

E-mail Spam – 30 Years After

A SHORT (HISTORIC) OVERVIEW



E-mail Spam – 30 Years After

Răzvan Livintz
Communication Specialist

E-mail spam represents an unsolicited message, usually (but not always) of a commercial nature, indiscriminately sent to you and to a large number of other recipients by an unknown sender.

If you are reading these lines, you are probably one of the 1,407,724,920 people from this planet, according to a statistic published couple months ago¹, who own a computer and get online quite often. Chances are that you received this article or a link directing you here within an e-mail. And, most likely, this should also be true for the other several hundreds of thousands of readers, laying their eyes on the same paragraph by now. You probably noticed some of them, by their names and e-mail addresses appearing next to yours in the header of the message I just mentioned. And, almost certainly, at least one or two guys from the *To* field are total strangers for you, if not all of them (not to mention the name appearing in the *From* field). There is also a very good chance for you not to be interested at all in receiving and reading this article, in which case I must humbly apologize in advance for wasting your time and patience, and respectfully assure you that this was not in any way my intention.

Technically speaking, an e-mail message bearing the features I outlined in the previous paragraph is called *spam* or *bulk e-mail* or just *junk e-mail*. An utterly unpleasant (post-) modern times invention that you, and me, and one fifth of the (Internet connected) world “enjoy” each morning in our daily routine, when we open our e-mail inbox.

Why do we call it spam?

Monty Python's sketch revolves around a lot of...
spam:

Waitress: Well, there's egg and bacon; egg sausage and bacon; egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam...

If you are willing to make an experiment and “google™” the word *spam*, the first result the search engine displays is the website of SPAM® luncheon meat from Hormel® Foods Corporation. Apparently, the unsolicited e-mail avalanches have nothing to do with the canned pork meat.

However, the alleged link between the two is to be found in a popular culture reference of the 70s, to be more specific, in a three and a half minutes sketch of the Monty Python's British television show. Obviously, the sketch name is *Spam*² and it depicts the troubles of a couple who's trying to order breakfast from a menu overwhelmed with all sort of dishes including spam.

A quarter century later, the discussion system developed in the early 80s at University of North Carolina at Chapel Hill and Duke University, USENET, the ancestor of our World Wide Web, got flooded by two immigration lawyers from Phoenix, Laurence Canter and Martha Siegel³, his wife. They posted the same message advertising their services in an upcoming green card lottery on thousands of newsgroups, pretty much the same way the characters from Monty Python's sketch incessantly repeated the word *spam*.

¹ As asserted by the *Internet World Stats*, last update 28 May 2008, Miniwatts Marketing Group, accessed last time 30 May 2008, <<http://www.internetworldstats.com/stats.htm>>.

² As you probably expected, the sketch is available on YouTube, Monty Python, *Spam*, added by zumpzump 14 February 2007, *YouTube*, accessed last time 06 June 2008, <<http://www.youtube.com/watch?v=anwy2MPT5RE>>. Do not skip the scrolling end credits!

³ For detailed media coverage of their “enterprise”, see Canter's own website, especially Laurence Canter, “Profile of Laurence A. Canter”, last update 31 May 2005, *Web Site of Laurence A. Canter*, accessed last time 06 June 2008, <<http://www.l-ware.com/press.htm>>.

Although this is not the first time when an event like this occurred, it is however the first time⁴ when someone thought to associate the word *spam* to this kind of action and its consequences.

When did spam appear?

I am quite sure you noticed in the introduction the prefix *post-* placed between parentheses. This is because the first spam attempts date most likely quite long before the age of Internet, no matter how strange would this look like.

If we agree that spam is always unsolicited and targets quite a lot of recipients, I think we can probably qualify as spam the first leaflets ever printed and dropped in numerous “classic” postal mail boxes (an “old” nasty habit we still experience today, but under the name of “printed advertising materials”).

Although postal systems (and, subsequently, mail boxes) appeared around the second half of the 3rd millennium B.C. in Egypt, and Gutenberg’s printing machine emerged four thousands years later, in the second half of 15th century, we might trace back different forms of spam in the early mankind days: from the Egyptian advertising papyruses or the Ancient Greece and Rome graffiti and incised pottery, to the printed selling announces, ballads and political pamphlets of the 17th and 18th fliers. With the establishment of the national and regional post services in the early and mid 19th century, commercial handbills type of spam entered a new age, being increasingly exploited later on, during World Wars, but not limited to, as a form of airborne propaganda through the so-called leaflet bombs.

The egression of new communication media also carried along the spam convolutions, whether we talk about the telegraph, fax, phone or mobile phone services, and last but not least e-mail.

