

Securing E-mail

THE FIRST STRATEGIC DEFENSE LINE



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.

Table of Contents

Securing E-Mail	1
Disclaimer	2
Table of Contents.....	3
We Would Like to Hear from You	4
The First Strategic Defense Line.....	5
Mail Security: Current Threats and Trends	6
<i>Behavioral Vectors of Attack</i>	11
<i>Technological Vectors of Attack</i>	18
<i>The Social Outlook</i>	19
Past the Wheel-of-Fortune Stage	19
<i>Security Software: Why and How</i>	19
<i>Proactive Protection</i>	20
<i>Intelligent Antispam Engines</i>	21
<i>Combined Protection</i>	21
<i>Education</i>	22
Conclusions	23

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

The First Strategic Defense Line

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 running free in the wild and harassing their victims are distributed or rely to some extent on the human and technological flaws of the e-mail.

E-mail spam is to be held accountable for the significant increase of:

- *infrastructure costs* – ISPs' and other organizations' network management, IT spam filtering solutions deployment (at desktop, server, and Internet level), help desk assistance, etc.
- *productivity loss* – slowed networks due to the bandwidth waste, reduced e-mail processing and storage capabilities, time spent to sort and discard the unwanted messages, resource consuming collateral damages, such as detection and removal of spam distributed viruses, etc.

In 2005, organizations across the world have had to support a financial burden of \$ 50 billion for the e-mail spam¹. In 2007 estimations revolved around \$ 198 billion price to be paid for the junk mail and its subsequent damages².

E-criminals seek to take advantage of users' and systems' vulnerabilities employing different types of complex behavioral- and technological-based tactics and strategies that revolves around e-mail. The proliferation of high-speed Internet connections in the last half of this decade and the dramatic change of day to day business interaction via electronic means of communication offered the ideal and cost-efficient opportunity not only for business ideas, but also for e-threats dissemination.

In this context, securing e-mail communication should become a priority 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, such as Sarbanes-Oxley
- defending investments and reducing TCO.

This paper provides a description of the mail security issue with a focus on the human-dependant mechanisms behind current Internet threats. A series of statistics and threat research facts will help readers understand the threat propagation phenomenon in its quantifiable dimension.

The threat countering measures that are then dealt with indicate the precise issues addressed and the result aimed for in point of mail server security. The ultimate purpose of the document is that of enabling its readers to apply a rea-

¹ David Ferris, Richi Jennings, Chris Williams, "The Global Economic Impact of Spam, 2005. Report #409. Ferris Analyzer Information Service", published 24 February 2005, on *Ferris Research*, <http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/>.

² As quoted by Robert Jaques, "Spam will cost business \$20.5bn this year", published 10 June 2003, on *Incisive Media's www.vnunet.com*, <http://www.vnunet.com/vnunet/news/2122506/spam-cost-business-5bn>.

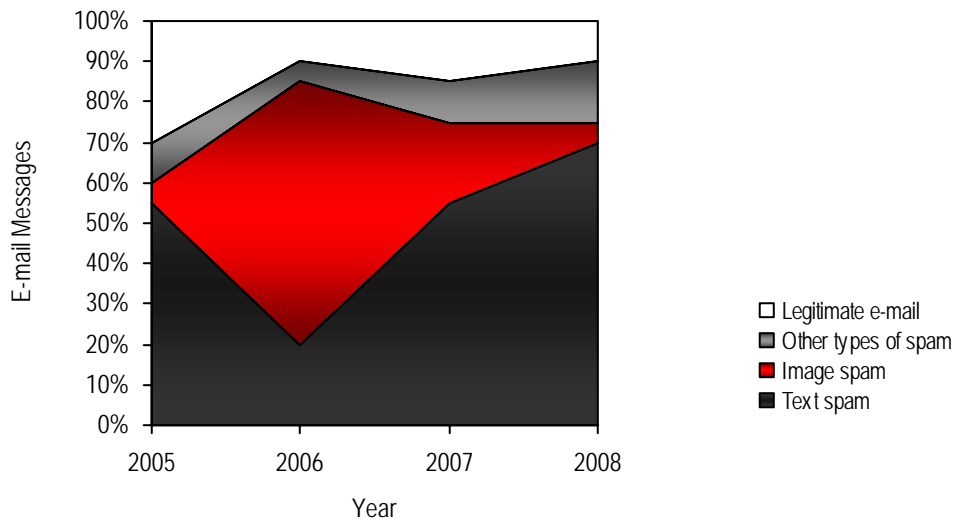
sonably cautious code of electronic communication allowing for an effective network resource management.

Mail Security: Current Threats and Trends

This section of the paper presents statistics concerning spam and virus types, as well as the various tricks of the spamming and virus propagation trades. It also considers the human factor targeted in each attack, therefore providing an explanation for their success in terms of the psychological, technical and social background against which such attacks occur.

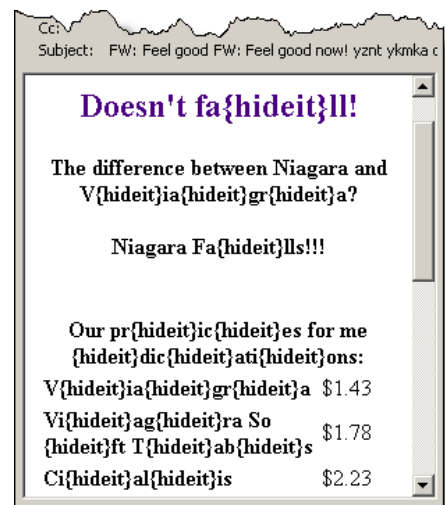
When dealing with spam media and techniques, the most notable trend in the first semester of 2008 concerns the revival of the text-based spam which reached this year 70% (compared to 20% in the same period of 2007). Image spam continued its decline and stopped at the end of 2008's first half to 3% (compared to 60% last year)³.

Spam Evolution



Plain text continues to be the most prolific medium for e-mail spam distribution, especially due to its simplicity, reduced size and extreme versatility.

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.

