



Q4 2008 Internet Threats Trend Report

Spam and Malware Levels Bounce Back Post-McColo

January 12, 2009

Introduction

The major Internet-threat related news of the fourth quarter was the downfall of one of the largest, most notorious Web hosting services, McColo, which temporarily reduced global spam levels to one-third their usual level. As a result, spam levels during the fourth quarter reached their lowest point for the year: 59 percent of all email. Spam levels over the course of 2008 ranged from 59 to 94 percent of all email sent on the Internet.

Also throughout the quarter, as they did during the rest of the year, spammers and malware distributors exploited legitimate sites to bypass traditional content filtering technologies. They hid their illegitimate content on various legitimate sites and employed social engineering tactics (e.g. e-cards, outlandish headlines) to trick users.

Additionally this year, user generated content has undergone massive expansion, and more and more users are blogging or participating in the collective exchange of knowledge around the world. Malicious script writers have branched out into the arena, introducing an increasing number of blended threats and devising new plans to attempt to infect users' machines.

Q4 2008 Highlights

- Streaming media and downloads are among the top 10 Web site categories infected with malware and/or manipulated by phishing. These are two of the most popular categories within user generated content sites.
- McColo, one of the largest hosts of cyber-criminal gangs was effectively shut down in November 2008, causing spam levels to drop to one-third their usual level for several weeks.
- Spam levels averaged 72% of all email traffic throughout the quarter, falling briefly to 59% following the McColo closing in November.
- An average of 301,000 zombies were newly activated each day for the purpose of malicious activity.
- Brazil led in zombie computer activity, producing 14.6% of zombies at the end of the quarter.
- Spammers continue to exploit legitimate sites like Google docs to bypass content filtering systems.

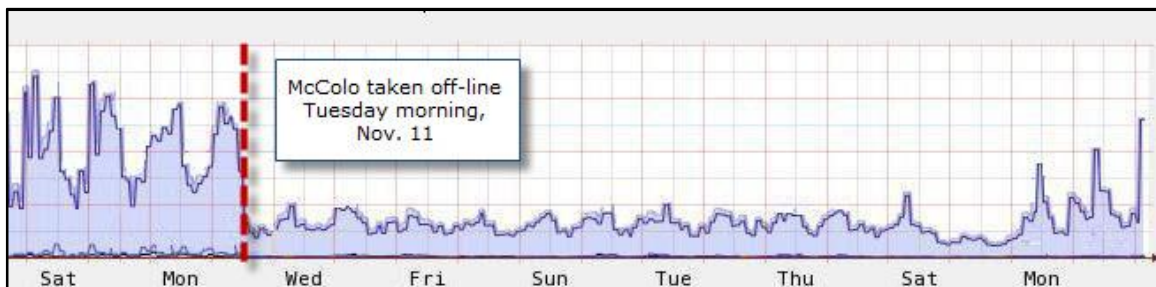


Effects of McColo Closing Felt Across the Web

The major event of the fourth quarter was the shutdown of San Jose, Calif.-based McColo, a major Web hosting service, whose client list experts say included "some of the most disreputable cyber-criminal gangs in business today." On the afternoon of Tuesday, November 11, the Commtouch lab noted a sharp drop in worldwide spam. There had been steady growth in spam levels over the past several years so this sudden drastic change was an unusual occurrence.

Brian Krebs of the Washington Post blog was the first to describe how backbone providers took McColo offline. McColo's client list included many pornography sites and companies like *viruslivescan.com* which installs spyware while purporting to scan your computer for viruses.

Through the years, numerous spammers have been criminally prosecuted or simply taken offline. but it rarely causes even a slight blip in spam graphs. If there is any movement, it is typically overshadowed by other spammers who fill the void with more spam of their own. In this case, however, there were several weeks of spam levels that were meaningfully lower than normal.