Even if the e-mail spam seems to be “the youngest” type of spam, it is quite old. 30 years old, actually! The *first e-mail spam* is the “son” of marketing manager Gary Thuerk and engineer Carl Gartley, from East Coast-based Digital Equipment Corporation. Thuerk, the first known e-mail spammer, wanted to advertise throughout the Defense Advanced Research Projects Agency Network (ARPANET) West Coast members the presentations his company held for several new computer models. His message was sent to almost 400 ARPANET users of the 2600 people who had an e-mail account in those days.

Thuerk does not believe he was the first spammer: “Actually, I think of myself as the father of e-marketing. There’s a difference. (...) E-spam is a blast of unsolicited e-mail and/or malware to an unqualified list of recipients. It is unwanted by almost all of those who receive it,” says Thuerk. As opposed to e-mail spam, e-marketing targets several people who “have a known or qualified interest in your product, service or the information you are sending”, he adds⁵.

In contrast to current days’ trend, Thuerk’s mail was quite a success, his initiative bringing to Digital Equipment Corporation several million dollars from sales based on that message.



Gary Thuerk
The Father of E-mail Spam

⁴ For other theories concerning the etymology of the word *spam*, please see the excellent article of Brad Templeton, “Origin of the term «spam» to mean net abuse”, *Brad Templeton’s Home Page*, accessed last time 30 May 2008, <<http://www.templetons.com/brad/spamterm.html>>, as well as his other essays available in the same location.

⁵ Gina Smith, “Unsung innovators: Gary Thuerk, the father of spam”, published 03 December 2007, in *Computerworld*, accessed last time 06 June 2008, <<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9046419>>.

Why do we get spam anyway?

*Top 10 of 2008's most
advocated content
through e-mail spam*

01. Drugs
02. Replica Watches
03. Phishing (tool for)
04. Pirated Software
05. Pornography
06. Loans
07. Hire & Employment
08. Trojan Viruses Spread
(tool for)
09. Dating
10. Diploma

*Source: BitDefender
Antispam Team*

From May, 3rd, 1978, when Thuerk sent his message until today, e-mail spam's main reason is pretty much the same. PROFIT!

Whether we talk about advertising special goods, announcing huge discounts on all different kind of drugs and their substitutes, promoting new social networks or last-minute hard-core porn websites, and so on, all spam creators and disseminators seek to gain some profit – either by determining you to buy the advertised goods and services, either by wasting (and sometimes neutralizing) your resources.

It is something we also do on a regular basis (probably without being aware of it) when sending a message to anybody from our address books like Thuerk did 30 years ago. Probably not all our friends are really interested about the stuff we “advertise” (not to mention chain letters, jokes and other similar “rubbish”). We do it for our profit – just to save some time (or to be fortunated in the future).

How does spam get in our inboxes?

In the early days of e-mail spam, the unsolicited messages were sent out directly, to the addresses the spammer grabbed. Eventually, the address or the IP he or she used was tracked back and blocked. This led to address and domain spoofing, as well as counterfeiting other “honest” e-mail elements to deceive the vigilance of e-mail server administrators.

Later on, the spam distribution mechanisms switched from the open relay e-mail servers (where a sender could, technically, mail any recipient) and modem pools (where spammers exploited ISP dial-up services' vulnerabilities) to the cable and ADSL modem based proxy servers.

Contemporary distribution methods are even more sophisticated, more aggressive, and, most important, automated.

The essential element for spamming is not, in fact, the spam message itself, but the *list of e-mail addresses*. Without a large number of recipients, the message content is worthless and useless. 21st century spammers no longer “dig” for e-mails in white/yellow pages or directories, like 30 years ago, but employ the so-called *bots*⁶. To be more accurate the *spambots*⁷, whose malicious job is to harvest e-mail addresses from Web pages, contact forms, guestbook pages, mailing lists, shopping and gift lists, as well as other sources which may contain this data, including (but not limited to) our business and personal address books like those we store in an e-mail client such as Microsoft® Outlook®, Mozilla® Thunderbird™, Qualcomm® Eudora®, etc. Try to imagine what a gold mine for a spammer would be the customers' e-mail list of a major online shop, with millions of active and valid addresses (not to mention other personal information, such as credit card numbers, for instance).

In addition to spambots, contemporary spammers may use some other automated scripts that can generate names' and domains' combinations which are probably to appear in an e-mail address. Think about your organization's e-mail policy, which most likely combines your first name, surname and/or their initials.

“A spammer unleashing a single spambot or harvester can gather in an hour at least **XXXX** e-mail addresses.”

