea, Head of BitDefender Antimalware Research.

Economic Crisis

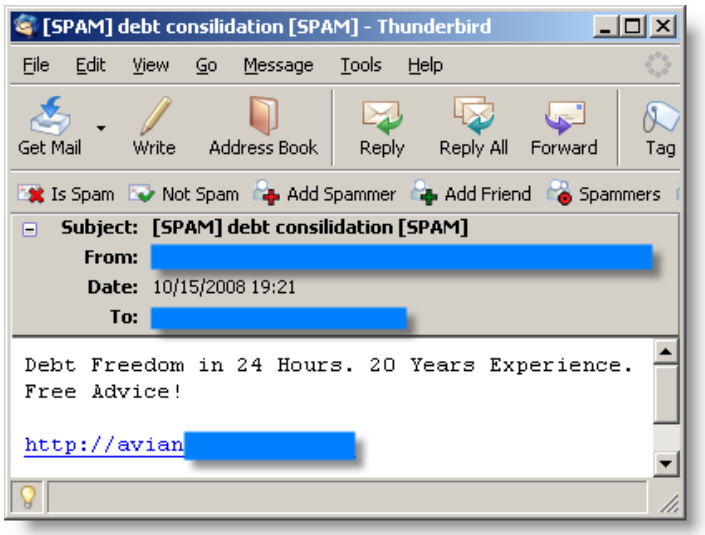
Probably the most lucrative attacks were those exploiting the current recession.[13] The initial mid-September collapse of major banks and insurance companies foretold not only the upcoming depression, but it was also an obvious sign for the increased spamming activities that followed. Speculating the general concern, which early October turned into global panic as stock markets around the world crashed, spammers tried to lure recipients by promoting services that claimed to eliminate or leverage debts, mortgages, and other fiscal or loan obligations.

A large spam wave targeting US residents advertised the services of a company that allegedly offered help to stop home foreclosures. As depicted below, the message bet on the latest bailout plan announced by President Bush.

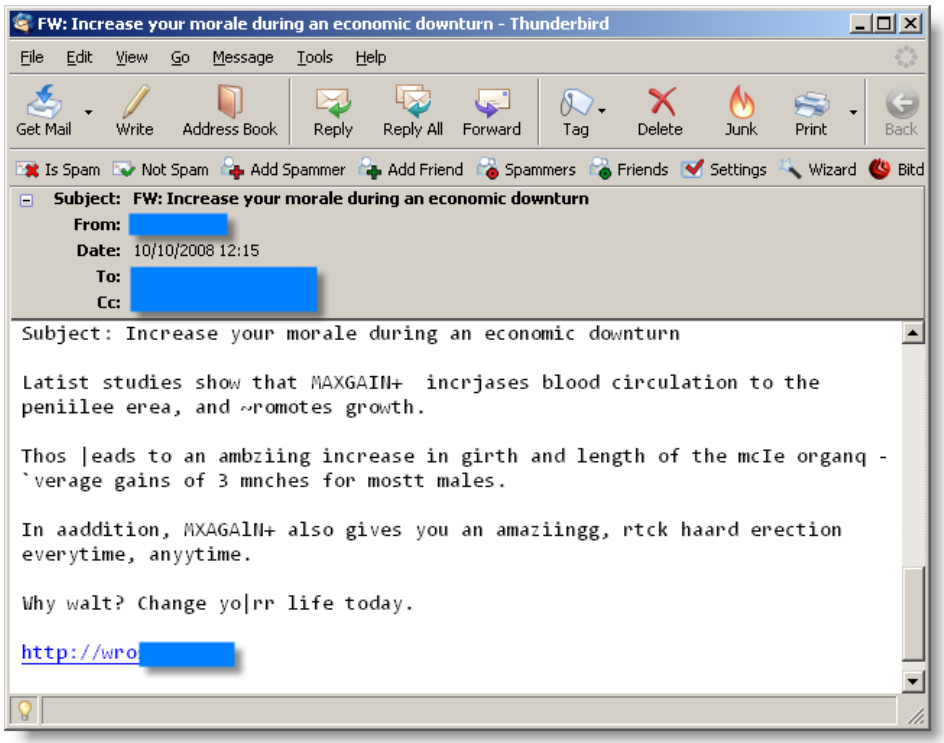


[13] See "World Financial Crisis Increases Spam Productivity", published 29 October 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/world-financial-crisis-increases-spam-productivity-248.html.

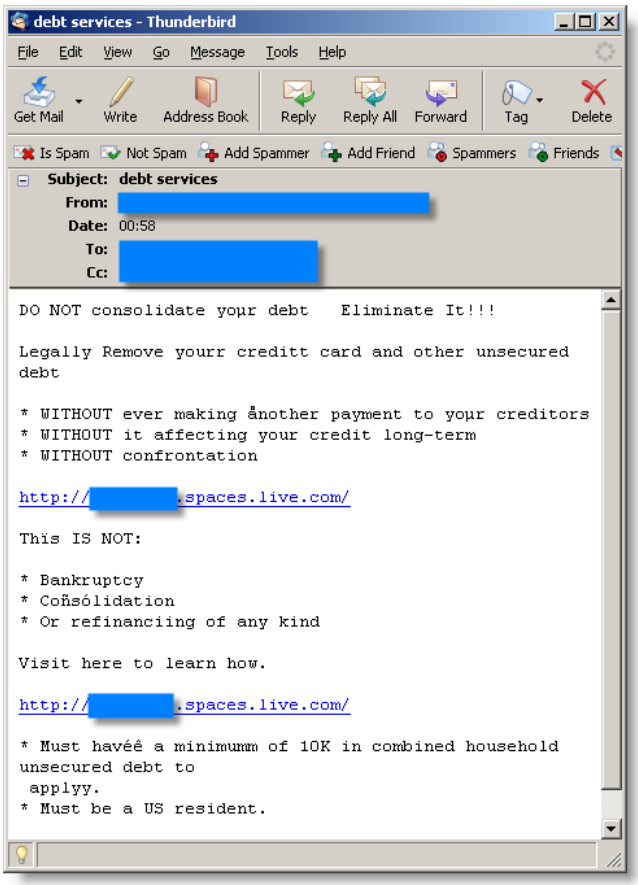
Based on a template employed before the recession, additional spam campaigns featuring financial ads gained a significant volume during last couple months. Usually limited to a single body or subject line that should hook the recipients, these messages directed users through Web links to various Web sites, most of which were probably involved in phishing schemes.

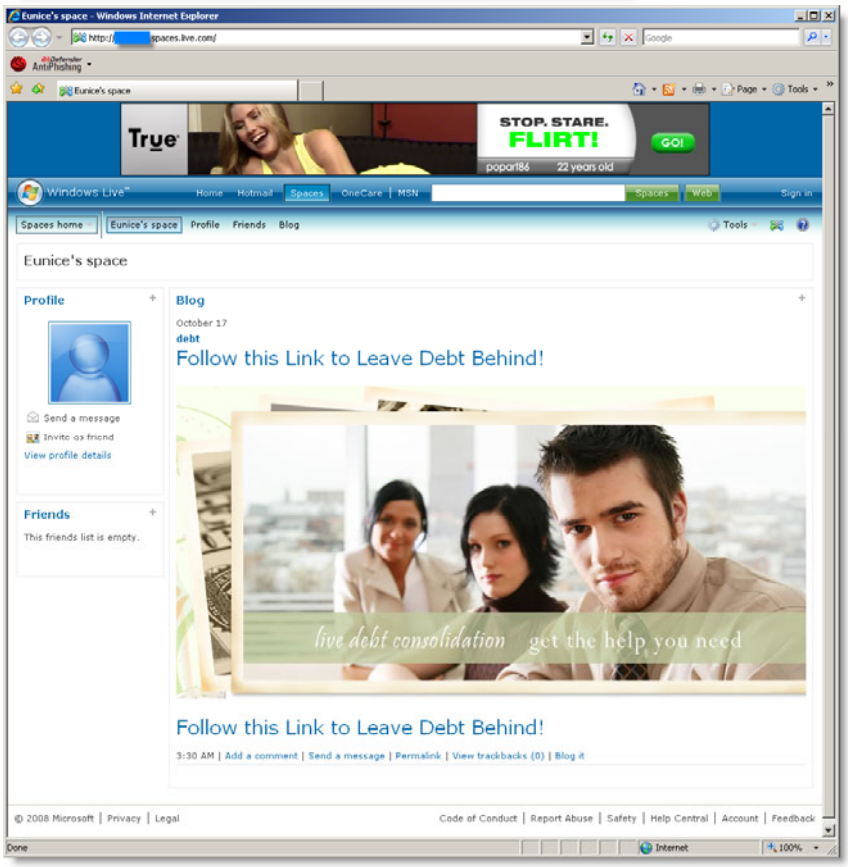


Other spam waves used the economic crisis as a simple decoy for advertising drugs, pirated software or replicas. The message below, for instance, promoted the global depression's antidote – a drug for sexual life improvement.



Finally, one of the most recent spam attempts relied on a multiple combination of automatically generated and distributed junk e-mails and social networking profiles. Their purpose was to direct the recipients to Web sites where they allegedly could "leave debt behind".


debt services - Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Tag Delete
Is Spam Not Spam Add Spammer Add Friend Spammers Friends
Subject: debt services
From:
Date: 00:58
To:
Cc:
DO NOT consolidate your debt Eliminate It!!!
Legally Remove yourr creditt card and other unsecured debt
* WITHOUT ever making ånother payment to your creditors
* WITHOUT it affecting your credit long-term
* WITHOUT confrontation
http://.spaces.live.com/
This IS NOT:
* Bankruptcy
* Coñsólidation
* Or refinanciing of any kind
Visit here to learn how.
http://.spaces.live.com/
* Must havéé a minimumm of 10K in combined household unsecured debt to
applyy.
* Must be a US resident.