Source: Commtouch Labs

**Peaks represent spam outbreaks*

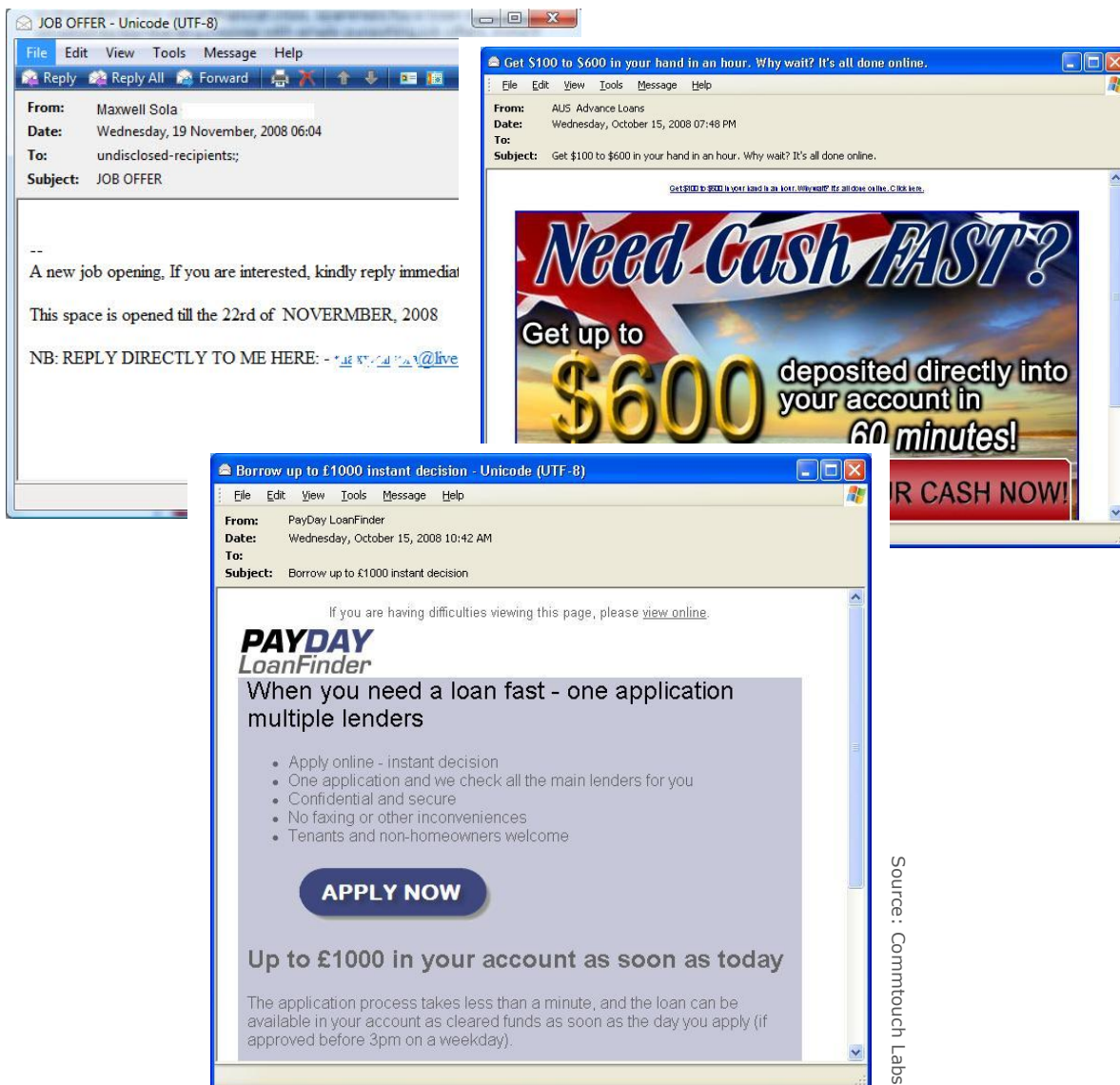
As seen in the graph, spam levels dropped abruptly when McColo was taken offline on Tuesday morning, November 11. This drop, bringing spam levels to a third of the normal volumes, was followed by nearly three weeks of significantly lower spam levels and finally a slow increase.

By the end of Q4, spam levels had returned to levels closer to those before McColo was taken offline.