Andra Miloiu

*BitDefender
Spam Analyst*

⁶ *Bot* represents an abbreviation of *robot* or *Internet robot*, designating a software application that can perform several automated and repetitive tasks, usually over the Internet.

⁷ *Spambot* is a coined term from *spam* and the abbreviated *robot*.

BUBBLE CONTENT
ABOUT CAPTCHA and
image TO BE ADDED

Last but not least, e-mail addresses can be bought. Spammers are all social individuals, and like everybody else do shop. E-mail lists can be either traded or purchased on the underground market, in exchange for other addresses' lists, credit card numbers, pirated software, or money.

Once the addresses are collected, the spam offensive can be launched. Since the dissemination medium is the e-mail message, the spammers would need an *e-mail account*. One or several. The easiest way to get one is, as we all know, to use a free web-based e-mail service, such as Yahoo!® or Hotmail®. But since they need to send out huge amounts of messages, chances are to use multiple accounts. Here again, the automated tools – bots – come in hand.

But bots can serve other spamming purposes as well. Like gaining access on other people's computers and using them as platforms for sending the e-mail messages. For instance, through a worm, Trojan horse, other virus types or any security breaches, the spammer place a bot software inside the machine of an innocent user⁸. The bot software usually contains *spreaders* that automate the task of vulnerability scanning. Once found, the unprotected computers are attacked and infected, starting a new bot distribution cycle. A collection of malicious bots whose purpose is to run different kind of computer applications controlled by the owner or the disseminator of the software robot source, on a group of compromised computers, usually connected to the Internet, is referred as a *botnet*⁹. The robot-controlled machines are known as *zombies* or *drones*, while the botnet owner is referred to as *herder*. A botnet may be small or large, depending on the complexity and sophistication of the bots the herder employed. A large botnet consists of thousands individual zombies. A small botnet counts only a several hundred drones. Multiply these figures with those of addresses we store within our address books and with a specific amount of spam messages per day and you can get an image of the quantity of e-mails¹⁰ a spammer may send without too much effort¹¹.

What does spam look like today?

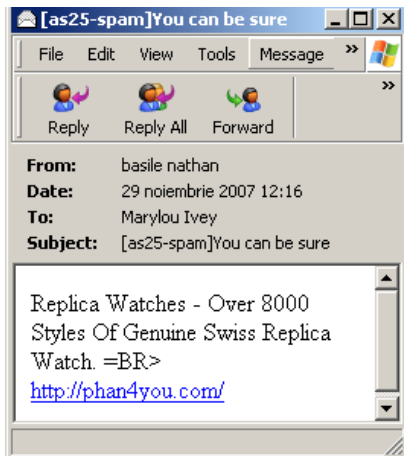
In a certain way, most of the 21st century's spam messages have the early days' characteristics. Meaning that they are mainly either "plain vanilla" text or simple HTML text messages, promoting different goods and services like those from the images below:

⁸ Although the (in)famous *Win32.Sobig.F@mm*, accountable for multi-billion dollars damages, is recognized as a conjunction between a worm and a Trojan, I think that, based on the complexity of distribution mechanism and its damaging capabilities, it might be consider as a precursor of the present-day bots. For a detailed description, please see "Virus Information for - Win32.Sobig.F@mm", in *BitDefender's Virus Encyclopedia*, accessed last time 09 June 2008, <<http://www.bitdefender.com/VIRUS-1519-en--Win32.Sobig.F@mm.html>>.

