Kaspersky Security Bulletin
Spam Evolution 2008

Daria Gudkova
Tatiana Kulikova
Katerina Kalimanova
Daria Bronnikova

Introduction

The year 2008 was special for a number of reasons. On the one hand, the first serious steps were taken to combat spam on an international level. The result of these efforts include a drop in the number of major platforms from which spam was sent, which in turn led to a certain downward trend in the overall percentage of spam in mail traffic.

On the other hand, the global economic crisis that began in 2008 and reached Russia in early autumn has also affected the spam business, as evidenced by changes in the structure of spam: we are now seeing less advertising of actual products and more criminalized spam.

Annual overview

- Spam represented 82.1% of all mail, which is 2.1% higher than in 2007.
- The percentage of spam in mail traffic fell during the summer holidays.
- For several days following the closure of McColo, a hosting service used to control several botnets, Russia experienced two times less spam, and the US saw 3 times less spam than usual.
- The amount of email spam targeting users of social networking sites and the amount of spam on such sites increased.
- Spam encouraging users to send costly text messages to short numbers became more common.
- During the second half of the year, the percentage of spam in the “Other goods and services” category decreased, reflecting the number of orders received by spammers in the real economy.
- The amount of adult-content spam increased nearly 10%, which resulted in increased traffic on pornographic websites.
- A new category of Russian-language spam emerged in 2008: fake luxury goods.
- In order to attract attention to the goods and services advertised in spam, the global economic crisis and the new US president became two recurrent themes.
- Spammers took advantage of some of the quirks of HTML in order to bypass spam filters.

Trends in 2008

Spam scams using text messaging

In 2008, more and more Internet users were encouraged to send text messages to short numbers leased by scammers who earned money from the high costs associated with sending text messages. This type of fraud became especially widespread this past year.

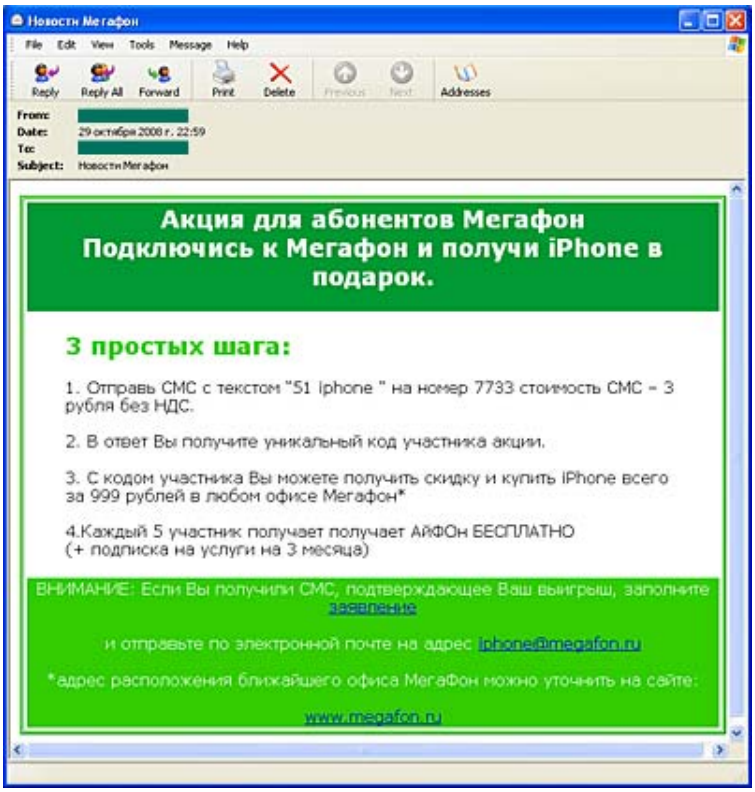
The false promises and threats used by spammers included the following:

– the promise that the recipient will win a price in a non-existent lottery

– an offer to read an email allegedly sent to the user which will not be made available until the recipient sends a text message

– a warning that the recipient's email account will be closed if a text message is not sent.

The email below is meant to look like an email from a cell phone provider:



It tells the recipient about a new special offer: sign up with MegaFon and get an iPhone at an incredible discount. All the recipient has to do is send a text message to a short number, after which he or she will receive a special promotion code, which can then be used to purchase an iPhone for just 999 rubles (about $30). It goes on to say that every fifth applicant will receive an iPhone and 3 months of cellular service for free.

The fact that Russia, unlike most other countries, does not require a license for the lease and use of short numbers, provides fertile ground for this type of fraud. All one has to do is sign a partner agreement with a cellular marketing agency that has entered into an agreement with a cellular service provider. If one and the same number is used by several companies (a so-called “shared” number), then each company will have their own codeword or prefix. Sub-leasers receive a portion of the income generated by the text messages that are sent.

Russian users are accustomed to paying for small services using text messages and often do not suspect a thing. Short numbers are legitimately used for voting, quizzes, and contests. By sending a text message, users can pay for content for their cell phones (ring tones, pictures, java-based games etc.), post messages on websites, forums, and blogs, and gain access to wap sites. Text messages are also used by a variety of services (dating services, reference services, information services, etc.).

Scammers take advantage of all of these factors. They lease short numbers with prefixes and then send out spam emails designed to look like official emails from the administrators of various resources and services. These emails use special offers to encourage recipients to send text messages to their short number, but fail to mention the cost involved (150–300 roubles, or approximately $4–9).

Cellular marketing agencies to try to control the activities of their text message billing partners by closing down fraudulent numbers. But it seems these types of scams will continue as long as the scammers are able to make money from it. In order to avoid unexpected expenses, don’t believe anything you read in a spam email. At the very least, you should always try to verify the information on the website of the company that sent the email.

Spam and social networking sites

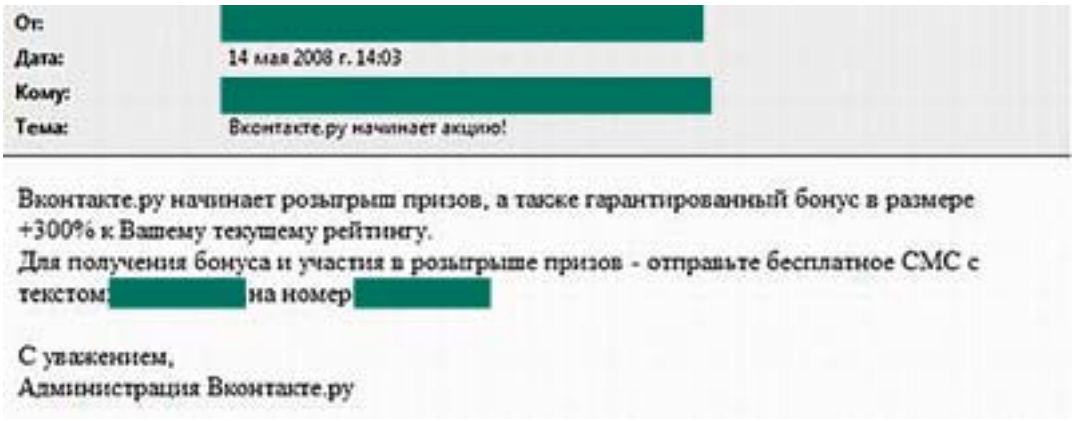
Social networking sites have become wildly popular over the last few years (and are essentially ready-made databases of user information!) and are a common target for spammers.