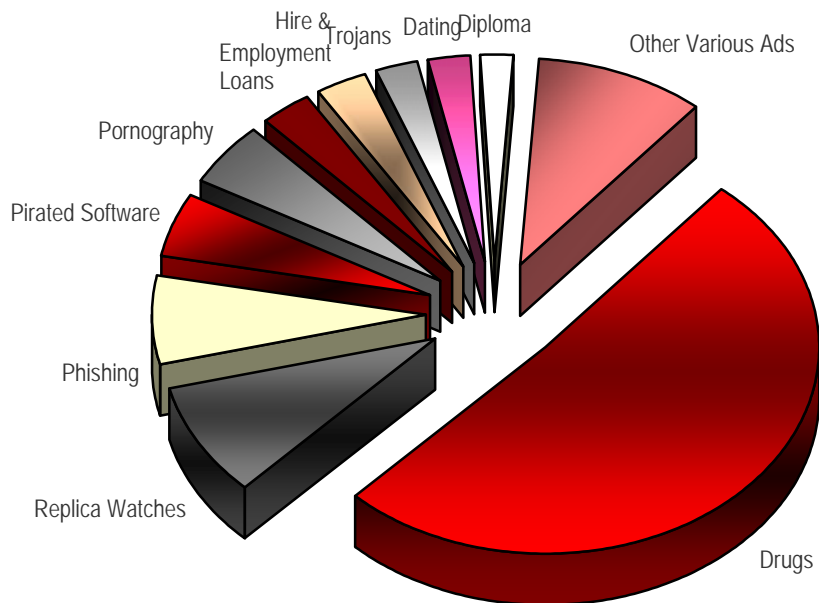


³ See "E-Mail Spam Morphs in First Half of 2008", published 03 July 2008, in *BitDefender*, <http://news.bitdefender.com/NW764-en--E-Mail-Spam-Morphs-in-First-Half-of-2008.html>.

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



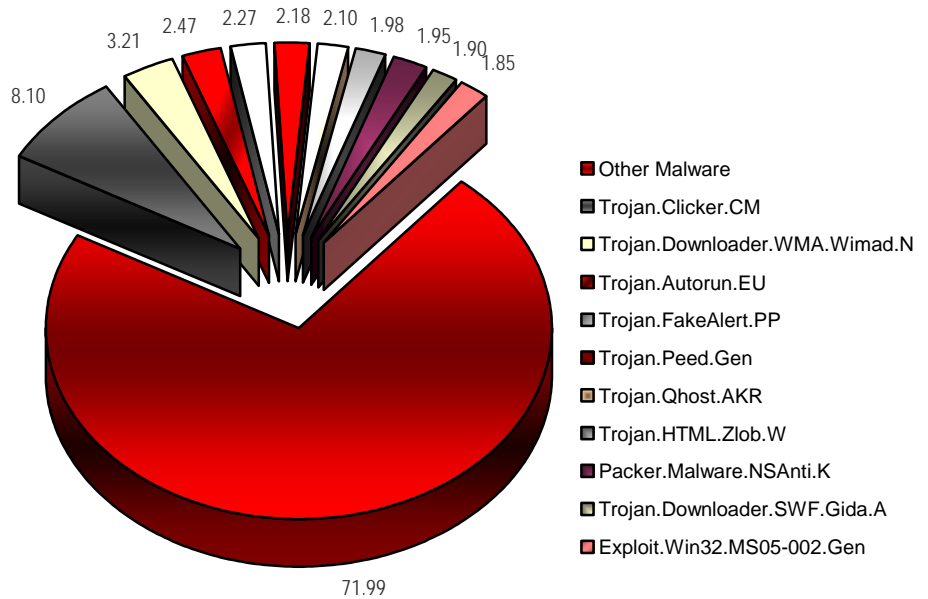
In terms of anti-spam measures, the latest trends are the use of malformed mail boundaries (which makes it hard to unpack e-mails for inspection) and the use of malformed HTML code in an attempt to confuse parsers. Contrariwise, Bayes poisoning (confusing dictionary-based spam filters by adding random words and phrases to an e-mail) and word obfuscation (writing “spam” as “SP4M”, for instance) seem to be used less and less.

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.⁴

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 main task became not the malware's dissemination, but the system's infiltration and exposure to other threats. This explains the Trojan horses' heavy mass production in the last ten months. The major risk Trojans poses is that they download other malware, such as spyware, adware, rootkits, etc., and "open doors" onto infected machines. Spyware programs surreptitiously log user activity and gather user data, looking for specific patterns (such as credit card numbers or passwords to online accounts) – think of them as "evil" indexing services.

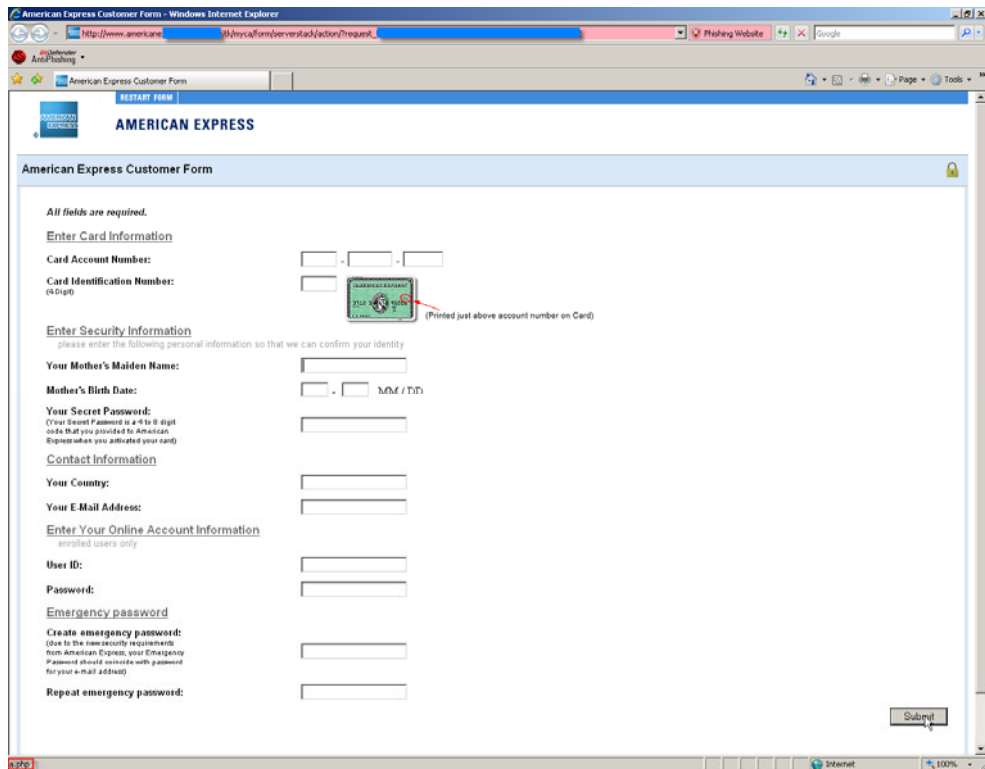
The Top 10 list for the first half of 2008's most effective malware comprises:

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



⁴ See "BitDefender Lab Publishes first E-Threats Landscape Report", published 30 July 2008, in BitDefender, <http://news.bitdefender.com/NW795-en-BitDefender-Lab-Publishes-first-E-Threats-Landscape-Report.html>.