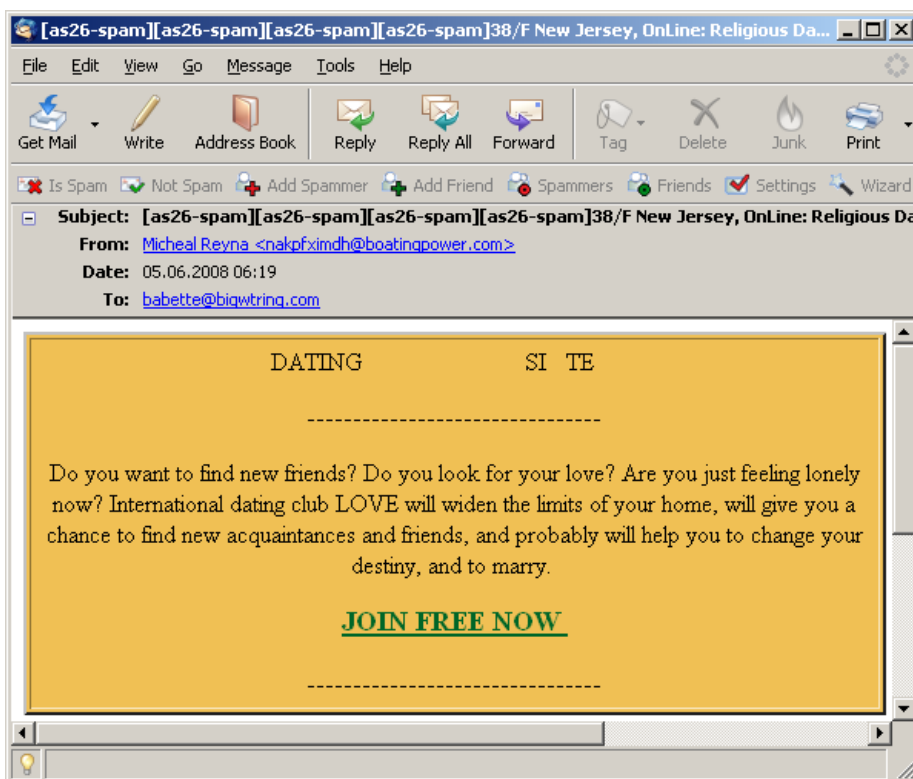
⁹ *Botnet* is another coined term derived from *robot network*.

¹⁰ For an example of spam abuse via botnet, see "BitDefender Captures Spam Used to Influence U.S. Presidential Election", published 29 October 2007, in *BitDefender*, accessed last time 09 June 2008, <<http://news.bitdefender.com/NW607-en--BitDefender-Captures-Spam-Used-to-Influence-U.S.-Presidential-Election.html>>.

¹¹ Actually, the effort belongs almost entirely to the exploited drones, since most of their resources (like memory, processing speed, Internet bandwidth, etc.) are drained out by the bots' mischievous actions.

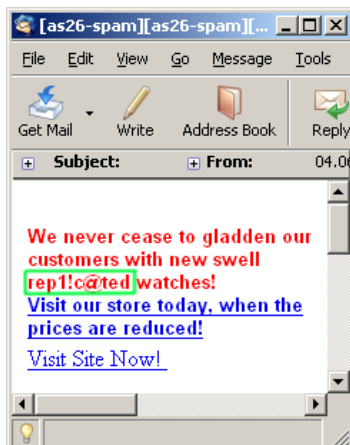


BUBBLE CONTENT TO BE ADDED



The message body varies from few words to several phrases or paragraphs and includes often a link directing to the Web site selling the products or hosting the announced services.

Because spam filters can be taught to block messages containing specific words most likely to appear in the subject line or body, one of the techniques the spammers employ is to alter, misspell, replace or add word characters. Although the spam filters cannot detect some of them, because of their unusual pattern, we, as humans, can easily recognize the encrypted words, as displayed in the following image:



“With 40 samples of different subjects, 50 samples of different titles and 30 samples of other titles, a spammer can easily obtain up to 60,000 individual combinations.”

Cătălin Coșoi

BitDefender
Antispam Researcher

To deceive the content-based spam filters¹², sometimes the same message body and its subject line are combined, partially altered, and switched, via automated scripts. This produces a virtual infinite range of unique messages, rather than a single, pattern-based message with a worldwide distribution. For instance, let’s assume a spammer has several text sources (even legitimate ones), as pools for the message’s corpus and subject line creation. He or she creates a script which picks a phrase from a pool, another phrase from another pool, and so on. In conjunction with the previously mention distribution bots and botnets, the effects can be (literally) devastating¹³.

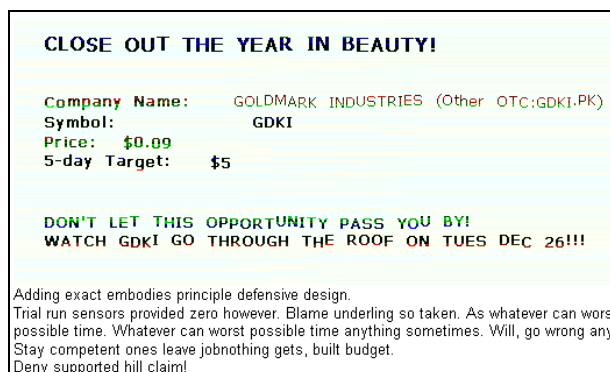
But also literary upsetting (no pun intended). On one hand, when filters detection methods became more sophisticated in recognizing common words, spammers started to use a rare an obsolete vocabulary, more difficult to be recognized and classified as pertaining to spam messages. On the other hand, and in close connection with the automated scripts previously explained, spammers started to add passages and quotes from classic authors such as Shakespeare or Dickens they extracted from Web sites offering literary content, such as the Project Gutenberg™.