Fake notifications are sent by spammers (allegedly from the administrators of social networking sites) in order to get users to visit a webpage infected with malware, send a text message to a short number, or to help phishers who are looking to collect user logins and passwords.

In June, a mass mailing was made imitating messages from the well-known Russian social networking website, www.odnoklassniki.ru. The email mimicked a notice that users often saw when they visited the site. An attentive user could see the difference: the link led to a counterfeit website as opposed to the official website (odnolassniks.info, odnoklass.ru, or odnoklassniks.ru). The URL, which incidentally was registered in Singapore, was extremely similar to the original. But users who clicked on this link would inadvertently download Trojan.Win32.Agent.qxk before being automatically redirected to the original site, www.odnoklassniki.ru.

These types of messages have been received by registered users of odnoklassniki.ru and others who do not use the networking service. The ultimate target of the mailing was doubtlessly the members of the website. This attack was meticulously designed, but nevertheless was not a success: the configuration of malicious sites allowed only a limited number of users to visit at any one time, and in most cases users did not end up downloading the Trojan.

In another attack, spammers used the popularity of social networking in order to get cash from Internet users. A message was sent from the alleged administrators of another Russian social networking site, VKontakte, and the recipient was urged to take part in a lottery and send a “free” text message to a short number:


От: [redacted]
Дата: 14 мая 2008 г. 14:03
Кому: [redacted]
Тема: Вконтакте.ру начинает акцию!

Вконтакте.ру начинает розыгрыш призов, а также гарантированный бонус в размере +300% к Вашему текущему рейтингу.
Для получения бонуса и участия в розыгрыше призов - отправьте бесплатное СМС с текстом [redacted] на номер [redacted]

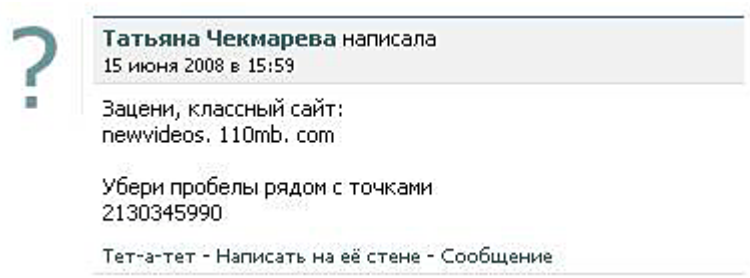
С уважением,
Администрация Вконтакте.ру

The message above tells the recipient that Vkontakte.ru has launched a special prize offer and a guaranteed +300% bonus in the user's current rating. In order to receive the bonus and participate in the lottery, the user was told to send a free text message with a specific code to a short number.

In October, spammers took another deliberate step “forward” by organizing another mass mailing allegedly from VKontakte. Users were asked to try a new service that was supposedly offered by the website's administration. Users that clicked on the link would be taken to a fake webpage where they were asked to register with VKontakte. After they entered their data, users were told that their email address was not registered, or that they entered their password incorrectly; the logins and passwords were thus made accessible to phishers.

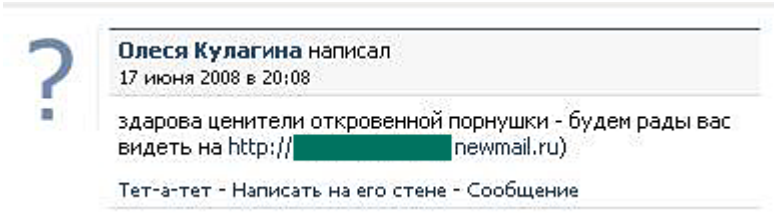
Social networking has become so popular, that malicious users have even come up with a program to automatically download logins and passwords when visiting a user’s personal page on a social networking site. This program, which was advertised in spam emails, did actually automatically fill out a registration form for site users, but it also transferred all of the user’s personal data to the websites of malicious users.

Spam is also spread directly on social networking sites. In June 2008, we saw the first cases in which VKontakte users started to find messages like those below posted on their walls.



This message says “Hey, check out this great site! Just take out the spaces after the periods.”

Or



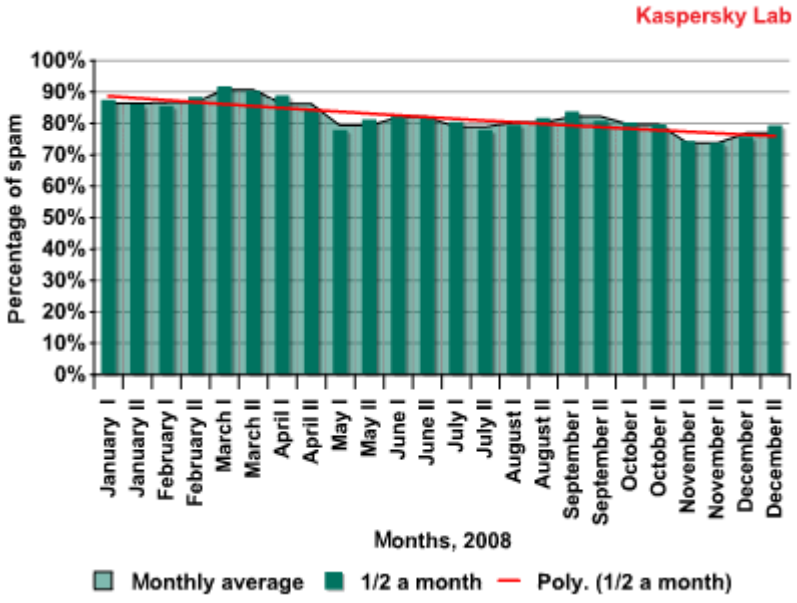
This message says “What’s up, porn lovers? Come visit us at http:// {site}”

These links led to pornographic websites.

The development of social networking sites in Russia and spammer attacks on the users of these resources has resulted in a new type of spam: social networking spam. This new spam is spread via email and directly within the social networking websites themselves. Social networking has become yet another niche for the spam industry. Spammers use social networking websites to infect user’s computers, make money through costly text messages, and steal user data (phishing).