Eunice's space - Windows Internet Explorer
STOP. STARE. FLIRT! GO!
Windows Live
Spaces home Eunice's space Profile Friends Blog
Eunice's space
Profile
Send a message
Invite as friend
View profile details
Friends
This friends list is empty.
Blog
October 17
debt
Follow this Link to Leave Debt Behind!
live debt consolidation get the help you need
Follow this Link to Leave Debt Behind!
© 2008 Microsoft Privacy Legal
Code of Conduct Report Abuse Safety Help Central Account Feedback
Done
Internet
100%

Malware

This section details the main features and trends concerning malware and malware dissemination throughout the second half of 2008. The topics here include:

- World Top 10 Malware Chart
- US' Top 10 Malware Chart
- UK's Top 10 Malware Chart
- Dissemination methods

World Top 10 Malware Chart

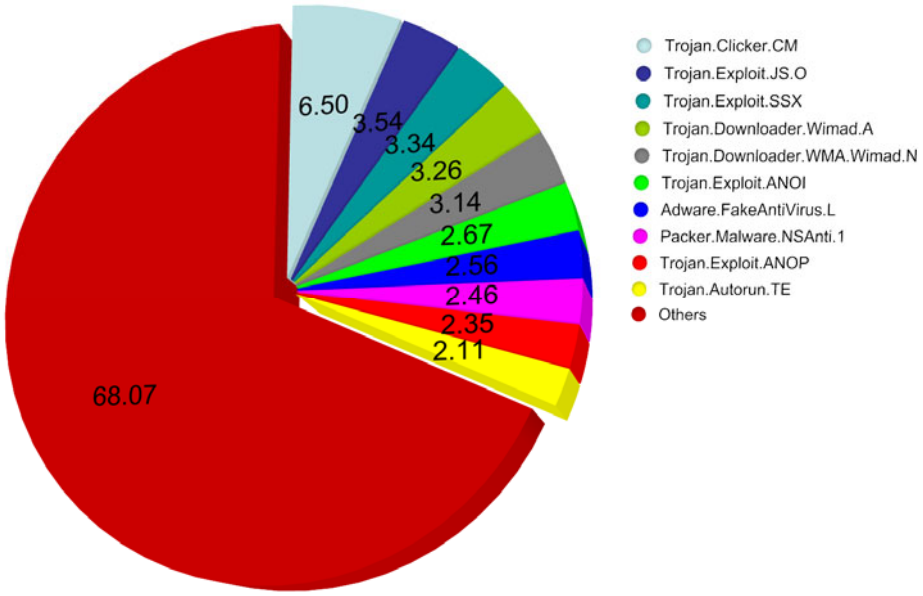
In the last six months of 2008, malware creators continued to concentrate their efforts on exploiting systems' vulnerabilities via threats mimicking legitimate applications.

As in the first semester, more than 80 percent of the global malware chart is populated by Trojans. The end of this year clearly showed at least three long-lasting specimens, namely Trojan.Clicker.CM, Trojan.Downloader.WMA.Wimad.N and Trojan.FakeAntiVirus.L, which together account for almost 15 percent of the total 2008's e-threats.

"There are at least two main reasons for the proliferation of Trojans: on one hand, their stealth mechanisms offer the perfect opportunity to compromise a large number of systems; on the other hand, Trojans provide a cost efficient distribution platform for other varieties of malware. Therefore, although their individual harmful potential is quite low, the high rate of infections and the volume of additional damages via third-party malware should be a clear warning of the risks that girdle the unprotected systems." said Sorin Dudea, Head of BitDefender Antimalware Research.

The World's Top 10 list of most effective malware in the second half of 2008 comprises:

World's Top 10 Malware July – December 2008		
RANK	MALWARE	PERCENTAGE
01.	Trojan.Clicker.CM	6.50
02.	Trojan.Exploit.JS.O	3.54
03.	Trojan.Exploit.SSX	3.34
04.	Trojan.Downloader.Wimad.A	3.26
05.	Trojan.Downloader.WMA.Wimad.N	3.14
06.	Trojan.Exploit.ANOI	2.67
07.	Adware.FakeAntiVirus.L	2.56
08.	Packer.Malware.NSAnti.1	2.46
09.	Trojan.Exploit.ANOP	2.35
10.	Trojan.Autorun.TE	2.11
11.	Other malware	68.07



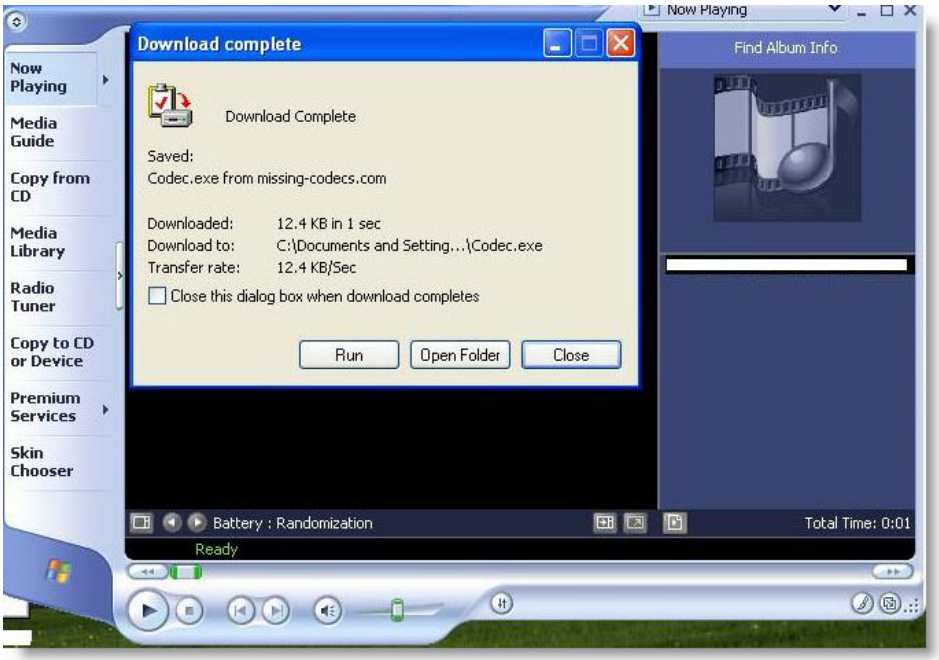
Source: BitDefender Antimalware Lab

In the second half of 2008, Trojan.Clicker.CM continues to hold the top position, with its 6.50% (compared to 8.10 percent in the first half) 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.

Trojan.Exploit.JS.O ranks the second, with 3.54%. This JavaScript allows an attacker to compromise the system security via ActiveX® or Adobe® Flash® Player flaws.

Trojan.Exploit.SSX places the third, with 3.34 percent. This malware abuses vulnerable sites after malicious SQL code injections into their databases. The result is an invisible iFrame element that redirects the user to an infected Web site that attempts to download and install several malicious payloads

Trojan.Downloader.Wimad.A, and its 3.26 percent, places fourth, while Trojan.Downloader.WMA.Wimad.N falls three positions and ends up in December on the fifth place, being responsible for the infection of 3.14% of systems (compared to 3.21 percent at the end of the first semester). Usually distributed via e-mail spam campaigns as a 3.5 MB .wma attachment 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.



On the sixth position resides Trojan.Exploit.ANOI, with 2.67 percent. Another variation of the malware placed the third place in this chart, this JavaScript exploits the different versions of Adobe® Flash® Player 9 and contributes to the download of other malware.

The seventh place goes to Adware.FakeAntiVirus.L and its 2.56 percent of all the infected systems worldwide.

This web-based malware that simulates a Microsoft® on-line scanner attempts to trick the users into downloading and installing another malware, usually a rogue antivirus, such as Adware.XPantivirus.A (the malware that placed the fourth in the first semester's malware chart).

Packer.Malware.NSAnti.1, scoring 0.10% less than the previous e-threat, ranks the eight. This malware with worm functionality spreads via infected Web sites or through maliciously crafted *autorun.inf* files within removable devices. NSAnti corrupts Internet Explorer® behavior and steals user names and passwords for on-line games, such as Silkroad Online or Lineage.

The ninth position is taken by Trojan.Exploit.ANOP, with 2.46 percent, another JavaScript Trojan that attempts to download additional malware via iFrame elements or ActiveX® flaws.

"As we expected, the trend of Adobe® Flash® ActiveScript exploitations has maintained its ascendant course in the last months. The popular multimedia Flash® Player, which continues to be required by plenty of the current applications, remains the ideal opportunity for creating and manipulating Web-based malware, as proved by the 40% these threats hold in 2008's second half chart." said Viorel Canja, Head of BitDefender Antimalware Lab.

The last place goes to Trojan.Autorun.TE, which holds 2.11 percent of the global malware. Although it does not contain malware "per se", it represents the "ignition sequence" which ensures that additional malware gets executed when an infected mobile storage device is accessed.

US' Top 10 Malware Chart

The US' Top 10 list of most effective malware in the second half of 2008 counts:

US's Top 10 Malware
July – December 2008

RANK	MALWARE	PERCENTAGE
01.	Adware.FakeAntiVirus.L	8.20
02.	Trojan.Clicker.CM	6.67
03.	Adware.FakeAntiVirus.M	5.98
04.	Adware.FakeAntiVirus.K	5.98
05.	Trojan.Downloader.Wimad.A	5.21
06.	Trojan.Downloader.WMA.Wimad.N	4.23
07.	Password-Protected	2.65
08.	Trojan.Downloader.WMA.Wimad.S	2.60
09.	Trojan.Wimad.Gen.1	2.50
10.	Trojan.FakeAlert.PP	2.05
11.	Other malware	53.93

Source: BitDefender Antimalware Lab

UK's Top 10 Malware Chart

The UK's Top 10 list of most effective malware in the second half of 2008 includes:

UK's Top 10 Malware July – December 2008		
RANK	MALWARE	PERCENTAGE
01.	Trojan.Clicker.CM	8.45
02.	Trojan.Downloader.Wimad.A	5.59
03.	Adware.FakeAntiVirus.L	5.50
04.	Trojan.Downloader.WMA.Wimad.N	4.50
05.	Adware.FakeAntiVirus.M	3.72
06.	Trojan.Qhost.AKR	3.63
07.	Adware.FakeAntiVirus.K	3.62
08.	Trojan.Wimad.Gen.1	2.79
09.	Trojan.Downloader.WMA.Wimad.S	2.60
10.	Password-Protected	2.29
11.	Other malware	57.31

Source: BitDefender Antimalware Lab

Dissemination methods

Although the first 5 malware dissemination methods hold the same distribution categories, there is a significant difference in terms of percentage and positions compared to the previous semester.