But text is not the only featured spam distribution medium. Spammers turned their attention to *image spam* as well. From simple .gif or .jpeg images attached to the e-mail message, to automatically obfuscated and digitally altered images, and also animated graphic content, as illustrated in the screenshots below:



¹² Such as Keyword Filters, Heuristics Filters, Statistical Learning Filters, Pattern Recognition Neural Networks, and so on.

¹³ For details about this technique, please see the comprehensive article of my colleague, Alexandru Cătălin Coșoi, “A False Positive Safe Neural Network. The Followers of the Anatrium Waves”, in *Alexandru Catalin Cosoi Personal Web Page*, accessed last time 09 June 2008, <http://www.catalincosoi.com/documents/COSOI_ACAnatrimAT.pdf>.



Because most of the spam filters now hold an OCR¹⁴ module that might scan and read the text embedded in an image, spammers usually alter the attached graphics on purpose. The common alteration methods consist in:

**BUBBLE CONTENT TO
BE ADDED**

- adding random pixels
- scrambling characters' and text's position and size, in conjunction with different types of (decorative) fonts
- adding different colors to different characters or text parts
- placing legitimate content within the spam image, such as company logos
- using borders, backgrounds, and other "noise" elements to obstruct the OCR process, but not human-eye decryption
- placing several scrolling images, encapsulated in the attached animated .gif or .png files¹⁵.

Image spam has a greater harmful potential than classic text spam, for a series of reasons. First of all, it allows spammers to detect which e-mail addresses are valid and/or active, by letting them know which address blocks the image display. Second, when one enables the image spam display, he or she actually tells to the spammer that can be "feed" with even more spam. Third, because forces the user to deploy even more resources to open and read them (if the size of a simple text message does not get over few Kb, an image might be considerable larger, and thus may require more bandwidth, additional RAM memory, etc.).

When combining images and text in the form of *HTML messages*, the e-mail spam can be even more deceitful. Especially when spammers use logos, commercial trademarks and other formatting elements to counterfeit the appearance of a specific organization which has nothing to do with spam. Usually, this kind of spam messages is in close connection with an electronic fraud or scam, like *phishing*¹⁶. For instance, in the screenshot below, the spam message appeared to be sent by the eBay®. The e-mail asks the recipient to verify and update his or her account information, by accessing the provided link. However, if you take a closer look at the e-mail client's status bar, you probably

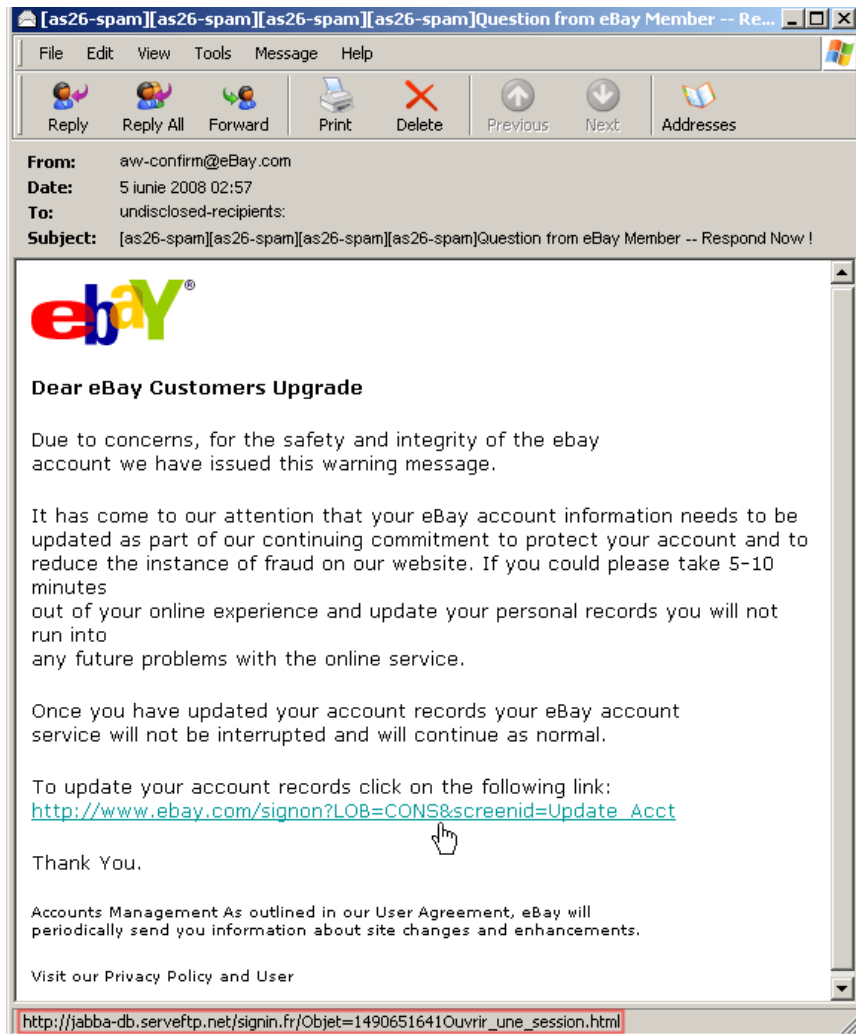
¹⁴ An acronym for Optical Character Recognition.