Distribution of spam

The percentage of spam in 2008 averaged 82.1% (2.1% higher than in 2007). The lowest percentage of the year was recorded on November 13 at just 50.5%, while a high of 97.8% was recorded on March 1.



Percentage of spam on the Russian Internet in 2008

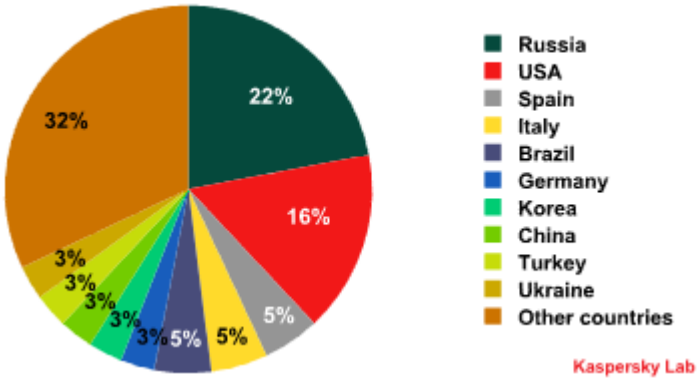
The chart above shows the percentage of spam on the Russian Internet in 2008. A downward trend in the percentage of spam in total mail traffic is clearly visible. However, it would be a mistake to say that this trend is the result of decreased spammer activity.

In the first quarter of 2008, the percentage of spam increased, and in the second quarter, it began to fall and remained at a relatively low level (80%) throughout the summer. This was the seasonally slow summer period, which is not truly indicative of a real downward trend in spam levels. In September, the amount of span in email traffic began to increase, only to experience a sharp drop in November. This decrease was the result of the closure of McColo, a hosting service that served as the control center for several major botnets (Rustock, Srizbi, Dedler, Storm, Mega-D, and Pushdo).

By the end of November, spam levels had begun to reach their previous levels, and in December the percentage of spam on the Russian Internet reached 82.5%.

The fact that the closure of one hosting provider had such a strong impact on the percentage of spam in total email traffic (several days after McColo was closed, Russia saw two times less spam, and the US experienced 3 times less spam that usual) is both unprecedented and revealing. Although spam gradually recovered its previous levels, this instance proves that spam can be — and should be — fought not only using software solutions, but also by taking action at an international level, with collaborative technological and legal efforts.

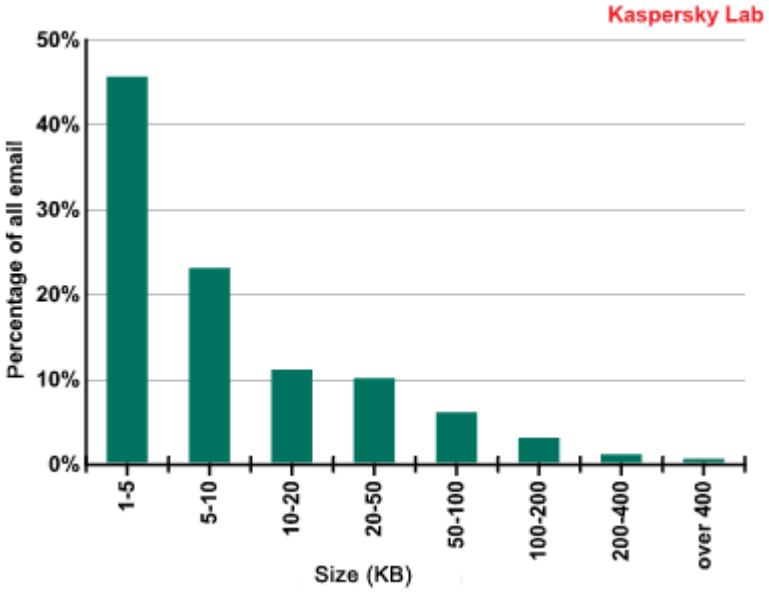
Key sources of spam



Countries that are sources of spam

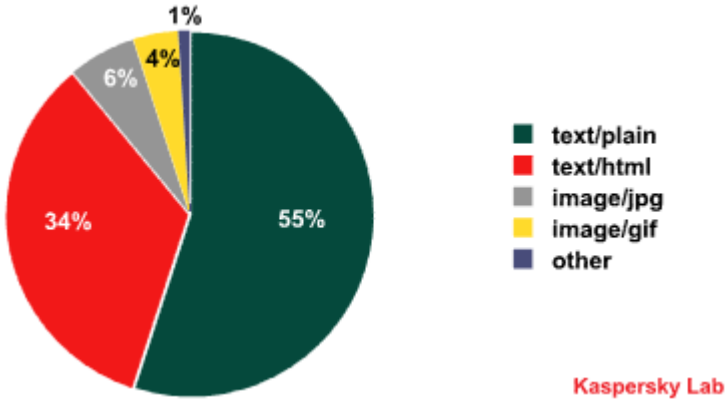
Among the countries that are sources of spam on the Russian Internet, Russia took the lead in 2008 (most spam came from the US in 2007). The US took second place and was followed by a number of other countries. The distribution by month is also varied; for example, over the year Spain was the source of 5% of the Russian Internet's spam, but in some months it was the source of as much as 10%.

Types and size of spam emails



Size of spam emails

As in years past, the size of the overwhelming majority of spam emails did not exceed 10 KB in size. Despite today's abundance of unlimited rate plans and broadband Internet, spammers continued to demonstrate a preference for small emails.



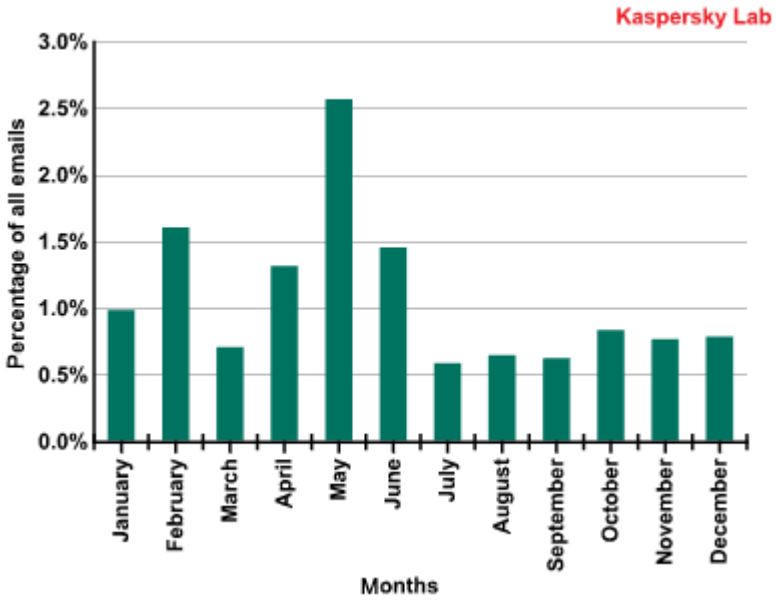
Types of spam email

The distribution of different types of spam emails did not undergo much change in 2008. Most spam emails are still text-based, which naturally result in such messages being small in size.