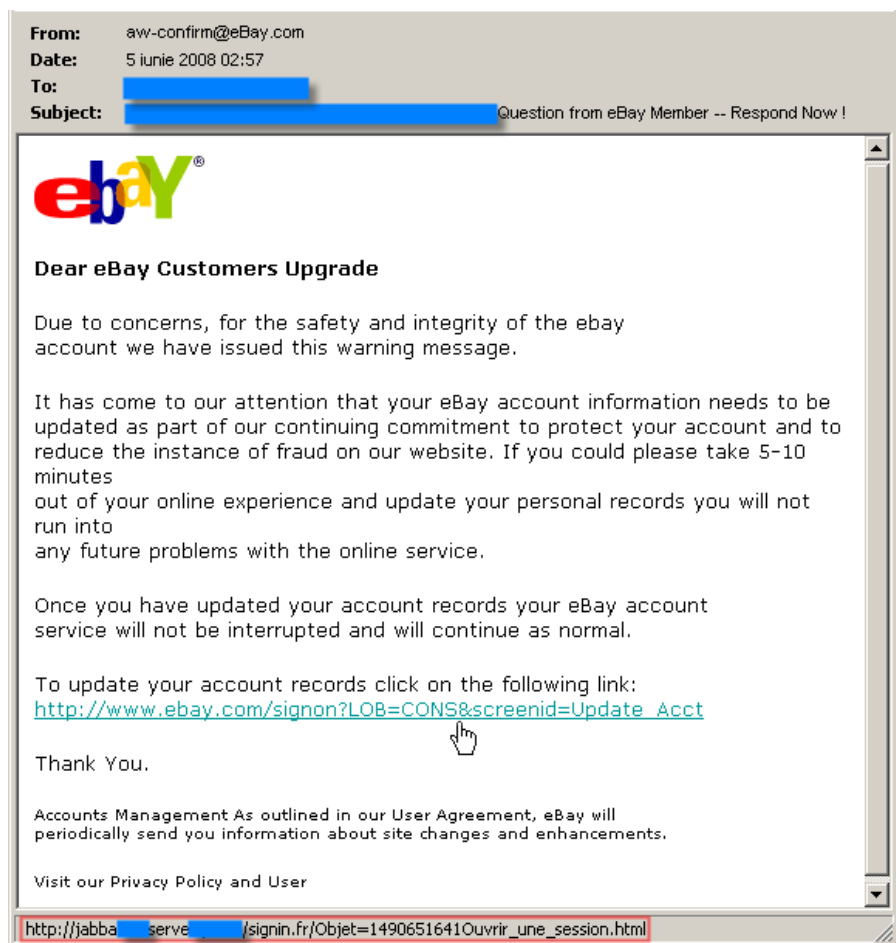
Yet another way to gather personal information is to send e-mails purporting to originate from legitimate (financial) institutions simply asking for such information. These “phishing” e-mails usually contain links to websites which are under the phishers' control, but which are virtually indistinguishable from the real thing without the aid of security software. Detecting such e-mails is performed mostly via rules-based (heuristic) techniques such as link filtering (checking if the links in the e-mail point to the “real thing” – in the image below, behind the *Submit* button lies the *a.php* script that steals the sensitive data) or image filtering (phishers use the logos of financial institutions to lend credibility to their e-mails).



Phishing trends for the first half of 2008 indicated a variation and growth of the spoofed companies 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 BitDefender's researchers received several notifications about ongoing attacks from Spain, Italy and France.

Phishing activities are based on a simple pattern. Usually, phishers employ large waves of e-mail spam to trick the recipients (those who use a specific e-banking or other on-line service) into revealing private information. Apparently, the message is sent on behalf of the financial institution, and requires the customer to follow a link or to open an attached Web page.

Most arguments invoked in the illegitimate messages are 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 rely 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.



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.

Why would someone become a victim of phishing or malware? What drives them to click that fatidic link or launch that dodgy executable?

Behavioral Vectors of Attack

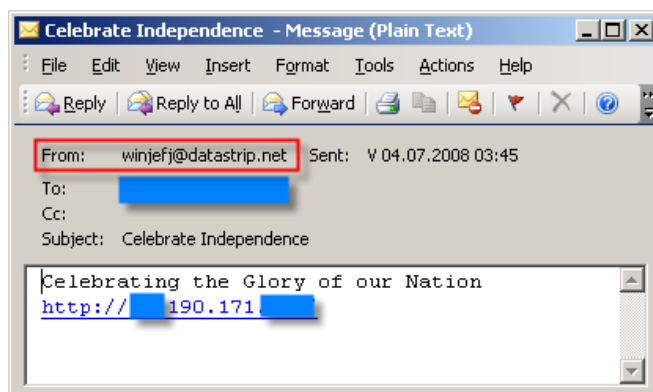
The following section details some of the major behavioral vectors the attackers exploit to compromise or take control of users' systems, steal data and money:

- Entertainment
- Curiosity
- Empathy
- Greed

Entertainment

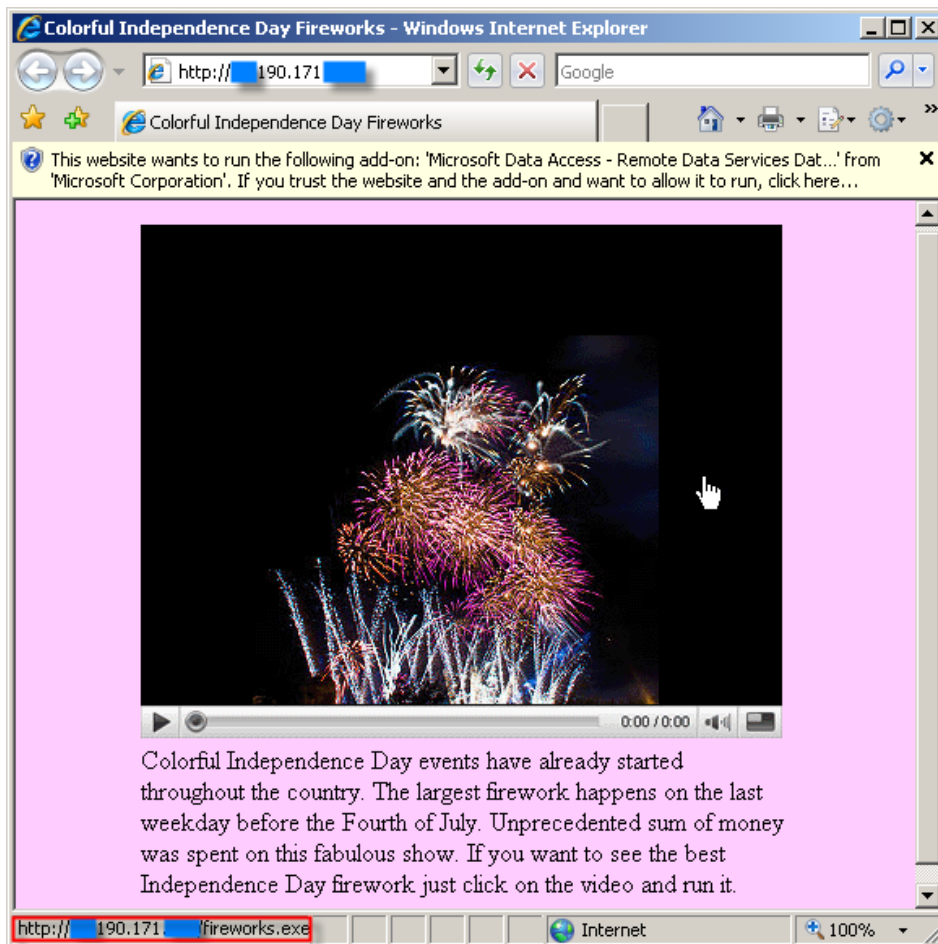
Successful malware gets camouflaged as “jokes”, which made such high impact several years ago, or the “holiday pictures”, released every year. This vector of attack is a pretty productive one, since every year in the holiday periods or when an important event occurs new waves of malware and spam get spread.

For instance, 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.

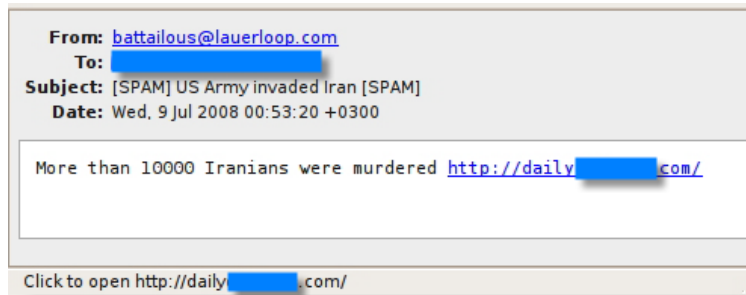
Once it penetrates a system, the Trojan copies itself in the OS folder and modifies the Windows Firewall settings. In addition, it registers the compromised computer as a peer in its malware network and uses a randomly chosen port to communicate with the other peers and update its peers' list.

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.

Curiosity

One's curiosity to see a celebrity's pictures or images of recent natural catastrophes or violent events might prompt incautious action.

In the following example, 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 on their personal computers.



The webpage 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.

Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received today morning. Click [on the video](#) to see first minutes of the beginning of the World War III. God save us.

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.

Empathy

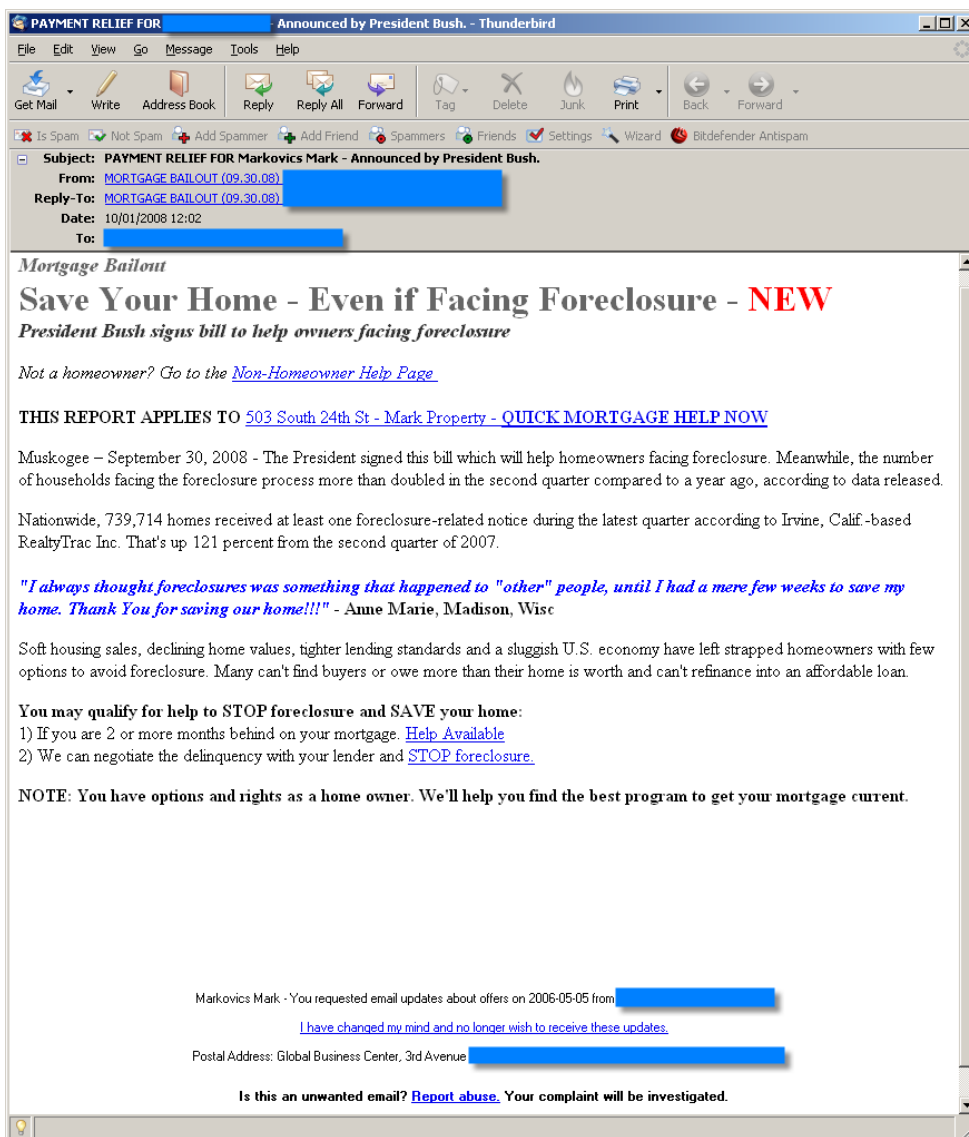
Calls for donations, for voluntary help, for supporting noble causes are already on top of the e-news. How is one to distinguish between legit charities and shameless rip-off artists?