¹⁵ For details concerning the image obfuscation methods, please see the thorough article of Alexandru Cătălin Coșoi, "The medium or the message? Dealing with image spam", published 01 December 2006, in *Virus Bulletin*, accessed last time 09 June 2008, <<http://www.virusbtn.com/spambulletin/archive/2006/12/sb200612-image-spam>>. A downloadable PDF copy of this article is also available on *BitDefender's Technology White Papers* page, accessed last time 09 June 2008, <http://www.bitdefender.com/files/Main/file/BitDefender_DealingWithImageSpam_VBDec06.pdf>.

¹⁶ *Phishing* should be understood as a type of illegal activity attempting to obtain personal and confidential information, such as usernames, passwords, social security and credit card numbers etc., by means of deception like false e-mails claiming to pertain to a legitimate enterprise.

notice the real website disguised behind that phony eBay URL. Chances are that this message got to thousands of recipients all over the world. Maybe some of them are not customers of the electronic auctions Web site, and detected immediately the fraud attempt behind this spam. As for the other recipients, those who are indeed customers of eBay, without paying close attention to details such this, it is most likely that they offered on a silver plate their accounts' username and password, as well as other personal information, such a valid e-mail address, mobile phone number, home and billing address, social security and credit card number, etc.

BUBBLE CONTENT TO BE ADDED – Vlad comment about spam and phishing.



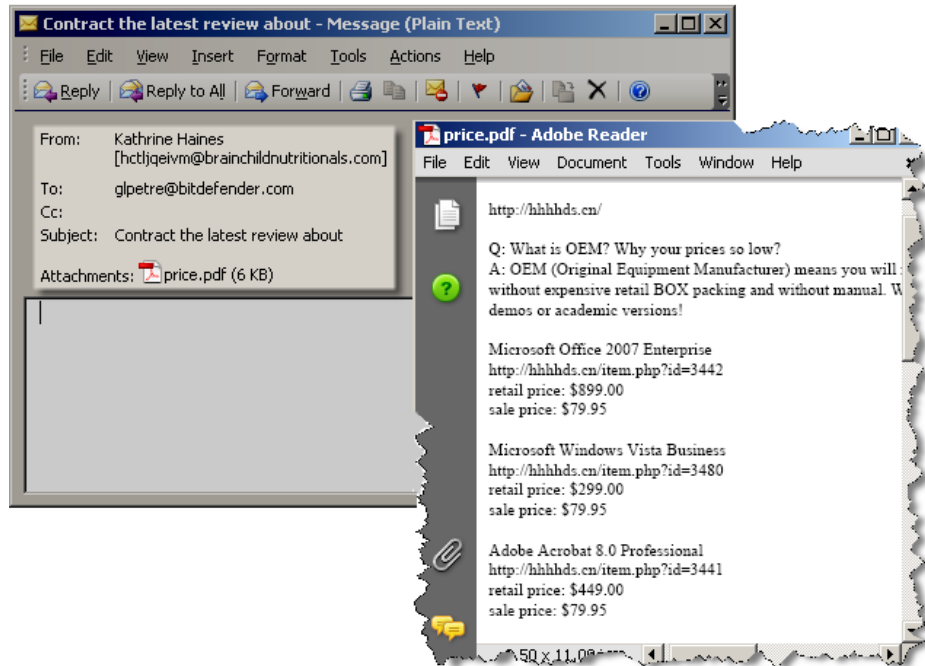
In addition to these techniques, spammers also employ e-mail attachments as spam, either as a simple medium for advertising their merchandise or as a method for *malware*¹⁷ propagation.