The most common language used in spam on the Russian Internet was Russian (of course), which represented 77% of all spam emails. The second most common language was English (14%). The percentage of other languages used in spam on the Russian Internet is a cumulative 9% and includes French, German, Italian and Portuguese.

Phishing

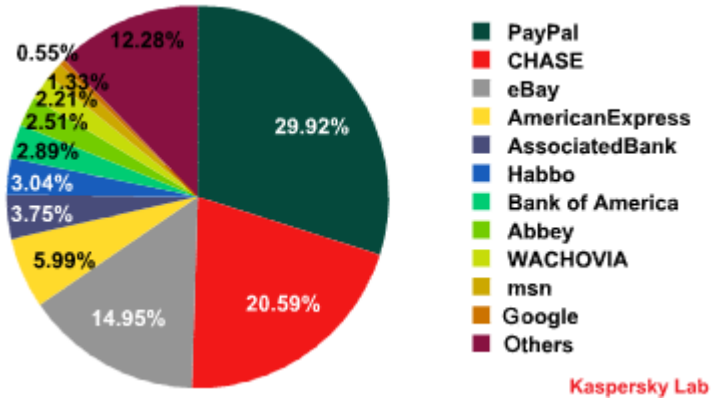
Spam containing links to phishing sites amounted to an average of 1.01%. In the first six months of the year, there was a great deal more phishing activity than in the second half (1.32% and 0.7%, respectively). A significant increase in the number of phishing attacks was also noted in May–June 2008.



Emails containing phishing links 2008

We expected to see much more phishing activity at the end of the year. It would have been logical if, in light of the financial crisis affecting hundreds of banks, phishers had reinforced their attacks against bank clients and used bankruptcy and other rumors to their advantage. Furthermore, during the Christmas and New Year's holidays, many people make online purchases and give and receive holiday e-greetings. With this in mind, cyber criminals actually had plenty of opportunities to launch attacks.

The lack of any burst of phishing attacks could possibly be explained by the closure of the McColo and Atrivo hosting services, which were used by scammers to host counterfeit websites and as control centers for botnets that were used to conduct mass phishing and spam mailings.



Top targets of phishing attacks

In 2008, phishers were most interested in the PayPal e-payment system, as more and more Internet users are opting to use these types of resources in order to make and receive payments. Phishers demonstrated much less interest in the confidential data of bank clients (in particular Bank of America and Wachovia). Remarkably, Chase Manhattan Bank was the target of a major attack in November and December 2008; the attack was so large that it put Chase high on the list of the top phishing targets in 2008.

Every month in 2008, attacks were launched against the Mail.Ru email service and social networking sites that are popular in Russia. Nevertheless, attempts were still made to steal money from Internet users, such as phishing attacks against the Yandex e-payment system.

We should expect attempts to steal user data to increase as the botnets that suffered in the autumn of 2008 begin to recover, especially under the conditions of today's crisis, which may be particularly conducive to fraud. In order to avoid becoming a victim of cyber scammers, just remember that no reliable Internet resource is going to ask its clients to enter confidential information on a webpage linked from an email.

Malicious attachments and links to infected websites

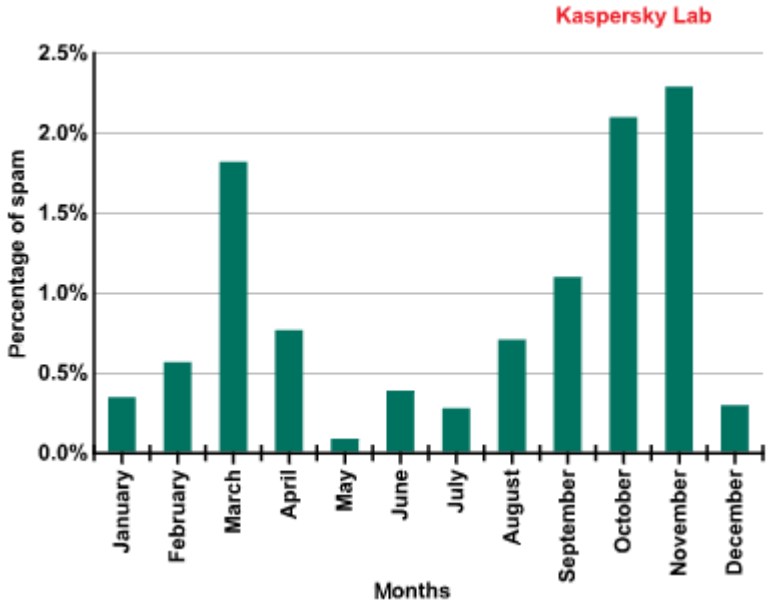
Data about malicious attachments in email was collected with assistance from Kaspersky Hosted Security, a Kaspersky Lab service offered to clients in Central Europe, the UK, the US, and Russia.

Emails with malicious attachments

These days, email is no longer the primary means of delivering malware and, consequently, poses a much lower threat of infection than in previous years. Emails with infected attachments are becoming less common as spammers have moved to sending emails with links to infected websites.

Nevertheless, the marked increase of 1.81% in March 2008, which was followed by a slight drop, the percentage of these types of emails continued to rise toward the end of

the year. There were a great many more emails with malicious attachments detected in the last six months of 2008 (1.12% of all mail traffic) compared to the first half of the year (0.66%). The average percentage of emails containing malicious attachments was 0.89% in 2008.



Percentage of emails with malicious attachments

The top 20 malicious programs found in emails in 2008

Trojan-Downloader.JS.Iframe.sh	31.07%
Backdoor.Win32.Hijack.e	8.98%
Trojan-Clicker.HTML.Agent.ag	7.73%
Backdoor.Win32.UltimateDefender.tt	4.42%
Trojan-Dropper.Win32.Agent.yzp	2.94%
Trojan-Dropper.Win32.Agent.xgg	2.72%
Worm.Win32.AutoRun.svl	2.02%
Trojan-Downloader.JS.Agent.cye	1.96%
Trojan-Downloader.Win32.Agent.algj	1.60%
Trojan-Downloader.Win32.Agent.afqa	1.52%
Trojan-Spy.Win32.Goldun.axt	1.46%
Trojan-PSW.Win32.Agent.lcc	1.37%
Trojan-Downloader.HTML.Agent.km	1.32%
Trojan-Dropper.Win32.Agent.xql	1.30%
Trojan-Downloader.JS.Agent.ckn	1.22%
Email-Worm.Win32.NetSky.q	1.12%
Trojan-Spy.Win32.Goldun.azl	1.11%

Trojan-Spy.Win32.Goldun.bbg	1.04%
Trojan.Win32.Buzus.hrp	0.98%
Trojan-Spy.Win32.Zbot.fql	0.92%

For the first time since we have been publishing our reports, something other than an email worm took first place among the most commonly emailed malicious attachments. The absolute leader in 2008 was a Trojan Downloader program, Iframe.sh, written in JavaScript and meant to execute a special code capable of downloading and launching other Trojans on recipients' computers.