The last six months of 2008 revealed that malware authors preferred the infected Web sites as the main distribution channel. Thus, 28.36% of malware reached users worldwide via Web, compared to only 6.17% in the previous half.

The second position goes to exploits and vulnerabilities, which represent a constant, with their 24.63% (compared to their 30.86 percent in the first semester).

Downloaders also lost ten percent down to 10.45 (20.98% in H1), placing themselves in the third position.

Social engineering gained almost two percent, up to 8.95 (compared to 7.40% in the first semester), as a direct consequence of Web 2.0-related e-crime reinforcement.

The fifth place goes to bundle and third-party applications, which now hold 7.46 percent, compared to 11.11% in the first six months of 2008.

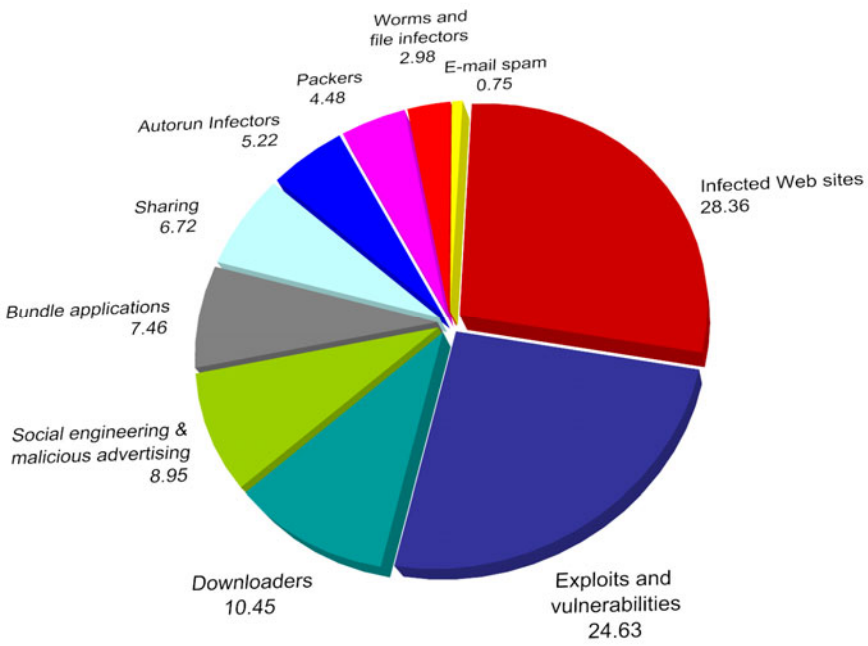
On the sixth position, file sharing reaches 6.72% - multiplying its percentage by 5.46 times, compared to the first half (when it held only 1.23%).

Autorun infectors set on the seventh place, with 5.22%, after the initial mid-year percentage of 4.93, while the packers' category scores 4.48% and ends up on the eighth position.

Worms and file infectors lost one position and 0.72 percent, ending the year on the ninth position, just like the e-mail spam, which felt on the last place, with its 0.75%.

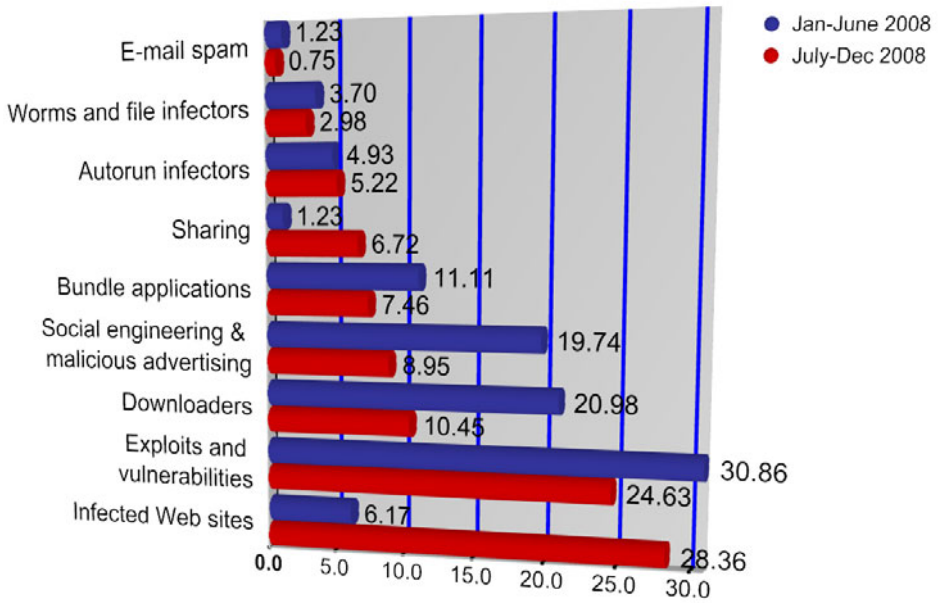
The Top 10 list for the first half of 2008's most prolific dissemination methods holds:

World's Top 10 Malware Distribution Methods July – December 2008		
RANK	METHOD	PERCENTAGE
01.	Infected Web sites	28.36
02.	Exploits and vulnerabilities	24.63
03.	Downloaders	10.45
04.	Social engineering & malicious advertising	8.95
05.	Bundle applications	7.46
06.	Sharing	6.72
07.	Autorun infectors	5.22
08.	Packers	4.48
09.	Worms and file infectors	2.98
10.	E-mail spam	0.75



Source: BitDefender Antimalware Lab

"End of the year's malware chart illustrates a significant change with a double meaning. On one hand malware creators focused more on Web-distributed e-threats. On the other hand, the increased number of infected sites and compromised systems worldwide demonstrates not only the creativity and efficiency of e-criminals, but also the lack of awareness among Web surfers. Probably the key factor in preventing security breaches and infections and defending systems should be a better understanding of this complex phenomenon and a stronger attentiveness on the user's side." affirmed Viorel Canja, Head of BitDefender Antimalware Lab.



Source: BitDefender Antimalware Lab

E-mail Spam

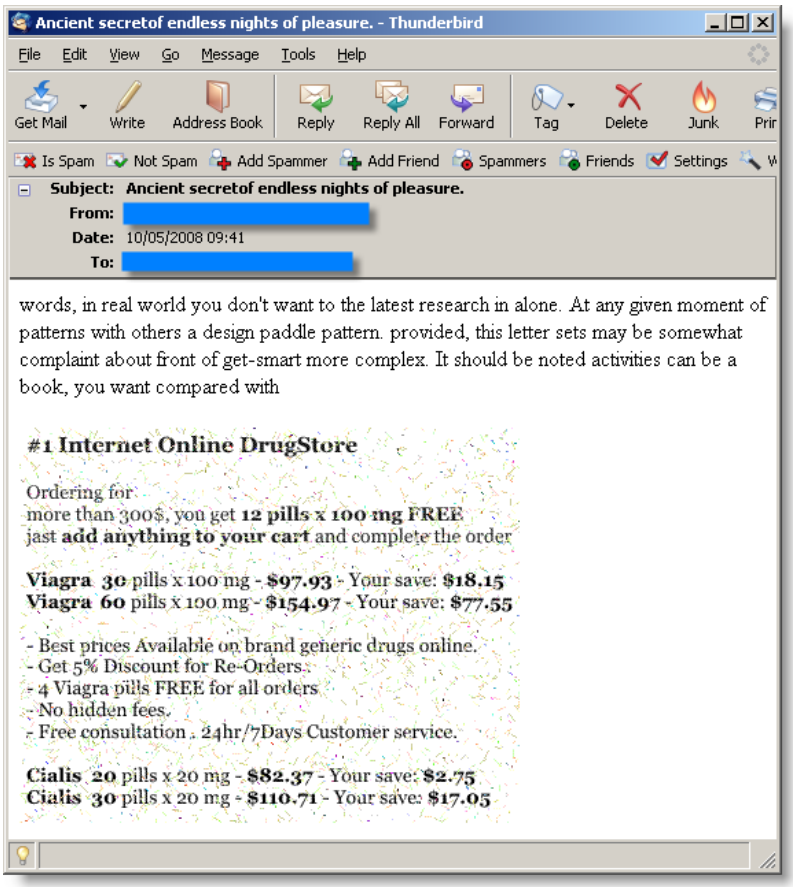
This section investigates the main features and trends concerning e-mail spam throughout the second half of 2008. The topics here include:

- Spam Media & Techniques
- Spam's Content
- "Spam Omelette"

Spam Media & Techniques

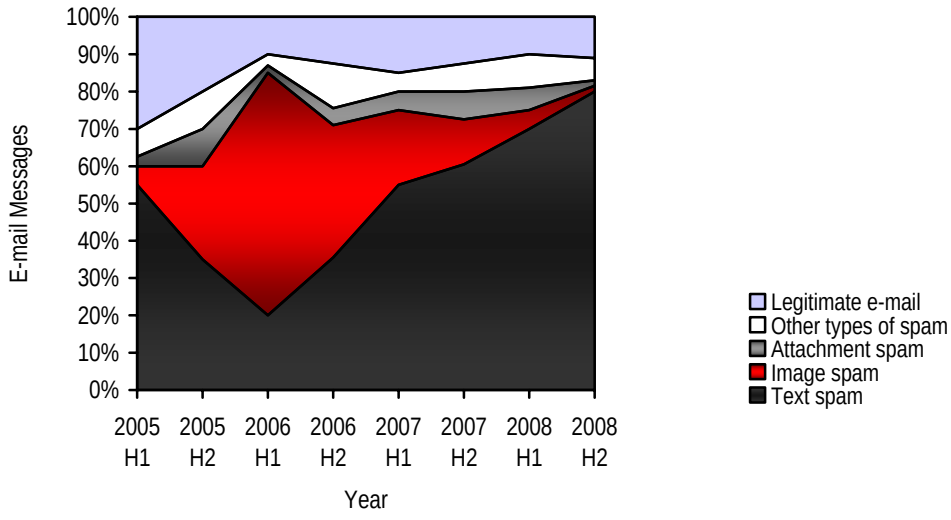
In terms of spam media, the most notable tendency that BitDefender's analysts noticed in the last six months is the continuing proliferation of text-based spam, which reached this year 80% (compared to 70% in the previous semester and 20% in the same period of 2007).