Spammers Exploit the Financial Crisis

In the wake of the global financial crisis, spammers have been exploiting the situation by bombarding inboxes with emails purporting job offers, instant loans and cash advances. As seen below, these types of spam messages have been received throughout the world, with each message touting a different currency and different benefits. The universal theme: the opportunity for easy money in these difficult economic times.



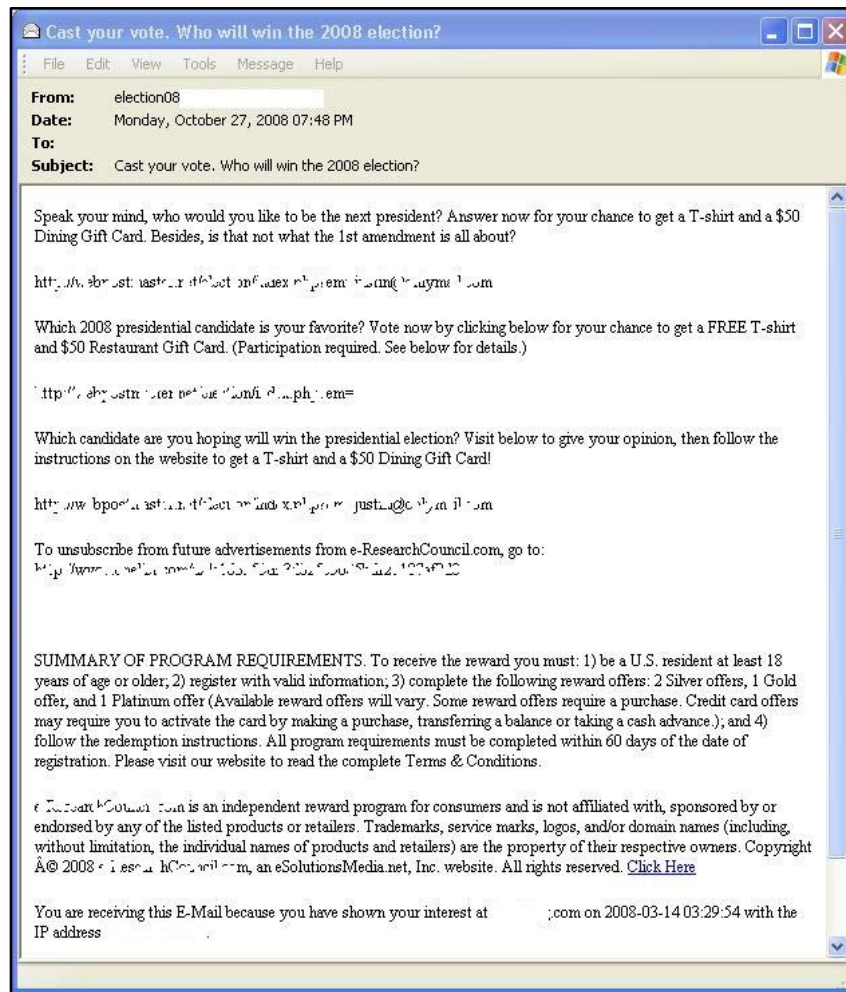
Source: Commtouch Labs



Presidential Election Fever in Spam and Malware

November 4 was Election Day in the United States, which prompted a flood of spam and malware related to the elections. Some spammers sent emails inviting users to participate in pre-election polls in order to win gift cards and T-shirts. Some of the links led to phishing sites stealing personal information from unassuming users or to malware sites that downloaded malicious software onto computers.

Many of these messages appeared to be genuine including an option to unsubscribe and a summary of program requirements as seen in this example:



Source: Commtouch Labs



After the election, there were several outbreaks of Barack Obama-related spam and malware messages. One outbreak was a simple blended threat that offered to show recipients the Obama acceptance speech, but instead downloaded the malware executable barackobama.exe. After the election, a new wave of Obama spam surfaced advertising an Obama sex scandal.