If we group the malicious programs from the top 20 by behavior, then we get the following statistics:

Trojan-Downloader	39.66%
Backdoor	13.39%
Trojan-PSW	9.09%
Trojan-Spy	8.49%
Trojan-Clicker	8.02%
Trojan-Dropper	7.72%
Worm	3.96%
Exploit	1.96%
Trojan	1.62%
Email-Worm	1.45%

This table demonstrates the radical changes that have taken place in the malware landscape over the last few years. The Email-Worm behavior, which was designed to be spread by email and was the most dominant behavior in 2000–2005, is now in last place in terms of prevalence and has conceded its previous position to behaviors such as Trojan Downloaders, Backdoors, and other Trojans.

Malicious users have resorted to a variety of tricks in order to get Internet users to visit a site or open an attachment that contains malware. Delivery of malicious programs to a personal email account in the form of an archived file is one of the most well-known and common spammer tactics. Some methods used to "persuade" Internet users to unpack an archived file are nothing less than shocking.

For example, one English-language email informed the recipient that his or her child had been kidnapped (or "hijacked," according to the spammers) and demanded a hefty ransom. In order to view the photos of the abducted children, users were told to open an attached file that actually contained malware: Trojan-Downloader.Win32.Delf.bfc.

> **We have hijacked your baby**
> Hey We have hijacked your baby but you must pay once to us $50 000.
> The details we will send later...
> We has attached photo of your fume

Russian-language spam with malicious attachments did not resort to such ruthless methods and instead attempted to pique the interest of recipients by, for instance, inviting the user to attend a college reunion.

Emails with links to websites with malicious files

The most common way of spreading malicious programs in 2008 was to include links to infected websites in emails. Spammers gave preference to this tactic in the summertime especially. English-language emails tried to fool recipients by faking emails from well-known news agencies (such as MSNBC and CNN). Any users that attempted to view the "hot topics" would see a window pop up informing them that their flash player was out of date and asking them to download a new one in the form of an .exe file. However, instead of getting an updated application, they would actually download a Trojan Downloader. Malware was also put onto hacked websites in various domain zones.

> msnbc.com: BREAKING NEWS: London named top literary destination
>
> Find out more at http://breakingnews.msnbc.com
> ==========
> See the top news of the day at MSNBC.com, and the latest from Today Show and NBC Nightly News.
>
> ==========
> This e-mail is never sent unsolicited. You have received this MSNBC Breaking News Newsletter newsletter because you subscribed to it or, someone forwarded it to you.
>
> To remove yourself from the list (or to add yourself to the list if this message was forwarded to you) simply go to
>
> http://www.msnbc.msn.com/id/61402101, select unsubscribe, enter the email address receiving this message, and click the Go button.
>
> Microsoft Corporation - One Microsoft Way - Redmond, WA 98052
> MSN PRIVACY STATEMENT
> http://privacy.msn.com (http://privacy.msn.com/>)

Russian-language spammers also demonstrated their resourcefulness by claiming that the recipient's name was mentioned in a certain document allegedly published on the Internet. They would then attempt to lure the recipient to a resource on a .tk domain, where a Trojan Downloader was stored in the form of a .doc file.

There is another trick used to lure Internet users to a site: an invitation to download software — including antivirus solutions — for free. The computers of the victims of these scams would download one of the variants of Trojan-PSW.Win32, and the range of "services" offered ran the gamut from login and password autofill programs for social networking sites like www.odnoklassniki.ru to the latest antivirus program which would only function properly if the user switched off his current antivirus protection.

Emails with intriguing subject lines reminiscent of tabloid headlines would contain only a link to a website. Recipients did not have to download any special programs to view the "news" — a program would automatically download once the user clicked the link.

Spammer techniques and tactics

HTML Spam

While 2006 can be called the year of graphical spam, and 2007 was a year for experimenting with attachments, 2008 was the year of HTML spam. Many old tricks were used by spammers, but the concept was reworked to take advantage of the idiosyncrasies of HTML.

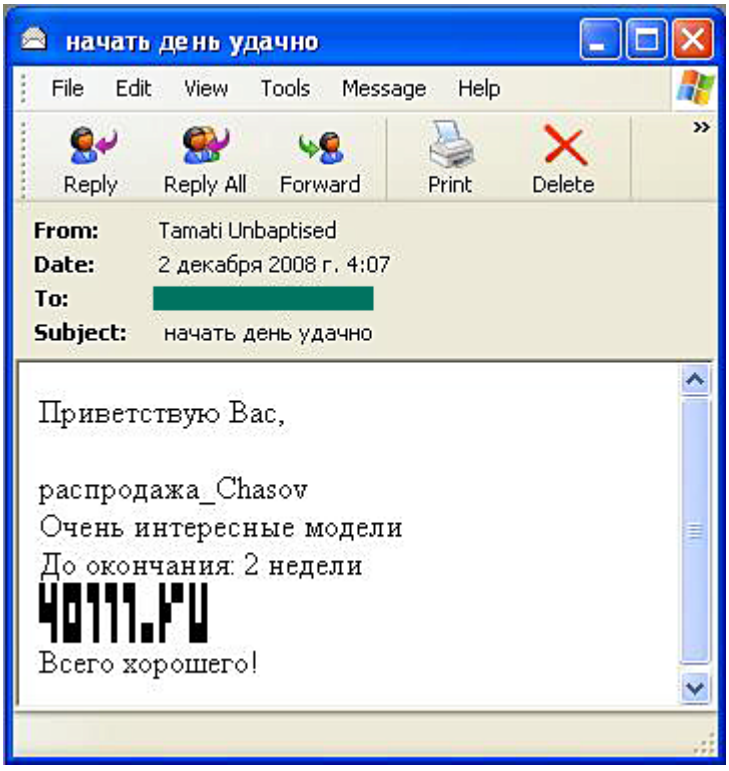
Using random symbols and characters as “noise” is one of the more common spammer tactics. This time, random characters were inserted into tags, which aren't visible to the reader. This method is very similar to the classic "white text" technique. What happens is that spammers add random sequences into the text using HTML tags, which most email clients see as auxiliary, which means they are not displayed to the recipient. These are comment tags, color tags, etc. The recipient will see only the advertising text, which is actually only a small portion of the email.