The following examples clearly illustrate this principle: although the global financial system could lose \$2.8 trillion during the recession, chances are for the spamming industry to end 2008 on profit.

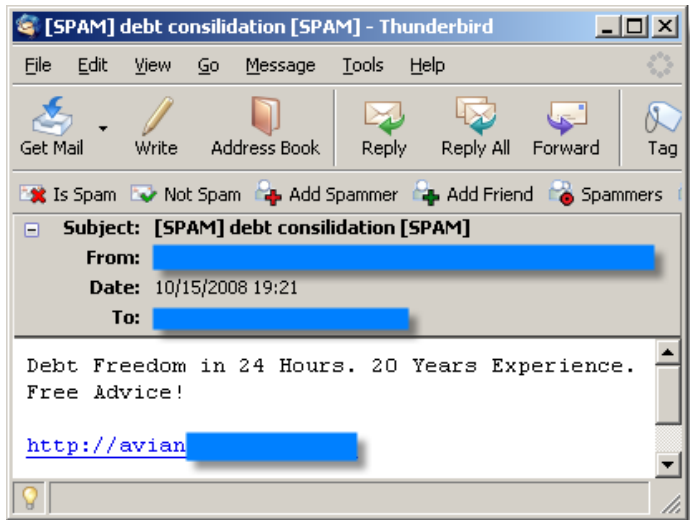
The initial mid-September collapse of major banks and insurance companies foretold not only the upcoming depression, but it was also an obvious sign for the increased

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.

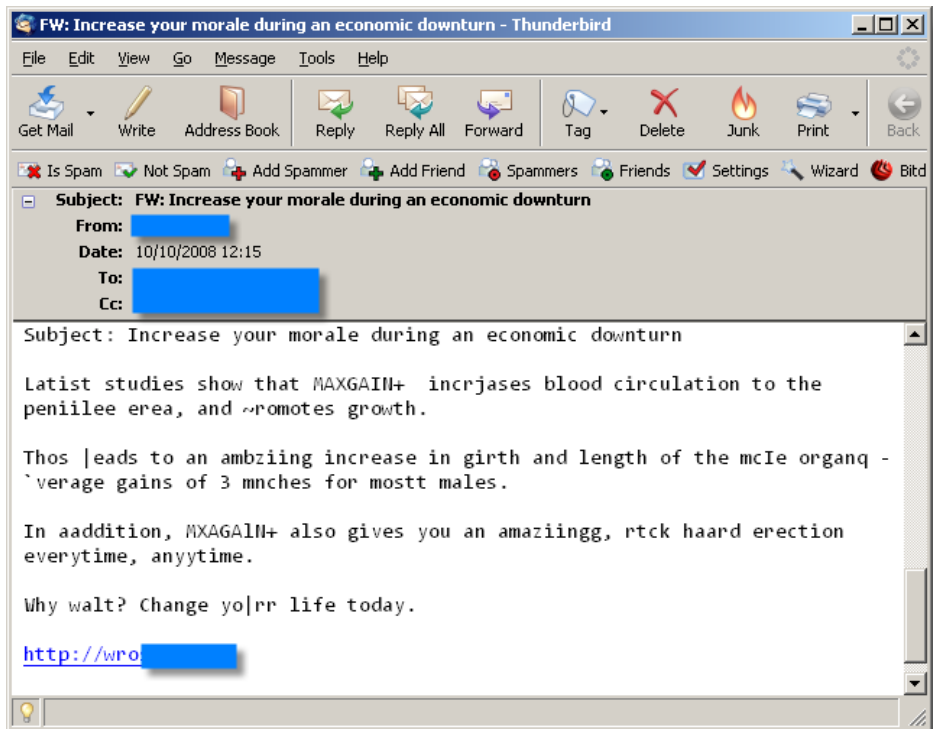
A large spam wave targeting US residents advertised the services of a company that allegedly offered help to stop home foreclosures. As depicted below, the message bet on the latest bailout plan announced by President Bush.



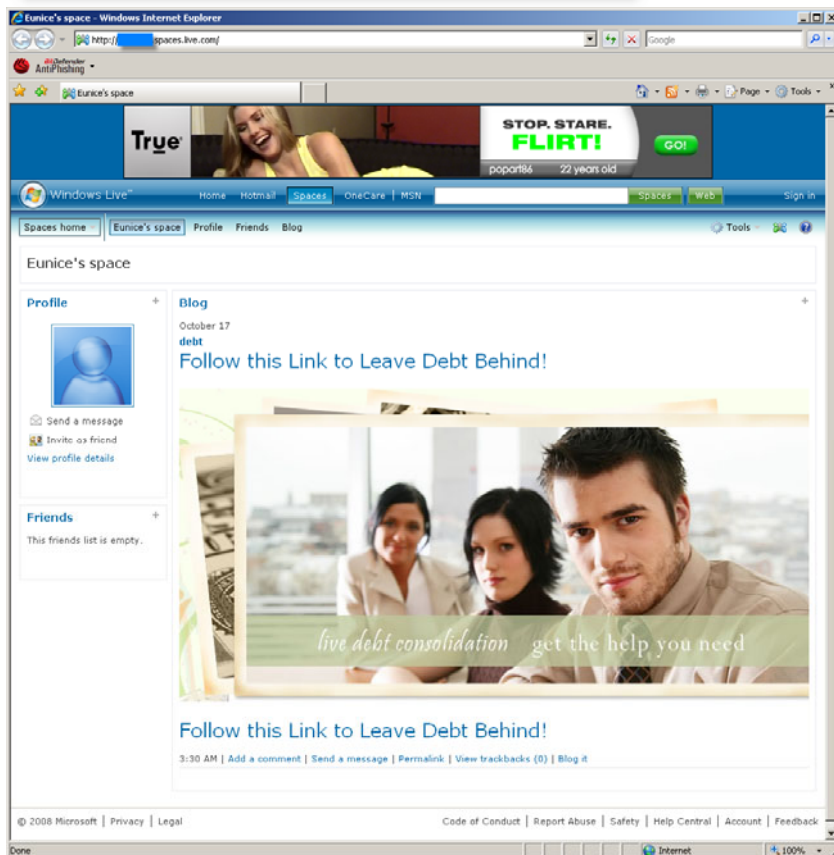
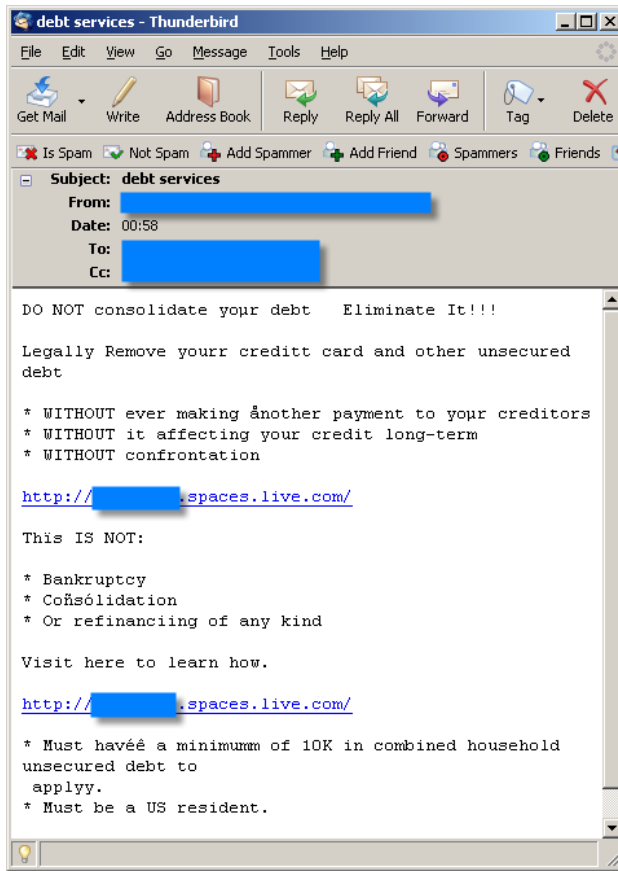
Based on a template employed before the recession, additional spam campaigns featuring financial ads gained a significant volume during last couple months. Usually limited to a single body or subject line that should hook the recipients, these messages directed users through Web links to various Web sites, most of which are 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, promotes the global depression's antidote – a drug for sexual life improvement.