The *Portable Document Format* or PDFs represents one of the latest trends in e-mail attachment used as spam. That is because the PDFs are a common standard for documents, especially when it comes to business, and we would really want to check these file types, to prevent overlooking or missing important information. Plus, we would expect spam as simple text, HTML format, or, since we discuss about e-mail attachments used as spam, probably images,

¹⁷ *Malware* is another coined term, derived from abbreviated *malicious* and *software*, and refers to the written and distributed code or application that infiltrates and/or damages a computer system, without the owner's consent. *Malware* includes computer viruses, worms, Trojan horses, rootkits, spyware, adware, plus other mischievous and unsolicited software.

like previously described .gifs or .jpegs. Another important factor is the PDFs size – usually they are larger than images, which may lead to even more serious resources waste, as previously mentioned (try to figure a spam attack where your organization's server is flooded with thousands of e-mails containing attached PDFs with size ranging between 2 MB and 5 MB per attachment).

The sample my colleagues from the Antispam Team provided as illustration for this special e-mail attachment spam has almost all the characteristics to be treated as an important or regular message.



The subject line points to the review of a document (something that we all probably deal with in our daily routine), the attached PDF seems quite OK (except the name, maybe; but, again, we all use peculiar names – I named the first draft of the document you read right now *ESP30YA* – how suggestive is this for someone else?), the body message is empty (again, this happens quite often, especially when we send a document to the e-mail client from an external application). The only oddity is the e-mail address behind the sender's name, which might offer us a clue – possibly automatically generated.

As for the PDF itself – it is actually a list of pirated software with links pointing to the download pages, something we used to receive before in simple text messages or obfuscated images.

On the other hand, the e-mail spam serving for malware distribution usually relies on the premise that an attached harmful or compromising file is opened by the message's recipients. Once triggered, a mass-mailing worm such as *Win32.Bagle@mm*, which arrives as a .zip archive in the e-mail attachment, starts to search for the e-mail address stored on the host machine, in all type of documents which might contain this type of information, including .txt, .html., and .xml files. Meanwhile, it disables almost 200 types of services from the major security products, including (but not limited to) antivirus, firewalls, monitoring tools, etc. Using its own SMTP¹⁸ engine, this malware sends itself to the addresses it harvested. The subject line and body may vary, depending on the virus variant. Bagle also sends as attachment a .gif file showing the password

¹⁸ Acronym for Simple Mail Transfer Protocol, the text-based standard for e-mail transmission between an e-mail client and e-mail server.

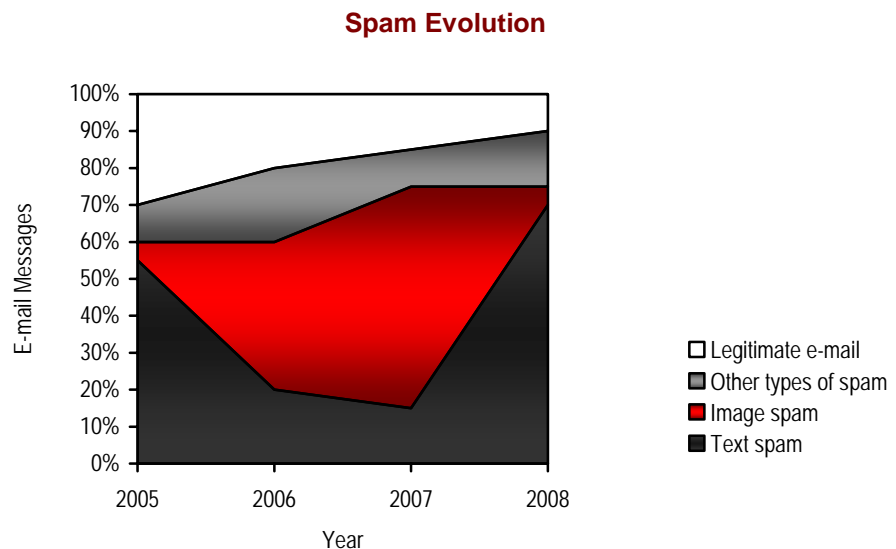
for the .zip archive the recipient should use for unpacking the files stored within the archive¹⁹.

The samples and cases presented so far are just few examples pertaining to the great variety of spam types and their distribution mechanisms. The opportunities seem, especially with the emergence of new threats with each and everyday. Once a mechanism or a technique becoming obsolete, less effective, or counterattacked, the spammers and malware creators return to their design and production workbenches.

How much spam do we get?

According to the results from the latest *Email Metric Report* for the second semester of 2007 released by Messaging Anti-Abuse Working Group two months ago²⁰, in a survey covering at least 100 million mailboxes, the number of abusive e-mails²¹ reached around 85%.