An email written with HTML tags	*The same email as it is seen by the recipient*
<html> **<!-- random sequence of letters or words-->** <body> Hi! **<!-- another random sequence of letters or words-->** Come visit my awesome site supersite.com **<!-- yet another random sequence of letters or words-->** </html>	Hi! Come visit my awesome site {site}.com

Spammers also used pseudo-text, or random sequences of characters in HTML tags which were actually not tags at all. Most email clients parse these “incorrect” tags as an error and do not display them to the recipient.

We have seen one method that at some point was dubbed “The Mona Lisa.” In this trick, contact information is shown to the user in the form of a graphic comprised of characters and symbols. Previously, spammers used primarily letters and spaces, but now spammers are using combinations of black and white cells in HTML tables.

The example below shows an URL displayed in the form of an HTML table:



This email invites the recipient to start his day on the right foot by visiting a website that sells watches. The address, 40777.ru, is a graphic made from an HTML table.

The table format has also been used to break up keywords in emails in order to avoid detection by spam filters:

An email using HTML code	*The same email as it is seen by the recipient*
<table> <tr> <td align=right>VI</td> <td align=left>AGRA</td> </tr> <tr> <td align=right>CIA</td> <td align=left>LIS</td> </tr> </table>	VI AGRA CIA LIS

In addition to the methods addressed above, spammers have used the following browser loophole: the symbols used in an URL can be encoded using various methods (16-bit ASCII, 8-bit ASCII, ASCII for HTML, etc). Furthermore, the browser will open the site correctly if it is entered as a hyperlink in an email. The browser will open the correct site, even if different code is used in a link or if the link contains certain errors.

For example, narod.ru can be written as:

%6e%61%72%6f%64%2e%72%75

Or even as:

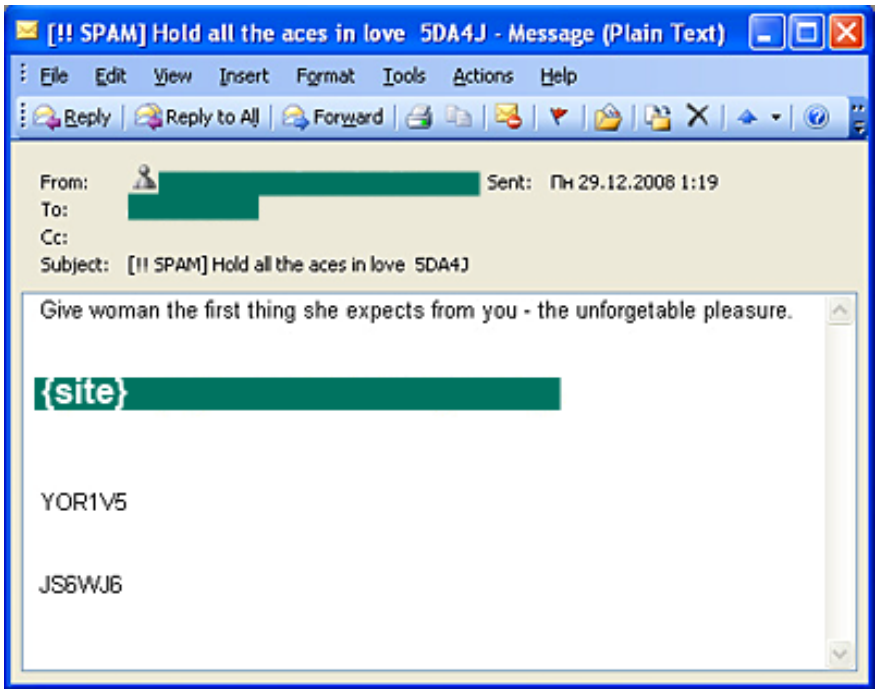
narod.r&#x000075

There can be any number of zeros, and any letter can be written “as normal” — the link will still open the site.

Advertising on free hosting services

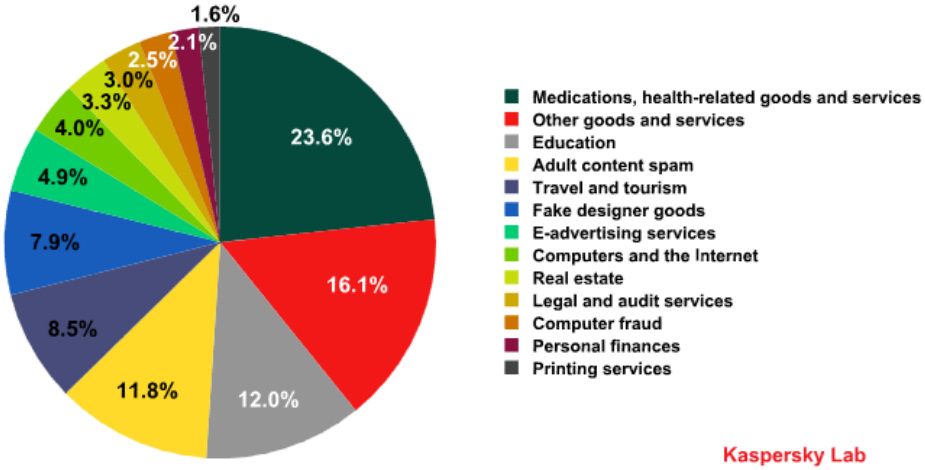
Yet another popular technique used to spread spam in 2008 was the use of free, public web services. Spammers would hold a webpage (or a redirect to their page) on a well-known hosting service or blog that was linked in the spam email.

This approach is designed primarily to bypass filters that work based on reputation. It also relies on the fact that a filter will not block their page, since the link leads to a well-known, legitimate service. Large hosting services were used, such as Google Docs, Microsoft SkyDrive, Microsoft Livefilestore, and others.



Many free services offered by email providers and other large Internet resources do not carefully track content. Note that a variety of old hosting sites and blogs for which this service is the sole or primary function (such as LiveJournal and LiveInternet) were not targeted by spam attacks. Clearly, security and protection against spam on these services is considerably better than that offered by newer services. It is the accessibility and lack of protection which allows spammers to take advantage of these newer services.