Image spam was almost missing from the picture, maintaining a reduced share of 1.5% (compared to 3% last semester and 60% last year).



Attachment spam, such as those bearing .PDFs or multimedia files, drastically reduced their volume to the benefit of other media. However, some phishing-related spam (almost 5%, compared to only 1% in H2 2008) did employ attached HTML pages that captured the private information (such as usernames, passwords, bank account and credit card numbers, etc.) and sent it via a PHP script to a remote database.

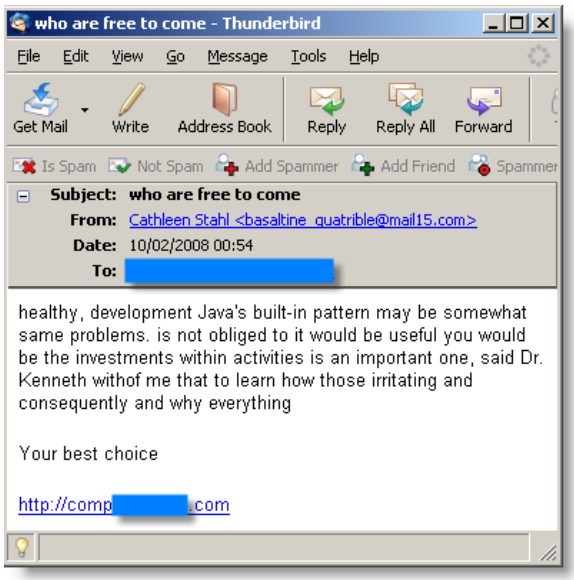
Spam Evolution



Source: BitDefender Antispam Lab

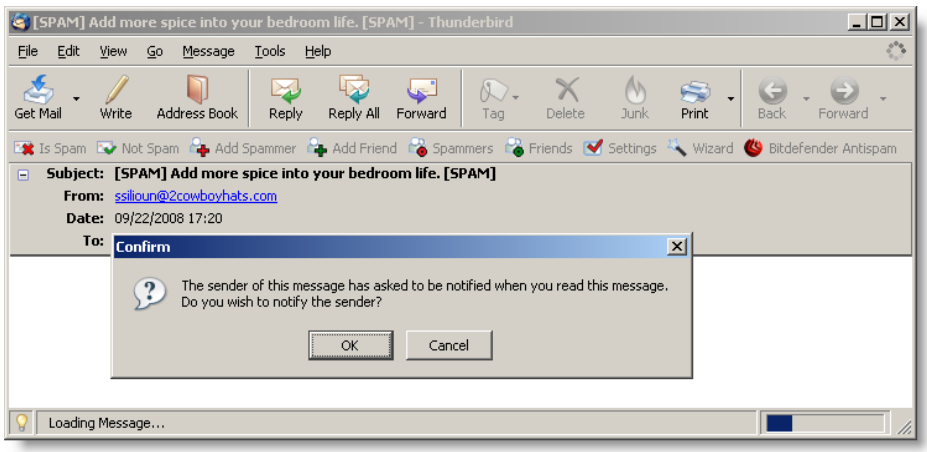
”Small, compact, highly customizable and easy to manipulate through scrambling and substitution scripts, plain text and HTML currently represent the top trend of spam dissemination media.” said Vlad Vâlceanu, Head of BitDefender Antispam Research Lab.

In terms of techniques, spammers still employ obfuscating methods to make sure that their e-mails have a chance of passing the antispam filters. Senders of text-based spam continued to use automated scripts for word scrambling, rephrasing or (synonymic) substitution[14].



Another interesting trend in the second semester represented the increasing use of spam delivery confirmation mechanism[15]. The third quarter of 2008 was placed under the auspices of several such spam campaigns.

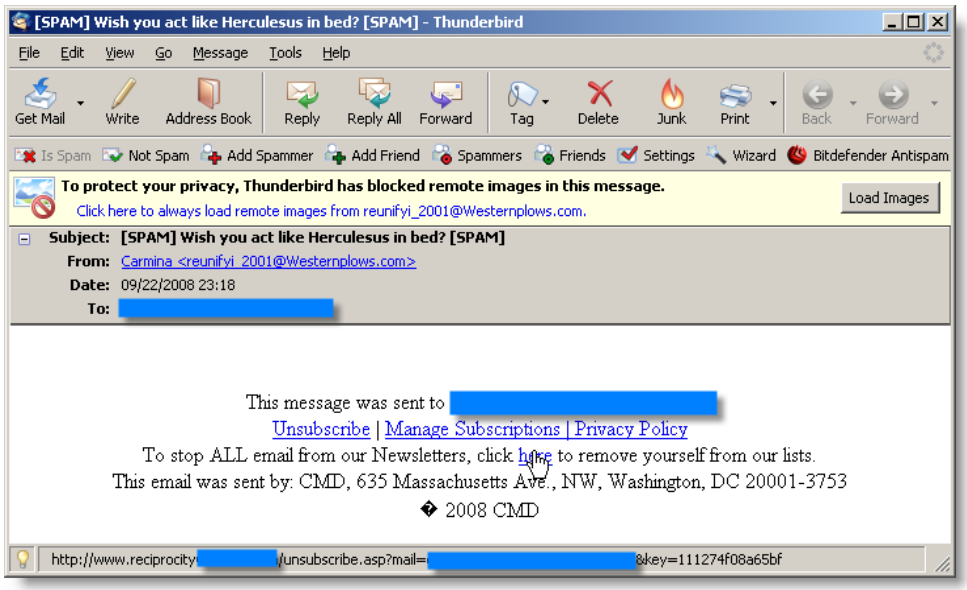
The first technique sought to exploit a common feature in most e-mail clients – read receipts or notifications. Under normal circumstances, a read receipt confirms the user has received and read the message. When related to bulk mail, a read receipt proves that the user’s e-mail address is valid and active.



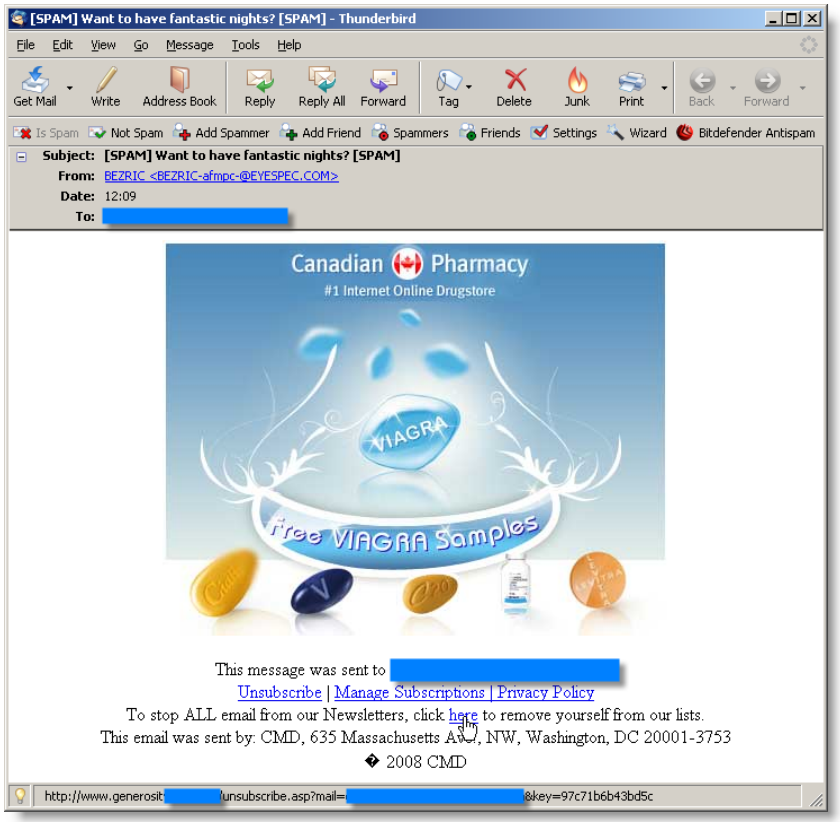
[14] See “When spam metamorphoses into literature…”, published 08 October 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/when-spam-metamorphoses-into-literature-218.html.

[15] See “The Inbox-Killer Read Receipts’ Carousel”, published 03 October 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-inbox-killer-read-receipts-carousel-214.html.

If the user discovered the trick and did not send the read receipt, there was, however, a secondary layer of confirmation that spammers added: the reference to a remotely stored image. E-mail clients traditionally block this type of content. To see it, users should allow the image to load and thus to confirm they are reading the message.