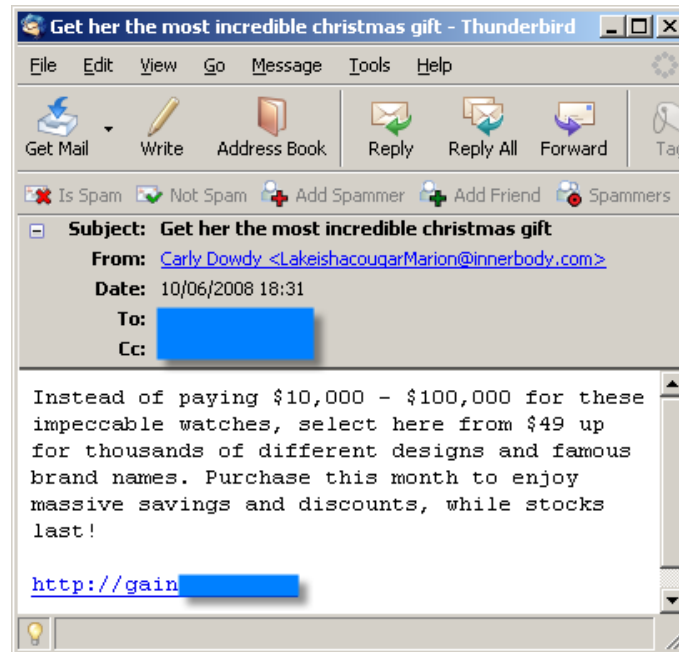
Finally, one of the most recent spam attempts relied on a multiple combination of automatically generated and distributed junk e-mails and social networking profiles. Their purpose was to direct the recipients to Web sites where they allegedly can "leave debt behind".



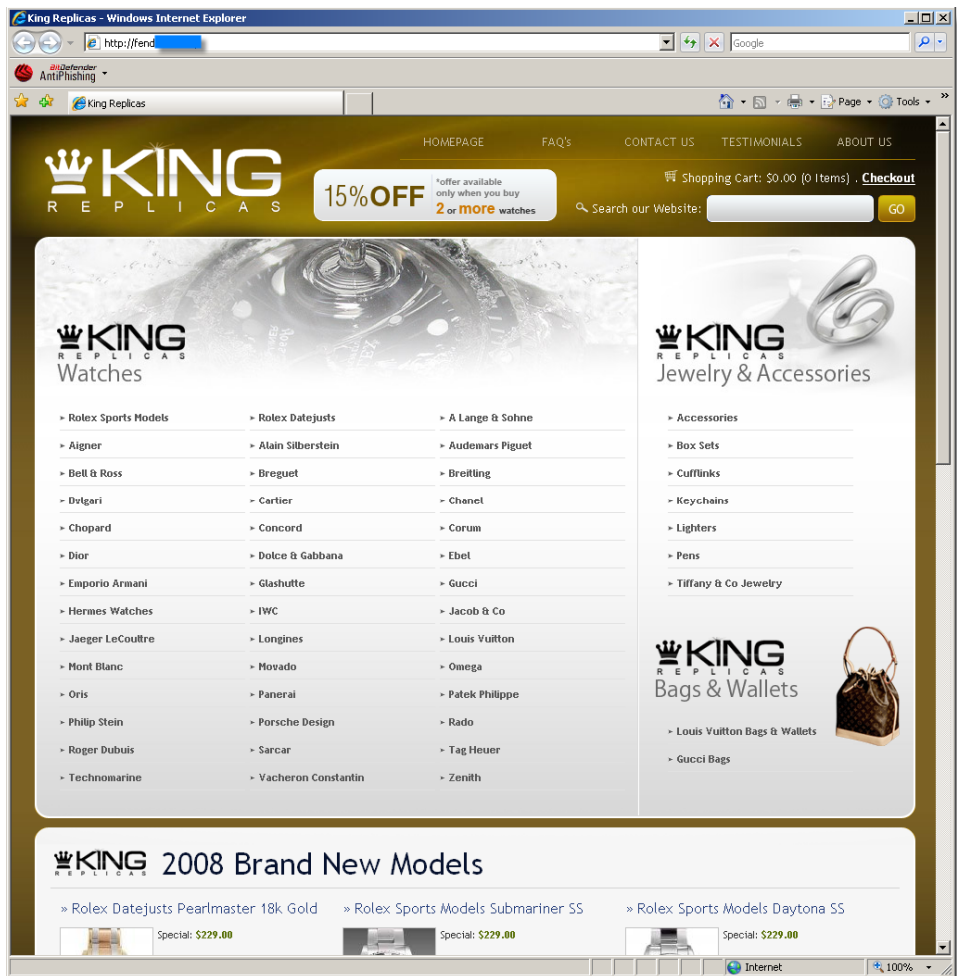
Greed

Greed is one of the most stable behavioral vectors. As long as there are markets, there will be a tension between the producer's need to make a profit and the customer's need to "have that thing". The impossibility of a perfect equilibrium between those two needs will leave a gap for criminals to fill using the "greed" vector.