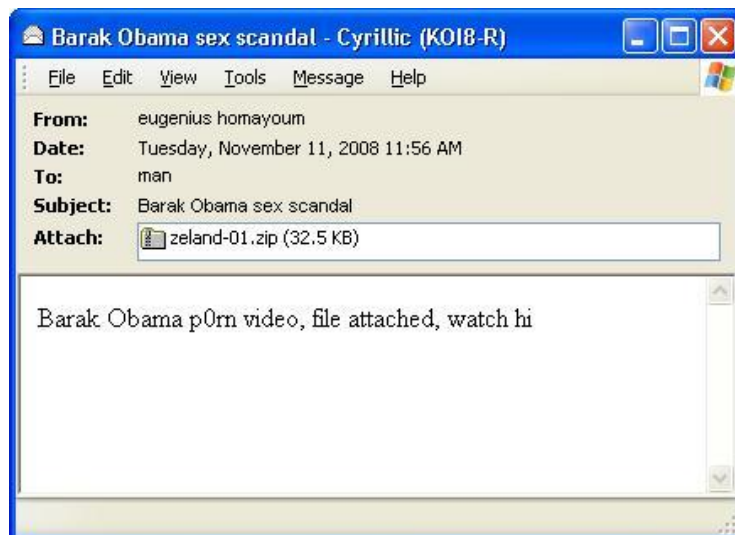
Below is a sample from an outbreak that began November 5, the day after Obama was elected:



Source: Commtouch Labs

In a separate outbreak less than a week later, malware was included as a file attachment, zeland-01.zip.

The messages pictured here were sent from zombies (aka botnets), which are typically home computers that have been taken over by spammers or malware distributors, and tend to come in and out of use as they are needed. The best way to block such messages is to use an email filtering solution that blocks zombie-generated mail based on the sender's reputation, rather than to rely on an anti-virus solution which may or may not have a signature for that particular variant.



Source: Commtouch Labs



New Blended Threat Outbreak Reminiscent of First Storm

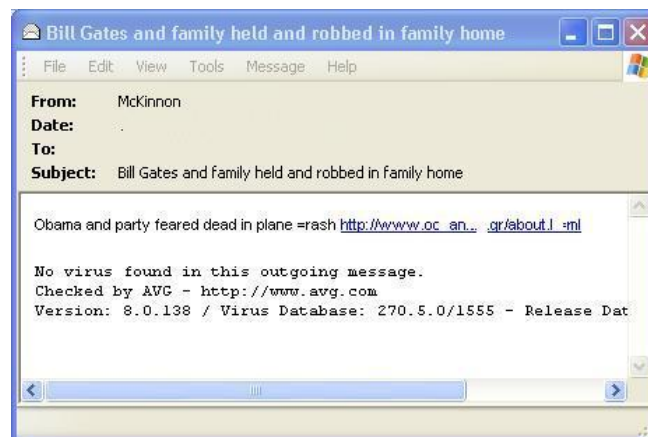
In mid-October, a new blended threat outbreak surfaced with subject lines and contents that were reminiscent of the original "Storm" outbreak from 2007 which created outlandish headlines to socially engineer people to open malware.

The latest case included headlines that were more topical to the events of September and October, including:

- Private investigation report on your colleague
- Iran announces completion of nuclear weapon
- Afghan capital in mourning
- India makes first nuclear bomb
- Sony stocks dips as president dies

There were also some celebrity and movie-related themes, such as:

- The loves of mini-me
- Nicole Kidman bedroom pics revealed



Source: Commtouch Labs

Spammers typically employ randomizing tactics to change message subjects and bodies automatically, thus cloaking the mass distribution and evading some anti-virus or anti-spam engines. In most of these Storm cases, the "randomize" function was not optimized and the subject line and the contents did not match. For example, in one message where the subject was "Bill Gates and family held and robbed in family home" the content of the message read "Obama and party feared dead in plane crash."

In this outbreak, malware files were placed on legitimate (but compromised) Web sites in order to bypass email filtering solutions. This placement demonstrates the need for Web security solutions to analyze Web sites' full depth, and not just block or allow based on the domain since in these cases, the domains were all legitimate Web sites. Clicking on the links forced an automatic download of *watch.exe*, a malware executable file.