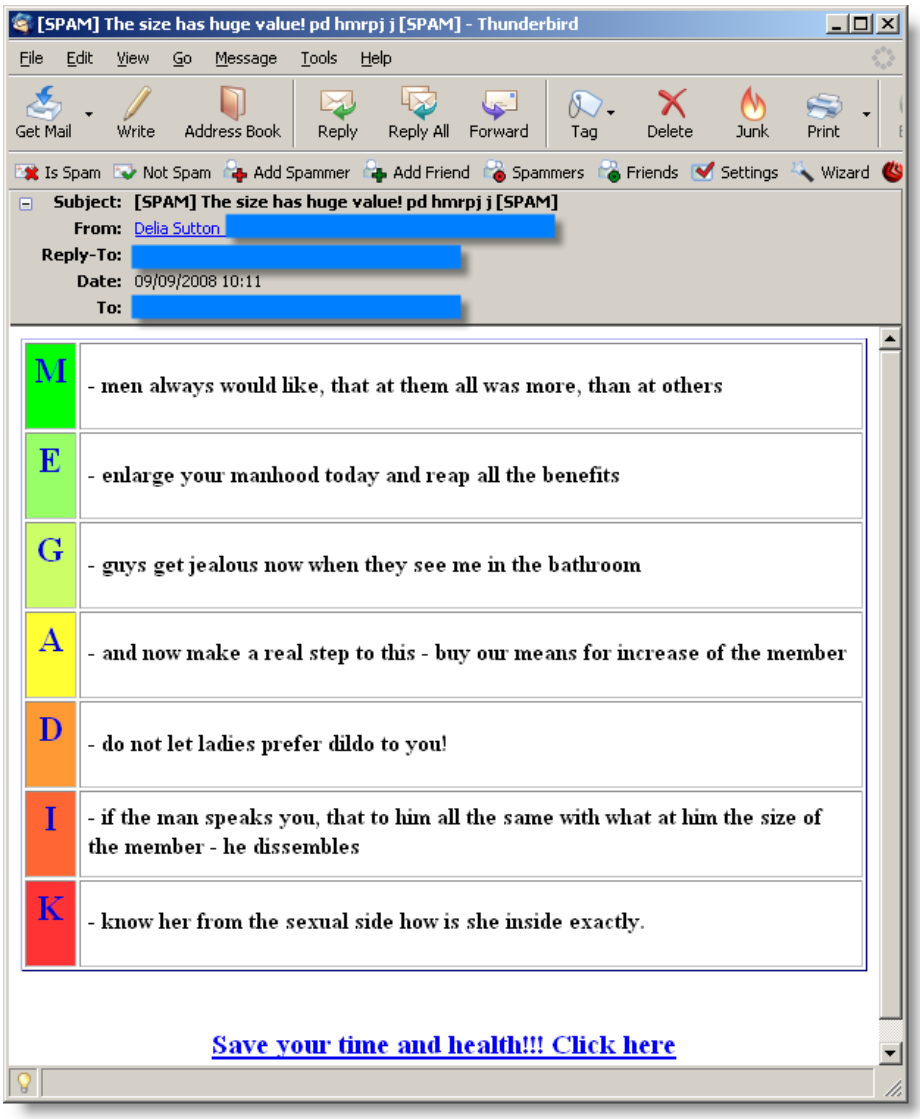
Last but not least, if the previous two confirmation schemes failed, the third layer should have been effective, especially when the users realized they had been duped and were not aware of the "classic" unsubscribe or opt-out scam. The alleged opt-out links did not unsubscribe the recipient from the mailing list, but confirmed that his or her address is fully functional and ready to get even more spam.



Spam's Content

Throughout the second half of 2008, the percentage of various types of e-mail spam content varied compared to the values of the first six months.

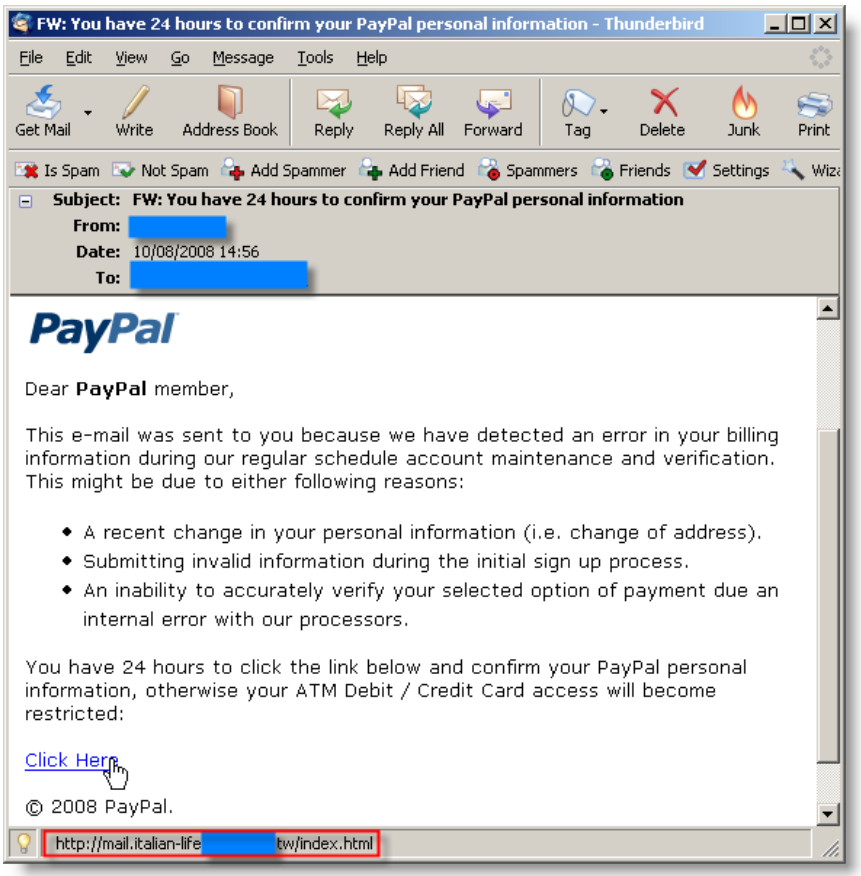
The percentage of pharmaceutical spam has dropped 2% in the last 6 months, arriving at 49%. This fluctuation was produced by the increasing number in Trojan spam.



In the last six months of 2008, the number of spam containing infected attachments or linking to a page where the user was asked to download a malicious program, has augmented 400%, getting at 10% (from 2.5% in H1 2008). This variation occurred on the basis of the extending botnets. The attackers made use of important worldwide events as the Olympic Games or the elections in US in order to reach their target.

For examples of e-mail spam leading to infected Web pages, see Attacks, Offensives & Malicious Strategies.

The phishing attacks not only keep their ground in the top, but they have also increased their numbers by 3%, probably following the same ascending trend in 2009.



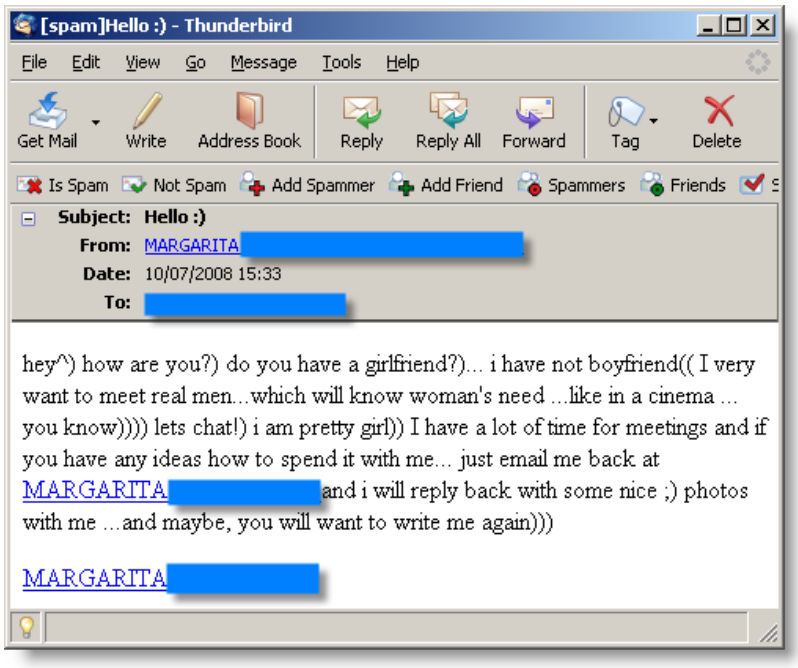
The spam selling replica watches dropped in favor of the remaining types of spam, thus losing 2 percent.

Although for most businesses the global economical crisis brought a period of recession, for the spam industry the present situation proved to attract increasing profits. The spammers are already using the depression to their advantage by increasing the number of loan messages.

The number of job employment spam runs has become more frequent, reaching in the second semester 5 percent of total volume (compared to 3% in the first half of 2008).

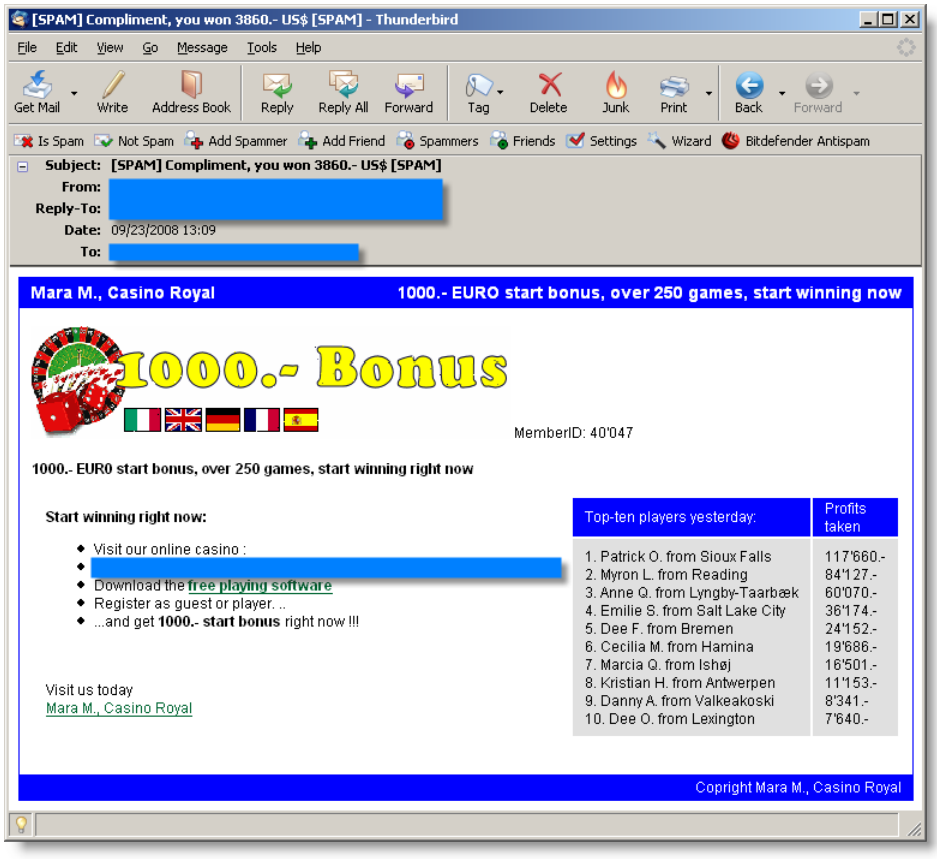
As in the first six months, the quantity of pirated software maintains its numbers, placing among the top 10 most popular contents, with 3.60 percent.

Dating scam e-mails have increased by 0.5% from the first half of 2008, reaching at the end of December 3 percent. Along the way, new techniques were employed such as getting in contact through social networks.