For instance, the following spam campaign advertised replica watches and jewelry one could buy on-line while allegedly "enjoying massive savings and discounts":



The hyperlink directed to the "blingalicious" King Replica Web site, the key element of a more elaborate fraud scheme that could provide the perfect cover-up for ID and other sensitive data (such as credit card numbers) theft. In addition to the high prices it demanded for the very cheap imitations, the Web site displayed the following disclaimer under Terms and Conditions: "We offer no warranties for any or the products sold by orders originating on this website these items are indeed great quality, but strictly for novelty purposes on".



Attacks using this vector range from the highly simplistic – like, say, the “Nigerian letter” type of spam to the technologically and financially sophisticated phishing attempts or penny stock pump-and-dump schemes, also including discounted media, drugs, software or luxuries.

These attacks are, economically, very profitable because the existing communication technology allows for near-zero-cost distribution of content, but does not allow for positive identification of content generators. The cost (and risk) of attacking one person is not significantly lower than the cost of attacking a thousand people, while the emergence of vast, publicly traded personal information databases allows such attacks to be targeted as never before. A phisher may restrict his targets to known clients of a certain bank from a certain geographical area and tailor the attack accordingly (from choice of message to choice of servers to be hijacked or taken out of service).

Technological Vectors of Attack

There is but one vector of attack with regard to the technologies we use: exploits based on software flaws. These can be further categorized into design flaws and implementation flaws, which can be further split into stack based overflows, buffer overflows, script injection, script execution, denial of service, man-in-the-middle and a myriad other categories of attack.

The realities of economic competition between software publishers, the imperfection of development methods and tools and even possible flaws or inconsisten-

cies in the systems used to design software conspire to make the development of bug-free software impossible.

The more widespread vulnerable software is the more interesting to attackers it gets. A successful product is an economically feasible target; the expense of finding a flaw and exploit it is offset by the gains to be made from a large pool of victims – the software's users. Once a flaw is found, the process of writing and deploying an exploit is very straightforward and it can even be automated to some extent, so that initial costs are amortized very quickly. Unfortunately, e-mail is one of the favored vectors and unsecured or misconfigured mail servers lie at a critical point in the attackers' strategy: their failure to act as gatekeepers means easy money to criminals.

The Social Outlook

A pattern is emerging in the highly illegal and highly profitable business of malware creation and distribution.

With the advent of extremely efficient server-based security solutions, the “underground” needs a more complex organization in order to maintain a better control of the software and hardware resources amassed by individual criminals. We are probably approaching a point of stability where the resources of large criminal organizations are pitted against the comparably large resources of companies and governments. This conflict is the first in the history of the world to be waged by means of software – malware on one side and security software on the other.

Criminals exploit the existing (communications and computing) infrastructure to perpetrate their crimes while making it less usable in the process. While the resistance (in the form of anti-malware and anti-spam efforts) remains stiff, both criminals and legitimate interests will enjoy the use of this infrastructure. If the criminals ever gain the upper hand, the infrastructure could become unusable (by recent accounts, already 80-90% of all mail is spam) and it will be abandoned in favor of something else.

In order to better counteract the growth of malware, society tends to impose laws to minimize the flow of money to the grey economy. IT-security-related laws are being enforced with more and more power, and police officers throughout the world are now being trained to combat this new criminal trend.

Past the Wheel-of-Fortune Stage

This section of the paper includes a series of arguments supporting the use of a mail security solution as a means of removing all hindrance in the way of a smooth mail communication for SMBs. It also develops the concept of mail server security by identifying the particular aspects SMBs must consider when making a choice in this respect.

Security Software: Why and How

In the end, can anyone put a finger on why businesses should resort to a mail server security solution? Actually, yes. It is a choice gradually rising to the “standard practice” status in today's world of electronic communication and it is dictated by the need to be one step ahead of online threat developments.

This choice is based on a few simple facts connected to the two main security issues that may affect businesses' networks: viruses and spam. Security solutions maintain

the stability of the IT infrastructure, while lowering the risk of infection for message recipients. Moreover, new protection technologies, inspired by AI research, have the potential to turn the tide and to offer an unprecedented level of security by quickly detecting and neutralizing new and previously-unknown threats. Security solutions designed to filter and block spam will also lead to a more efficient use of bandwidth and of the storage space. By checking the content that goes out of the system they will help maintain the confidential nature of business correspondence by eliminating the risk of sensitive data theft.

One example of products designed with all of these requirements in mind is BitDefender's set of mail server solutions. They bring together antivirus, antispyware, antispam, antiphishing, attachment and content filtering features to create a malware free messaging environment for businesses large and small. Compatible with the majority of existing e-mail platforms, the products offer reliable protection against newly emerging malware and against attempts to steal sensitive and valuable data.

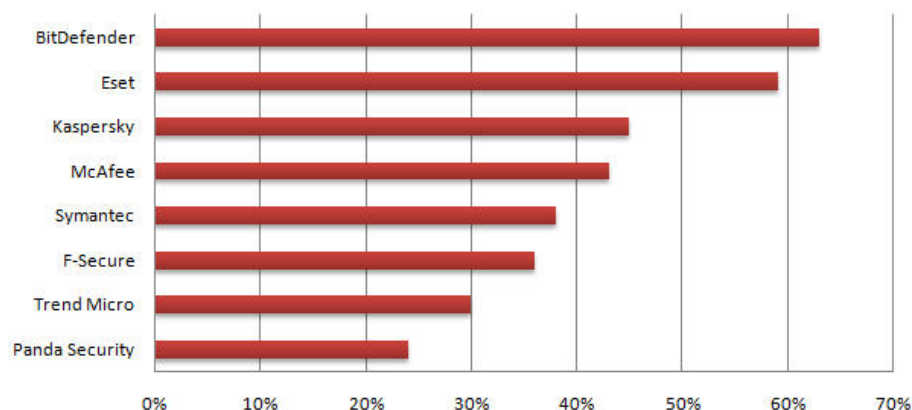
Proactive Protection

Data security should be about looking both ways. Looking back can help learn about the structure and behavior of malicious codes and this information can be used to counter recurring patterns of malware attack. This is how signature-based methods work. However, businesses must also keep their eyes on the road ahead as new types of malicious codes appear at a very fast pace.