Chinese-Language Spam and Blended Threat Malware

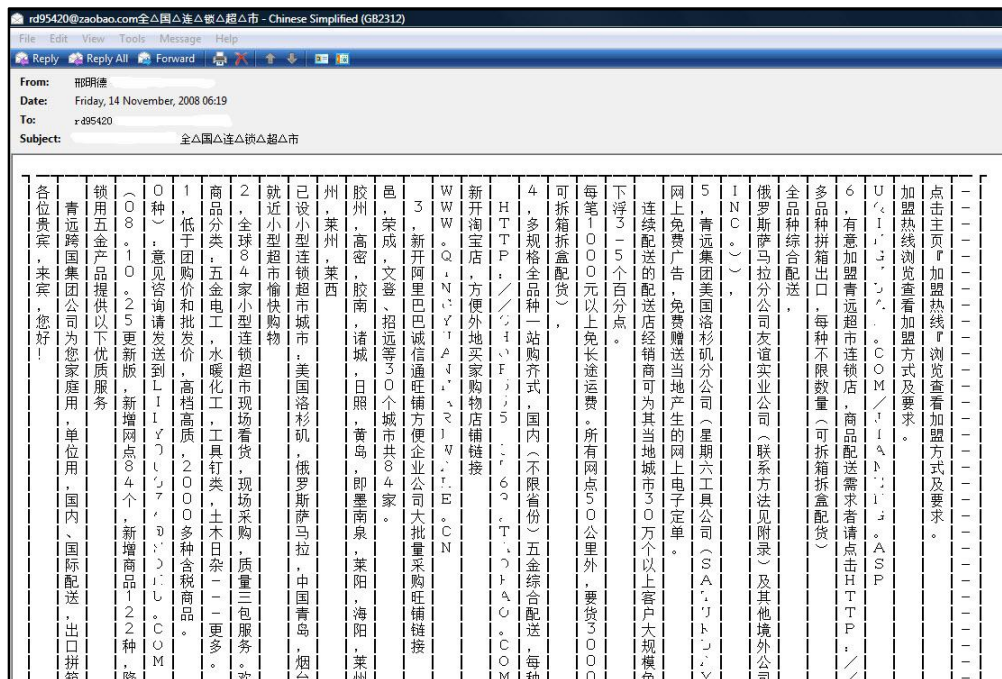
At the end of October, a growing trend emerged in the spread of Chinese-language spam and blended threat malware. Here is an example of a recent outbreak of Chinese e-card messages, a blended threat where email messages are sent as spam containing links (and in this case an HTML attachment) to malware sites.



Source: Commtouch Labs

Both the link within the message and the attached HTML file lead to the download of the malicious *boss.exe* malware.

Another outbreak in mid-November included Chinese messages arranged vertically as seen below; the vertical alignment helps bypass content filters that scan text horizontally. In this example, a construction material company was promoting a sale, with details including URLs:

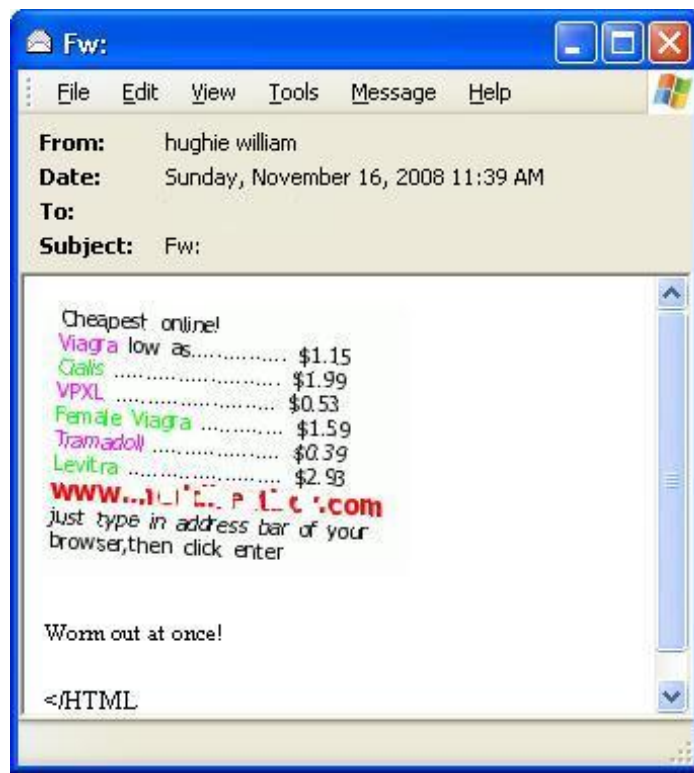
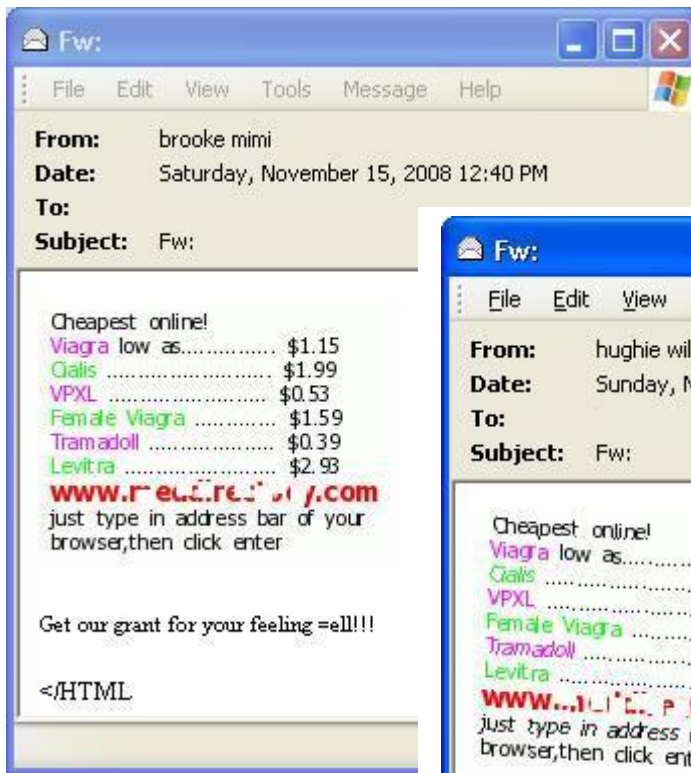


Source: Commtouch Labs

The Resurgence of Image Spam

Image spam experienced its heyday in early 2006 and began to taper off as anti-spam filters improved at blocking it, which decreased profitability for spammers. In November, however, there was a brief resurgence of this type of spam.

As seen in the following samples, image spammers kept the content nearly identical but slightly altered the image to try and confuse anti-spam technologies that analyze images based on optical character reading (OCR); in the second example, the image sits at a slight angle. Both images include URLs embedded into the image.



Source: Commtouch Labs



Google Docs Spam Makes a Comeback

Throughout 2008, spammers have been exploiting legitimate tools (or what appear to be legitimate) like Google Docs, Flickr, Blogger and Blogspot for illegitimate activities. This quarter, a new outbreak using Google Docs emerged.



Source: Commtouch Labs

One advantage of hosting content on a system like Google Docs is that the spammers can leverage Google's strong reputation. This helps email messages that contain Google Docs hyperlinks to get past traditional anti-spam methods. Many traditional filtering solutions do not have the depth-of-knowledge necessary to block one Google Docs link (containing the spam content) vs. another one (containing legitimate content). Using a legitimate site like Google Docs to host spam content will either bypass traditional email and Web filtering solutions, or "train" them that Google Docs is corrupt, which leads to false positives, i.e. blocking of legitimate content.

The Google Docs spam outbreak pictured above took place at the end of November, and advertised dating and pharmaceuticals.