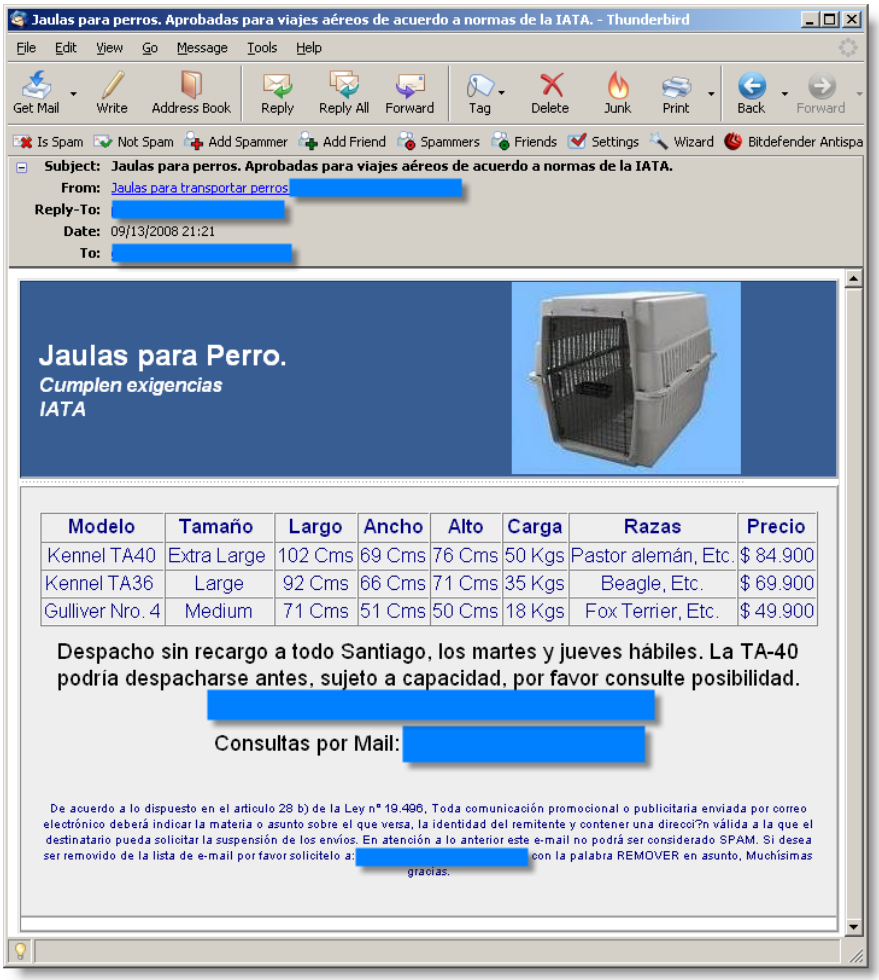


The figures for spam advertising pornography have decreased in the last six months by three percent, reaching 2.90%. It is interesting that some of the Trojan waves appealed to fake pornographic content in order to motivate the user to access the infected Web sites and compromise systems' security.

The frequency of gambling spam has increased this semester and stopped at 2.50 percent, surpassing diploma spam, which was the lowest entry in the previous chart.

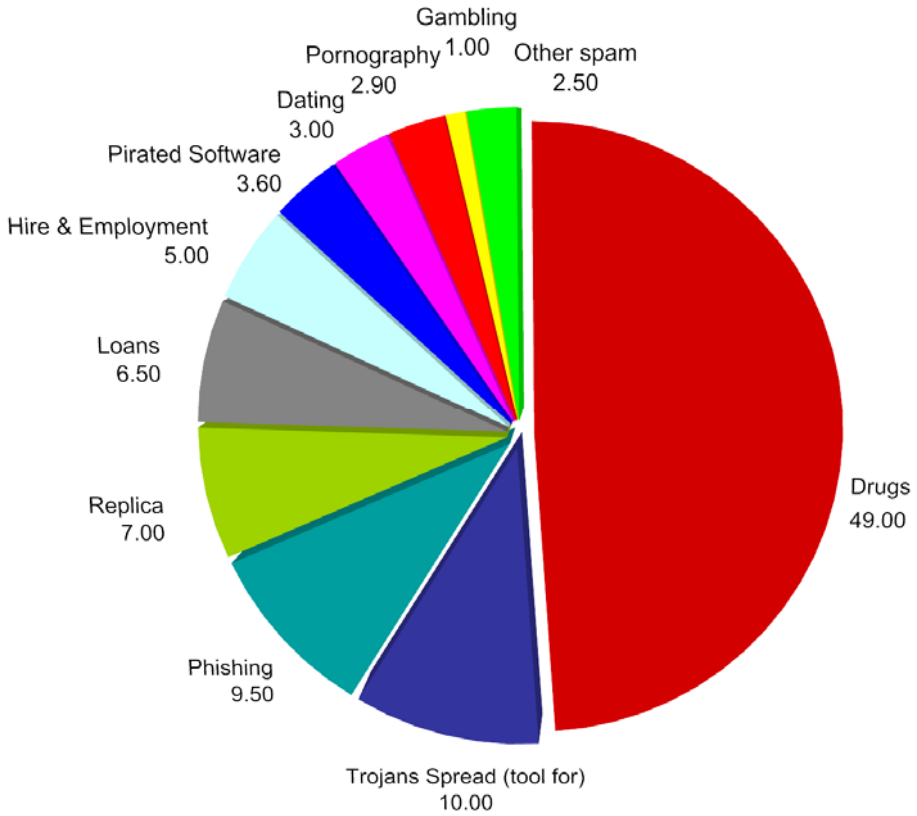


Other types of spam advertising various products or services, such as diploma spam, stock scam, lottery scams and Nigerian letters accounted together for 2.5%.



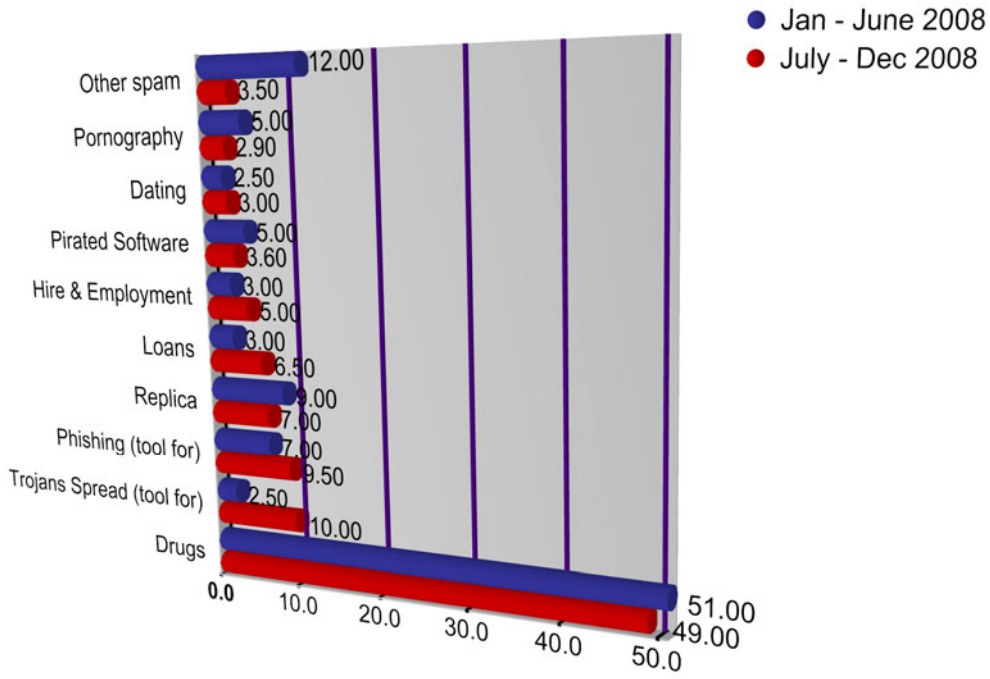
The Top 10 list for the second half of 2008's most advocated content through e-mail spam includes:

E-mail Spam's Featured Content July – December 2008		
RANK	CONTENT TYPE	PERCENTAGE
01.	Drugs	49.00
02.	Trojans' Spread (tool for)	10.00
03.	Phishing	9.50
04.	Replica	7.00
05.	Loans	6.50
06.	Hire & Employment	5.00
07.	Pirated Software	3.60
08.	Dating	3.00
09.	Pornography	2.90
10.	Gambling	1.00
11.	Other spam	2.50



Source: BitDefender Antispam Lab

”Probably the most important variation in spam’s featured content chart is the alarmingly increasing percentage of messages employed to spread or lead to malware. The high amount of potentially hazardous bulk messages disseminating Trojans multiplied four times its volume, in close connection with the accelerated growth of Web-based e-threats.” added Vlad Vâlceanu, Head of BitDefender Antispam Research Lab.



Source: BitDefender Antispam Lab

"Spam Omelette"

BitDefender's researchers analyzed a significant amount of spam messages in order to create a visual map with the most frequently used words in bulk messages. This map is intended to provide visual cues for the understanding of the new trends in spamming, while providing significant insight to researchers on the current spam waves.

The testing methodology is based on the analysis of approximately 7 million spam messages collected through BitDefender's worldwide network of honeypots.

The Top 10 of the most employed words in e-mail spam[16] counts:

1. Email
2. Please
3. Message
4. New
5. Click
6. Offer
7. License
8. Debts
9. Live
10. Marketing

[16] See the latest issues of *Spam omelette* in "The Spam Omelette", published 28 October 2008, in *MalwareCity*, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-245.html; "The Spam Omelette #2", published 04 November 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-2-255.html; "The Spam Omelette #3", published 11 November 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-3-264.html; "The Spam Omelette #4", published 19 November 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-4-275.html; "The Spam Omelette #5", published 26 November 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-5-284.html; "The Spam Omelette #6", published 11 December 2008, in MalwareCity, accessed last time 22 December 2008, http://www.malwarecity.com/blog/the-spam-omelette-6-304.html.