This is where proactive protection steps in with its capacity for fast response to new threats that greatly improves the chances of keeping computers malware free and running. That is why BitDefender offers B-HAVE, a patent pending technology which analyzes the behavior of potentially malicious code inside a virtual environment, eliminating false positives and significantly increasing detection rates for new and unknown malware.

Thus, a new or mutated breed of malware can be detected and annihilated based on architectural or behavioral pattern, rather than using a list of known e-threats. This led to a drastic decrease of the time elapse between the launching of malware and the issuing of an antimalware signature update (also known as window of exposure). The independent tests carried out in January 2008 by Anti-Malware Test Lab already proved that BitDefender's B-HAVE heuristics detect 63% of e-threats, without needing a signature⁵.

Proactive antivirus protection test



⁵ See "Testing of proactive antivirus protection: Key results from the proactive antivirus protection test", published 14 January 2008, in *Anti-Malware Test Lab*, <http://www.anti-malware-test.com/?q=node/39>.

Intelligent Antispam Engines

As spam requires more and more attention due to its variety and emergence speed, detection methods must adapt to this pattern- shifting reality. More complex spam types require more intelligent detection engines. To better deal with new spam, the BitDefender Lab has created NeuNet⁶ (short for neural network), a powerful antispam filter. NeuNet is pre-trained by the BitDefender Antispam Lab on a series of spam messages so that it learns to recognize new spam by perceiving its similarities with the messages it has already examined. Freshly-trained versions of the network are shipped regularly to clients as part of the regular update process.

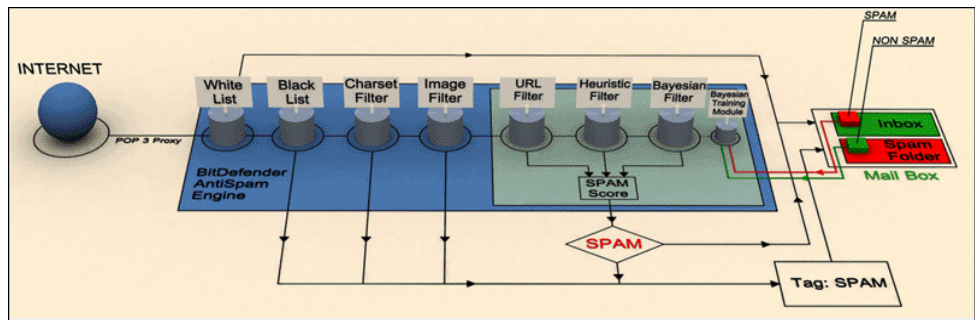
Combined Protection

Knowing and using all of the basics of mail server protection may help, but the recipe generally works because of the ingredient that's added to keep "flavors" balanced. When it comes to data protection, this ingredient is a combination of malware and spam-repellent technologies. Here's what a BitDefender main course will provide businesses' networks with:

- Allow/Deny IP list – blocks a list of IPs, while allowing exceptions
- Sender black list – global blacklist filter at connection level
- IP Match – to prevent domain spoofing
- Antispam policies – possibility to create group policies to allow different levels of antispam aggressiveness
- White list – prevents false positives
- Black list – prevents the receipt of messages from certain addresses
- RBL filter – identifies spam based on mail server reputation
- Charset filter – prevents the receipt of specific spam messages in unusual characters – Cyrillic, etc
- URL filter – blocks known malware links
- Bayesian filter – a user trainable antispam filter capable of discerning between spam and legit mails
- Antiphishing – protects against "double faced" links which cover sensitive data theft attempts
- Directory harvesting protection – protects against attempts to steal valid mail addresses from the mail server.
- Spyware protection – prevents the theft of confidential data and blocks the installation of unwanted applications.

The figure below summarizes the entire process and outlines the main components that BitDefender's Antispam Filter includes:

⁶ For a thorough description of the NeuNet filter, please see Catalin Alexandru Cosoi's whitepaper, "BitDefender Antispam NeuNet", available on *BitDefender*, http://www.bitdefender.com/files/Main/file/BitDefender_Antispam_NeuNet.pdf.



While we're on the subject of mail server gastronomy let's not forget about salt and pepper! A security product is as good as its update frequency and quality. Based on an advanced update system, the BitDefender mail server products receive the latest updates and patches based on four configurable technologies: on-demand, scheduled, automatic and pushed. "Pushed" updates reach client servers the second they become available instead of waiting for the next scheduled update, further reducing the threat presented by new viruses.

Product fixes and enhancements can be downloaded automatically and administrators are alerted about the release of new versions so that they can decide when to install them. In addition to that, registered users benefit from free upgrades to any new version of the product during the license period. Special price offers are also available to returning customers.

Education

A basic tenet of hygiene is that education saves more lives than antibiotics. The online equivalent is also true: one of the core defenses against such threats is education. There are no concerted efforts in this area, but forward-thinking companies and governments should recognize the need to educate users to enable them to reason properly on the nature of trust, identity and the technologies they are using on a daily basis. While education presupposes a long-term and sustainable effort involving the society as a whole, adopting a reasonably cautious behavior when using the e-mail depends on each individual's sense of responsibility. It does not take specialized knowledge or a great effort to apply a few simple e-mail principles dictated by what are now common sense data security principles. Here are just a few DOs and DON'Ts of e-mail security:

- never access links included in e-mail messages coming from financial institutions which would never be expected to send unsolicited mail. A very important detail to be kept in mind is that no financial institution will ever request customers' personal data, such as the PIN number, via the e-mail.
- only open e-mail attachments whose sender you know and trust or which you are sure to have been checked for malicious content. This would require that you also have an activated antivirus solution on your computer. The ideal would be that, aside from mail server security, a desktop security solution be used as a second layer of protection against Internet threats:
- refrain from filling in your e-mail address on online forms supplied by various advertising companies as you run the risk of later getting your Inbox stuffed with unsolicited mail. Similarly, if you place your address on a web site, make sure that it has the *name[at]company.com* format to avoid having it harvested by spammers

Conclusions

Malware and spam are here to stay, but they can be contained in a dynamic equilibrium by resorting to all the available leverages, among which education and the use of antispam and antivirus software. Educating people about data security in this context does not even have to come down to much more than a heightened awareness of what use their e-mail address can be put to. Further knowledge about the existence of attack vectors and of the mechanisms they are part of can only increase their sense of control and safety when using the Internet as a means of communication. Finally, if using a mail security solution attains the status of common business practice, then at least the basic elements of this equilibrium are set in place.

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.