As for the types of spam, my colleagues from Antispam Team say that in 2005, text spam represented almost 55% of the total e-mail messages sent worldwide, while image spam barely reached 5%. The situation changed dramatically in 2006, when text spam decreased to almost 20%, whereas image spam augmented its share up to 40%. In 2007, text spam stopped to 15%, whilst image spam gained 60%. The beginning of 2008, find text spam returned to its 70%, image spam decreasing to only 5%, as depicted by the chart below:



¹⁹ For a complete description, please see "Virus Information for - Win32.Bagle.GU@mm", in *BitDefender's Virus Encyclopedia*, accessed last time 10 June 2008, <<http://www.bitdefender.ro/VIRUS-1000122-ro--Win32.Bagle.GU@mm.html>>.

²⁰ Messaging Anti-Abuse Working Group (MAAWG), "Email Metrics Program: The Network Operators' Perspective. Report #7 – Third and Fourth Quarters 2007", issued April 2008, on *Messaging Anti-Abuse Working Group*, accessed last time 10 June 2008, <http://www.maawg.org/about/MAAWG_2007-Q3-4_Metrics_Report.pdf>.

²¹ The authors of the report consider that the syntagma *abusive e-mail* should not be mistakenly understood as *spam*. In their opinion, "most would agree that «spam» can be defined as electronic communications that likely are not wanted or expected by the recipient", while "abusive emails are communications that seek to exploit the end user", in *op. cit.*, "Explanatory Notes", p. 3.

How much does spam cost after all?

The answer to this question is not as simple as it might seem. For the individual home user, e-mail spam cost could range between several minutes wasted to identify and delete the messages from his or her inbox to the entire credit card overdraft or savings from a disclosed bank account, as previously shown.

For companies and business in general, the figures look much worse, especially in terms 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 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, .

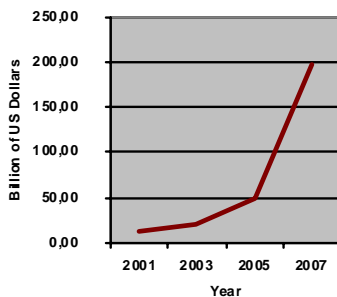
EU Internal Market Commissioner Frits Bolkestein, announced in a press release²² that a study of the European Commission conducted in 2001 revealed that the cost of e-mail spam was € 10 billion.

An investigation of Radicati Group²³ from mid-2003 estimated the global costs of spam for business to \$ 20.5 billion.

In 2005, a report²⁴ issued by Ferris Research, a San Francisco-based market and technology research consultancy, estimated that organizations across the world will have to support a financial burden of \$ 50 billion for the e-mail spam.

The same Radicati Group study²⁵ predicted a \$ 198 billion price to be paid for the spam to be sent in 2007.

Worldwide Cost of Spam



How can we fight against spam?

Apparently we cannot. This is one of the main reasons people switched back to the “classical” pen and paper method of writing to one each other. In addition to the smell, look and feel of ink, envelopes and stamps, there’s also some distinction and class that e-mail will never get.

Plus an ethic of waiting and longing... which, of course, does not apply when we talk about business, where the key words are “time and money”. In this case, you can drastically decrease the number of incoming e-mail spam and reduce the chances to contract any malware, by following the common sense recommendations below:

²² “Data protection: «Junk» e-mail costs internet users €10 billion a year worldwide – Commission study”, released 02 February 2001, on *EUROPA, the portal of the European institutions*, accessed last time 10 June 2008,

<<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en>>.

²³ As quoted by Saul Hansel, “Totalling Up the Bill for Spam”, published 28 July 2003, in *The New York Times*, accessed last time 10 June 2008,

<<http://query.nytimes.com/gst/fullpage.html?res=9502E5DB1E3FF93BA15754C0A9659C8B63&sc=&spon=&pagewanted=all>>.

²⁴ 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*, accessed last time 10 June 2008, <<http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/>>.

²⁵ As quoted by Robert Jaques, “Spam will cost business \$20.5bn this year”, published 10 June 2003, on *Incisive Media's www.vnunet.com*, accessed last time 10 June 2008, <<http://www.vnunet.com/vnunet/news/2122506/spam-cost-business-5bn>>.

- install and activate a reliable antivirus, firewall solution and spam filter.
- update your antivirus, firewall and spam filter as frequent as possible, with the latest virus definitions and suspicious applications/files signatures.
- 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 open or copy on your computer any file, even if it comes from a trusted source, before running a complete antivirus 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 e-mails, but printed notification forms 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.
- always delete the spam messages; if you accidentally open them 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 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.