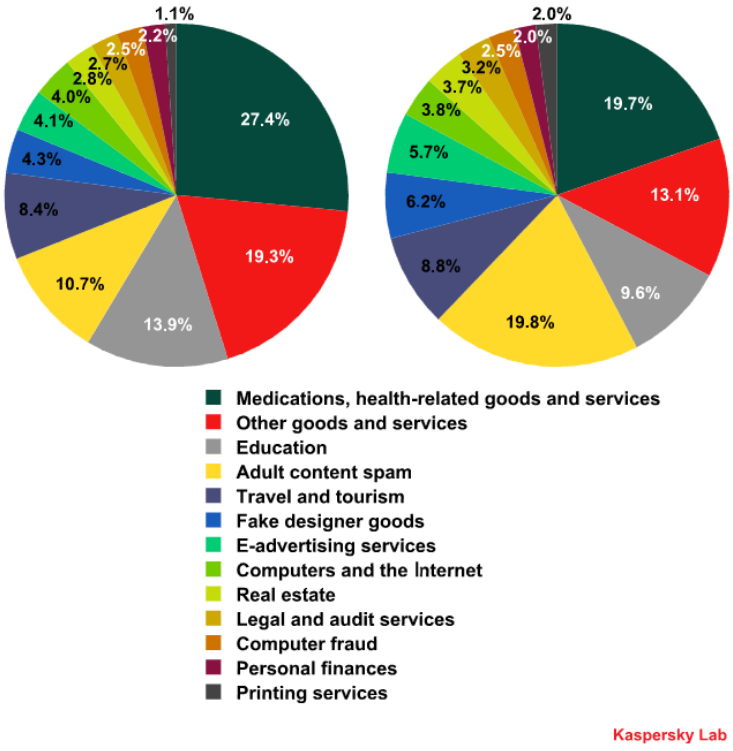
Spam by category



Spam by category on the Russian Internet in 2008

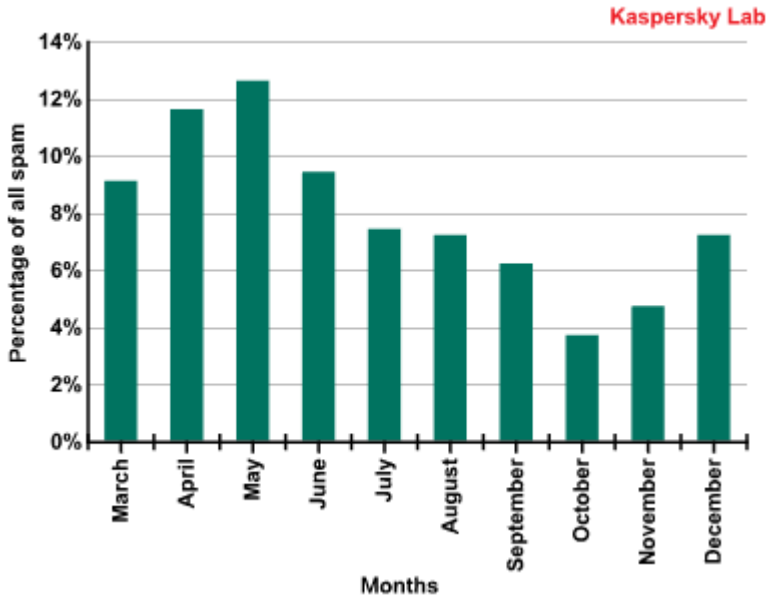
Despite the fact that the different categories of spam do not undergo many changes, the makeup of the categories did change substantially in 2008. New categories emerged throughout the course of the year and the most prevalent categories also changed. This is particularly evident if one compares movement among the categories in the first six months of the year to movement in the second half of the year.

Spam by category in the first and second half of 2008



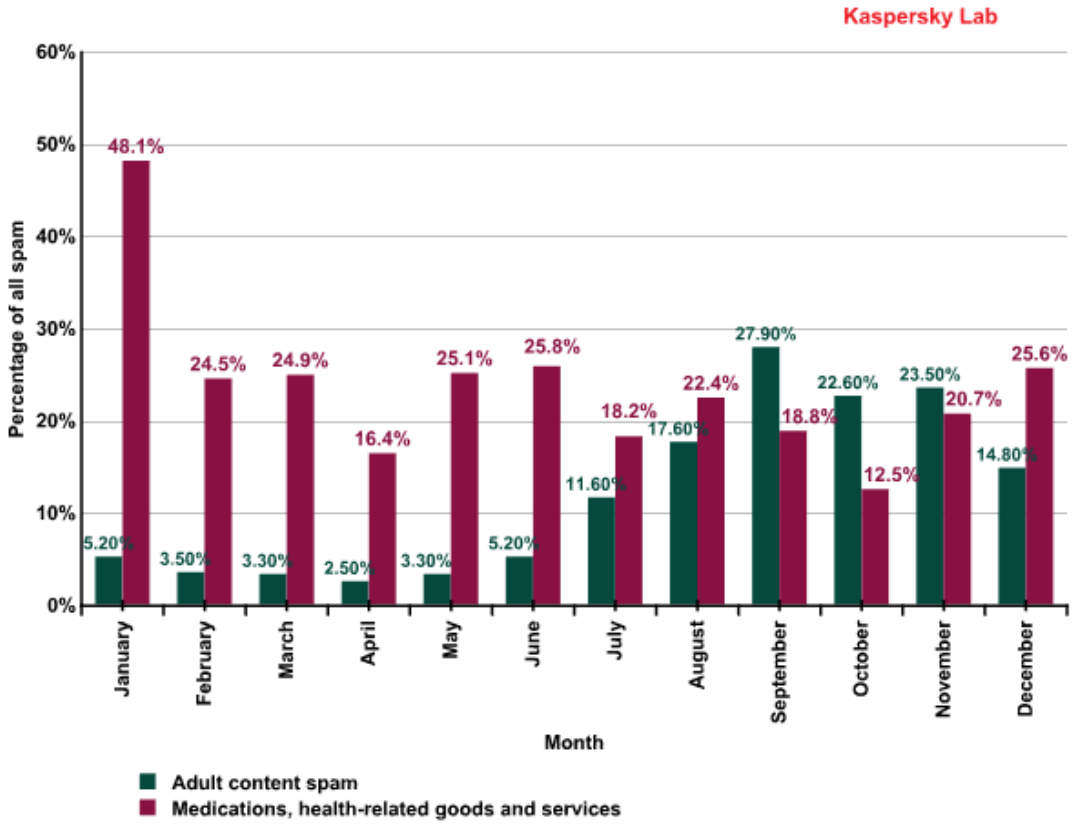
Note that the Other goods and services category fell by 6.4% in the second half of the year. This category tends to reflect the number of orders received by spammers from the real economy.

The month of March arrived with the appearance of a Russian-language advertisement for fake luxury goods. This new category immediately climbed into the top three spam categories. The relative percentage of this spam, after achieving its peak in May, began to gradually fall thereafter. However, we can expect this type of unwanted correspondence to find its own niche in Russian-language spam (just as it will in English-language spam) and remain at a level of 5–6% of all spam.



Fake luxury goods

The number of Russian-language emails with links to pornographic websites began to increase in July. In the second half of the year, Adult content spam increased by over 15%. One of the ways spammers make money from this type of spam is to drive traffic to a website. The rapid growth in the number of emails in this category put it in first place, pushing aside Medications and health goods and services, which was the long-term leader. Adult content spam maintained its position in first place for three months.