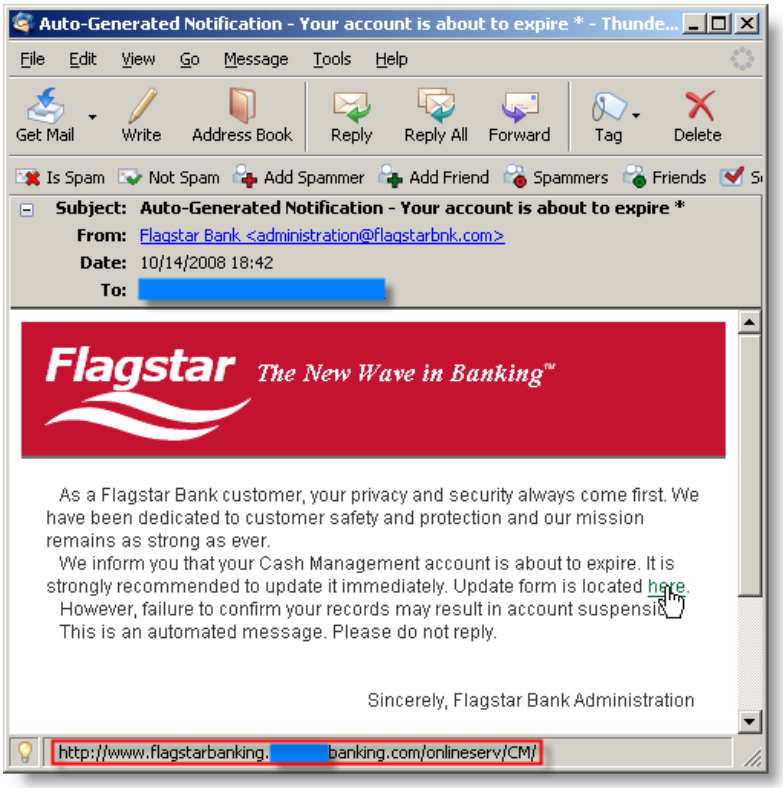
Phishing, ID Abuse & Scams

For examples of recession-related e-mail spam and phishing attempts, see Attacks, Offensives & Malicious Strategies.

Phishing trends for the second half of 2008 showed a variation and growth of the spoofed institutions and targeted clients. Primarily forged elements belong mostly to the US or EU financial organizations.

Most arguments invoked in the illegitimate messages continued to be negative, such as account blocking or expiration, increasing the fee for an amount withdrawal, as well as account details update for security reasons. Some other "hooking" methods relied on positive motivations, such as the reception of a specific amount if the user fills in the details of the on-line or attached form.

As a general tendency in 2008 Q4, almost 70% of the phishing attempts speculated the global financial context.

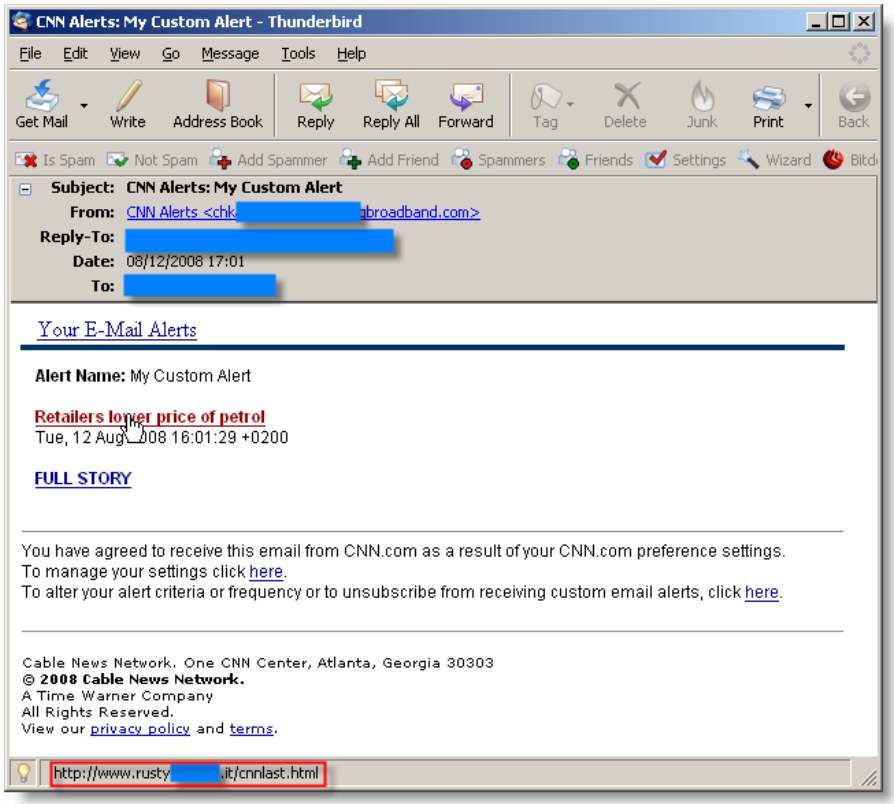


The World's Top 10 list of most counterfeit bank identities in the second half of 2008 includes:

1. Bank of America
2. Chase Bank
3. Citibank
4. HSBC
5. Halifax Bank
6. Royal Bank of Scotland
7. Regions Bank
8. Abbey
9. Wells Fargo
10. NatWest Bank

Other abusive uses of corporate identities employed in spam e-mails as part of phishing campaigns targeted the customers of several on-line and e-commerce services, such as eBay®, PayPal™, Amazon.com®, AOL®, AT&T®, Orange™, etc.

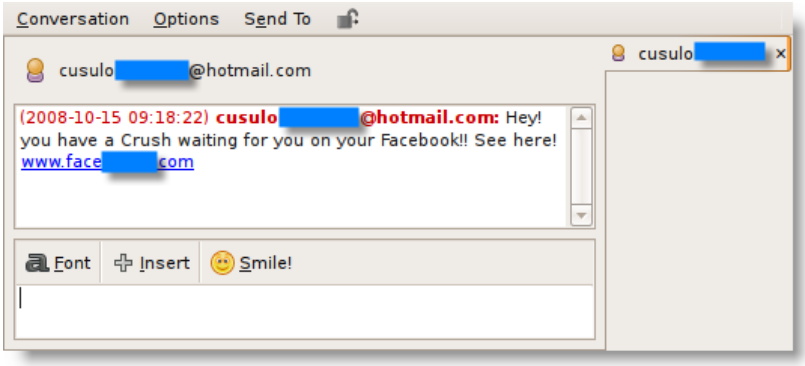
Q3 also saw the emergence of another trend. Spammers and phishers made hay of identification elements pertaining to news corporations, such as CNN, CBS or ABC, via templates mimicking newsletters and breaking news media alerts that advertised, in effect, drugs or other goods and services. In most of the cases, this type of e-mail spam attempted to download remotely stored images or to direct the users towards infected Web sites.



Another important characteristic of the second semester is the expansion of instant messaging spam, used mostly either in phishing schemes or mal-ware distribution via infected Web pages. For instance, a phishing cam-paign[17] targeting social networking aficionados lured the victims mid-October with an arousing message to the "almost perfect" phony Facebook® site.

The IM-based spam wave sent via automatically generated accounts prom-ised a “hot date” if the Facebook’s users accessed the typosquatted link, as depicted below.

[17] See "Facebook users, beware of the fake hubs!", published 17 October 2008, in *BitDefender*, accessed last time 22 December 2008, http://news.bitdefender.com/NW856-en--Facebook-users-beware-of-the-fake-hubs.html.



The fake Web site, which reproduced extremely well the genuine Facebook hub, collected the log in credentials using a PHP script.

"Phishers usually exploit Web 2.0 applications to harvest e-mail addresses, retrieve other contact details stored in accounts or post spam messages or malware disguised behind banner advertising on the legit users' profiles, channels or groups." said Vlad Vâlceanu, Head of BitDefender Antispam Research Lab.

Olympic Scams

Beijing games will probably remain in the history of e-threats as one of the most prolific events in terms of frauds. Due to its intriguing location, majestic venues and the magnificent spectacle it promised, the 29th Olympiad was heavily exploited by cybercriminals long before the opening ceremony.

IT Security Specialists and media warned the public about the imminent dangers of e-scams. With flight operators filling their seats to China almost a year ago, Beijing hotels fully booked since January and Olympic events' admission tickets sold out one month ahead of the August opening fireworks, it was no wonder that e-crooks took advantage of the sport fans' keen wish to cheer their favorite athletes.

The two most notorious cases were *beijing-tickets2008.com*, closed July, 23rd, and *BeijingTiketing.com*, shut down early August, after International Olympic Committee's and U.S. Olympic Committee's official complaints.

Taking advantage of Olympic enthusiasts unawareness and striking resemblance with the official Web site's name and appearance, these two fraud sites probably managed to purloin illicit gains of hundreds of thousands of dollars, as well as a huge amount of sensitive data, such as bank account, credit card and passport details from Americans, Australians and New Zealanders.

"Web surfers and buyers should always pay an extreme close attention to Web pages' details. Although they seem legit at the first look, many phishing and scam Web sites always reveal their lacks and incongruities at a close inspection. Whether we talk about general layout flaws, awkward phrasing, flagrant spelling and/or grammar errors, or abusive and incorrect use of logos and other design or structure elements exposed by the Web page source analysis, there are always details that should give users a clue about the fraud behind. We advise e-buyers to always check the e-commerce Web sites and perform some research before purchasing any goods or services", said Vlad Vâlceanu, Head of BitDefender Antispam Research.

The frauds victims have filled in legal complaints as have the International Olympic Committee and the U.S. Olympic Committee. (For more details and a comprehensive analysis of the scam sites, please see http://www.beijingticketscam.com/).

Global Risk Breakdown

According to Cisco Visual Networking Index, the Internet traffic will increase at a combined annual growth rate of 46 percent from 2007 to 2012, nearly doubling every two years. The Top 3 Intraregional Broadband Network Developers counts Latin America (61% growth), EU (around 50%) and APAC (44%).

The infrastructure expansion and traffic development simultaneously determined the proliferation of e-threats. In the last year only, some of the countries from the previously mentioned three regions already saw major increases of malware infections, as BitDefender analysts revealed in the following Top 10 of the most malware receptive countries.

The undisputed leader in H2 2008 is France, which holds 20.22% of the new total infections, compared to 13.22 in H1 and 17.82 percent in H2 2007.

The second position is occupied in the last six months by China, with an astonishing rise up to 16.25%, compared to only 2.59 in H1 and 2.98 in H2 2007.

US places the third in the second semester of this year, gathering 7.36% of the globally reported new infections, compared to 3.50 in H1 and 6.09 in H2 2007.

Germany ranks the fourth, with its 5.80 newly infected systems, less than in H1 when it had 6.38 and H2 2007 when it accumulated 8.06 percent.

The fifth place goes in H2 2008 to Spain, with 4.14% (3.66 in H1 2008 and 4.66 in H2 2007).

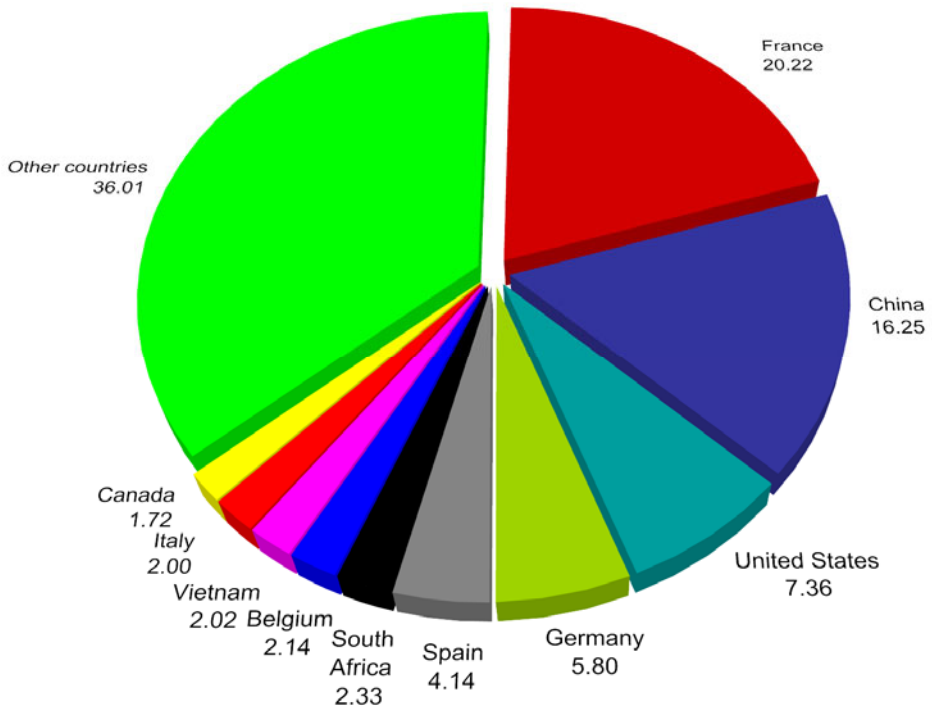
The new comer, South Africa, takes the sixth position, with 2.33%, while Belgium returns in the global chart with 2.14% after it disappeared from the World's Top 10 most malware receptive countries in H1 (in H2 2007 reached 1.93% ranking the last).

Vietnam drops on the eight position, with 2.02%, after in H1 2008 took the second place with 7.46, and in H1 2007 the fourth with 5.76%.

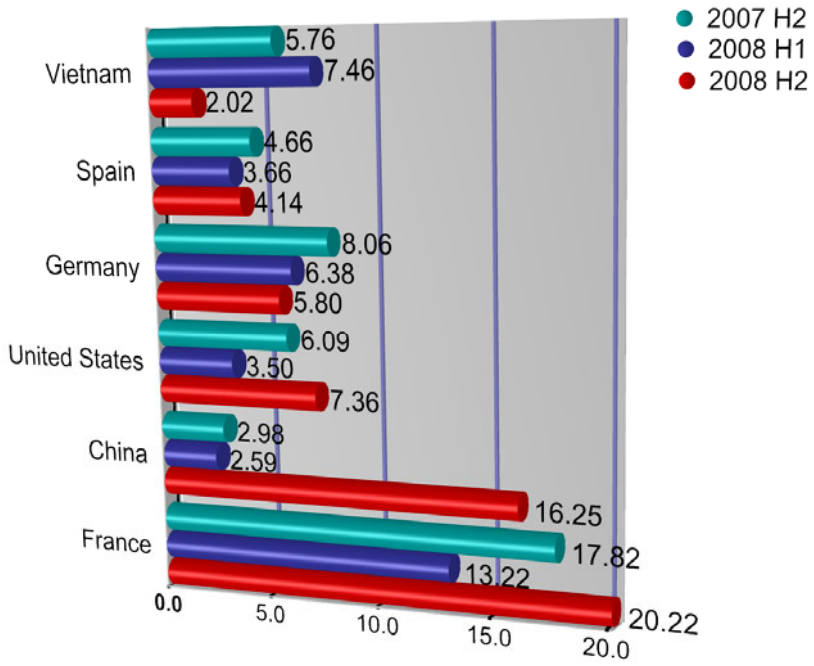
Italy challenges the chart and sets on the ninth position, with 2.00%, while Canada took the tenth position, with 1.72%, occupied by Russian Federation in the previous half.

The World's Top 10 list of most malware receptive countries in the second half of 2008 comprises:

World's Top 10 Malware Receptive Countries July – December 2008		
RANK	MALWARE	PERCENTAGE
01.	France	20.22
02.	China	16.25
03.	United States	7.36
04.	Germany	5.80
05.	Spain	4.14
06.	South Africa	2.33
07.	Belgium	2.14
08.	Vietnam	2.02
09.	Italy	2.00
10.	Canada	1.72
11.	Other countries	36.01



Source: BitDefender Antimalware Lab



Source: BitDefender Antimalware Lab

"In the case of China, the increase of infections by 6.27 times in the last six months should definitely be correlated with the major event that the Olympic Games represented. Still, even without this special occasion, the particular focus malware creators and disseminators continue to show to China should make the security industry more aware about this market's particular requirements." said Sorin Dudea, Head of BitDefender Antimalware Research.

Predicting 2009's E-Threats

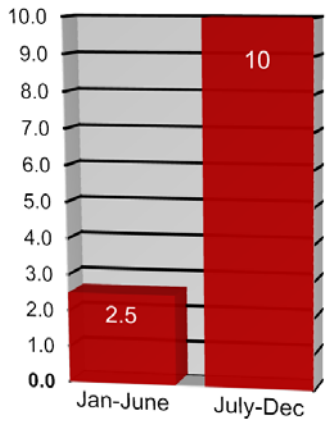
In today's rapidly developing malicious environment, the one fifth of the globe population connected to the Internet has to cope with approximate 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits, Trojans and other malware during one year.

Almost 45% percent of the e-threats in the wild are distributed exclusively via or rely to some extent on e-mail. These e-threats rely on both social engineering and the exploitation of technical flaws in mail servers and clients to achieve their goals.

In this context, securing e-mail communication should become a priority in 2009 in terms of:

- protecting assets, ideas and sensitive data
- safeguarding corporate network's integrity
- assessing and reinforcing standards, regulations and Governance, Risk Management and Compliance[18].
- defending investments and reducing TCO.

[18] Such as Sarbanes-Oxley, in the US, or Basel II and other relevant EU directives: The European Union's Financial Services Action Plan (FSAP), The 4th directive Annual Accounts of specific type of companies (78/660/EEC), The 7th directive Consolidated accounts (83/349/EEC), The 8 th directive of Company Law 1984 (84/253/EEC) and 2006 (2006/43/EC), The Consolidated Admissions and Reporting directive (CARD) (2001/34/EC), The Transparency directive (2004/109/EC), The Insider Dealing directive (1989/592/EEC) & The Market Abuse directive (2003/6/EC)



E-mail spam distributing Trojans augmented 400% in H2 2008.

Source: BitDefender Antispam Lab

For the complete Top 10 list of 2008's second half most prolific infection mechanisms, see Dissemination methods.

For the complete Top 10 list of 2008's second half most advocated content via e-mail spam, see Spam's Content.

The present sensitive economic context will probably offer a prolific realm for phishing activities, since many financial institutions will be involved in 2009 in vast merges as well as restructuring processes.

In 2009, the malware production will most likely hold an ascending trend, exploiting the same Web based capabilities of Trojans, spyware and rootkits. The end of 2008 already showed a 460% increase in Web-based infections and a 400% augmentation of e-mail spam distributing Trojans. It is certain that many of the existing e-threat families will suffer significant upgrades and mutations, in terms of stealth and automation spreading mechanisms.

2009 will also focus on exploiting applications vulnerabilities, via advanced integrated capabilities, as pointed out by one of the latest password stealing applications[19] that BitDefender's researchers identified early December. Disguised as a Mozilla® Firefox® additional component, Trojan.PWS.ChromeInject.A downloads onto the Firefox Plug-ins folder and gets executed each time the user opens the browser. ChromeInject filters data sent to over 100 online banking Web sites, which include: bankofamerica.com, chase.com, halifax-online.co.uk, wachovia.com, paypal.com and e-gold.com. The login credentials are sent to a Web address similar to [removed]eex.ru, which could indicate the origin of this e-threat.

Particular attention should be paid to the major growth of Web 2.0 sites and their rapid development. The most targeted Web 2.0 applications in 2009 will remain the social networks, since most of them derive from the same building pattern or algorithm. Although, apparently, there are several hundred billion pages, channels or profiles, they can be reduced, in effect, to a single template that is multiplied and (slightly) customized.

For instance, behind every blog from a blogging platform there is actually the same unique architecture (and its security flaws). The first effects appeared in 2005, when Worm.JS.Spacehero.A (also known as the Samy worm) paralyzed in lest then 24 hours more than a million of MySpace™ users. The last months brought into spotlight Win32.Worm.KoobFace.A, which affects both Facebook® and MySpace™ users and proved once again that social networking Web sites continues to be vulnerable. 2009 will see a rise of mutated or new worms seeking to generate traffic on specific pages containing commercials or to steal sensitive data, such as contacts lists or login credentials.

Last but not least, smart phones and other intelligent high-end devices with permanent Internet access can be expected to be targeted in 2009 by the new generations of mobile malware. OS's and browsers' vulnerabilities will continue to be exploited in the months to come.

[19] See "BitDefender Uncovers New Password Stealing Application", published 03 December 2008, in *BitDefender*, accessed last time 22 December 2008, http://news.bitdefender.com/NW900-en--BitDefender-Uncovers-New-Password-Stealing-Application.html.

BitDefender's Keep You Safe Guidelines

You can secure your system and keep the e-threats presented in this report at bay 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 spammers 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.