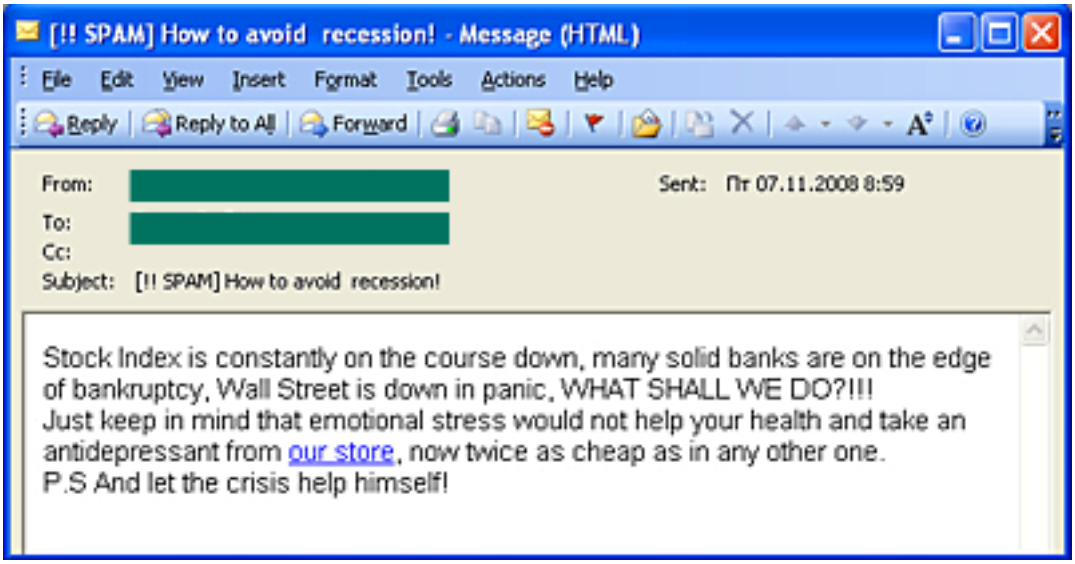
Categories

In November the amount of Adult content spam decreased, possibly as a result of the closure of the McColo hosting provider and the difficulties faced by spammers in finding a new home for their botnet control centers. Furthermore, fraud is predominant in this category of spam. The porn websites that users are linked to in an email often tell users to send a text message to a fee-based short number in order to view content. The swindlers promise that the cost of the text message will be minimal (RUB 5 – 7), although the actual cost of the text message is much higher (about RUB 300). It is possible that the reduction in the amount of this spam was related to the fact that Internet users caught on to the scam and stopped falling for the bait.

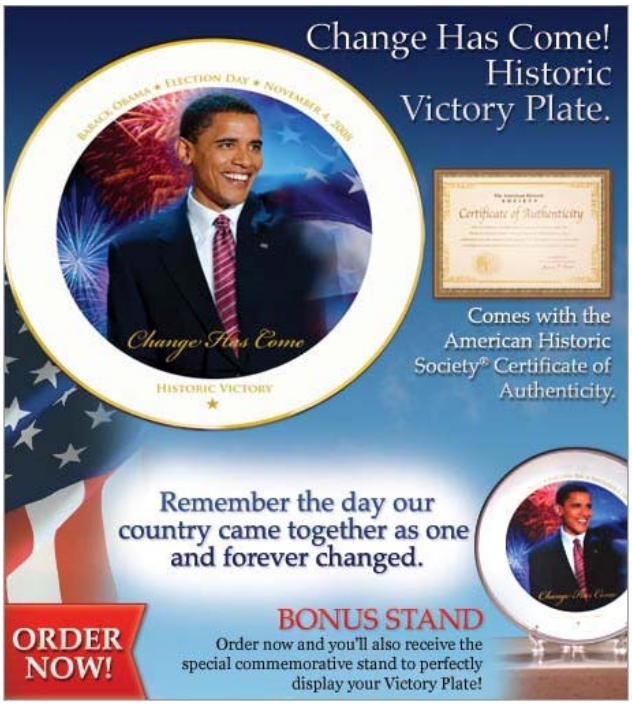
The emergence of new spam categories and mass mailings conducted over a long period of time demonstrates there are some major players in the Russian spam industry who have the resources required to carry out these large-scale operations.

Spam and global events

It is a well known fact that referencing global events will get Internet users to read spam emails. This year the main events included in spam were the World Cup, the US presidential elections, and of course the global financial crisis. What's interesting is that despite expectations, most emails that mentioned the crisis did not fall into the Personal finance spam category. They did not advertise special loan offers, nor did they promote any get-rich-quick schemes. Most of the crisis-themed spam emails advertised a variety of anti-crisis seminars. Furthermore, the crisis was a recurring theme throughout many advertisements for a wide range of goods and services.



The elections in the US were another major theme in spam mail in 2008. During the presidential campaign (and before and after it), spammers mentioned the elections in order to advertise different goods and services and in attempts to spread malicious programs. There was no limit — practically any and every subject mentioned Barack Obama. Even ads for Viagra sported headlines such as “Obama didn’t receive free pass” and “Barack Obama’s Victory Speech.” Other spam advertised souvenirs with Obama’s image. We wrote about spam that promoted busts of Putin in the spring of 2005. In 2008, we saw spammers offering commemorative plates with the new US president’s portrait.



Conclusion

The global financial crisis, which has affected almost every sector of the real world economy, has also had an impact on cybercrime. The types of spam directly linked to the real economy are losing ground. Meanwhile, spammers have turned to using technologies that can help them make some fast cash, such as fraudulent spam using text messaging and driving traffic on pornographic websites.

The drop in the percentage of spam advertising goods and services demonstrates that the number of orders received by spammers from real business has also decreased. Meanwhile, increased criminal spam attacks clearly point to the fact that cyber criminals are starting to suffer from a loss of income and are looking for new ways to make money.

It should be borne in mind that spam is a global phenomenon, and changes in its structure — even before the crisis spread to Russia — may reflect the state of the economy. If the correlation between spam structure and macroeconomic processes turns out to be rather strong, we may be able to predict the end of the crisis by observing spam trends.

For now, Internet users need to bear in mind that the crisis has created the preconditions needed for phishing to prosper and grow, especially phishing aimed at bank clients and users of e-payment systems. In terms of criminal trends in spam, we can expect another wave of Adult content spam.

We do not expect spam to decrease in 2009; instead, the volume of criminalized spam will likely rise. Furthermore, in today's crisis conditions, spam may become the only means of advertising accessible to a large number of businesses.

Given the instability of the global economic situation, these forecasts refer to the first six months of 2009. Kaspersky Lab will continue to track the latest developments in spam evolution.