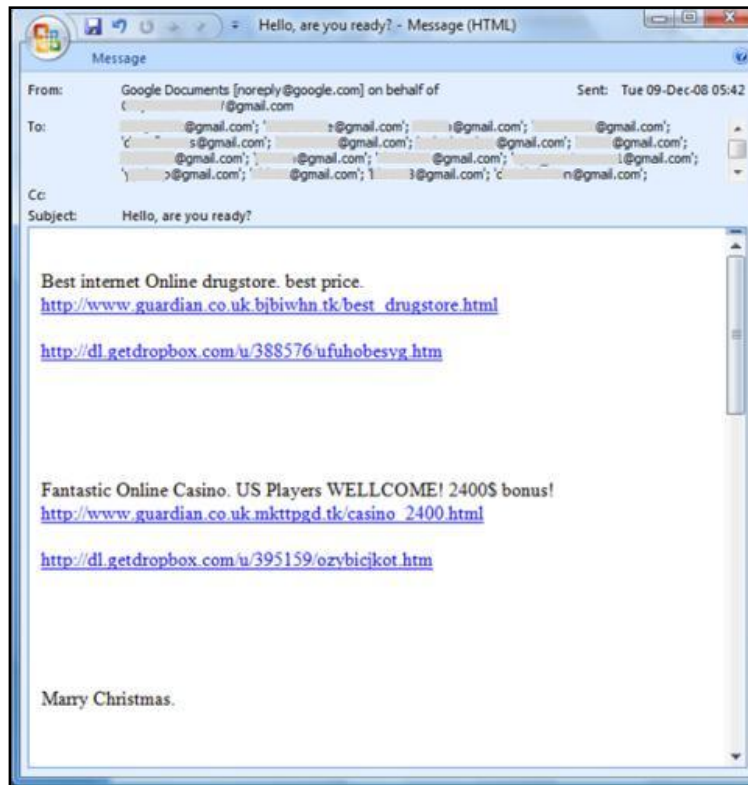
The landing pages have a much more professional look than earlier Google Docs outbreaks.

Commtouch Recurrent Pattern Detection Technology blocks this type of spam because they are identified based on the recurrent patterns in the message outbreaks.

In early December, another such attempt to exploit Google Docs surfaced. The emails appear to have been sent from Google Docs using the "Share" function and every recipient is a Gmail user. The text of the message contains completely unconnected "services" being offered - both prescription drugs and gambling.



Source: Commtouch Labs



Source: Commtouch Labs



Culture Clash

Spam is written in nearly every language; sometimes Portuguese-language spam is circulated in Russia or Chinese-language spam finds its way to Italy. Recently, the translation of some German language spam into English, yielded proof that cultural differences carry over into the world of spam, beginning with the fact that the email – selling sexual enhancers – was written in third person to denote respect, something that does not typically occur in English-language pharmaceutical spam outbreaks.

One of the paragraphs reads:

Life is too short – enjoy it to the fullest.

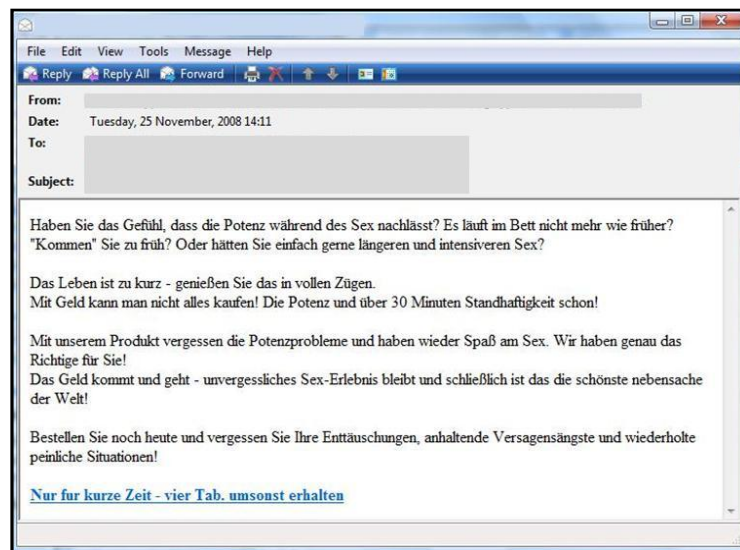
Money can't buy everything! (like) the potency and steadfastness of over 30 minutes now!

And another part reads:

Money comes and goes – (but the) unforgettable sex experience remains forever, and after all this is the next best thing in the world!

Order today and forget your disappointments, persistent fears of failure and repeated embarrassments!

The link pointed directly to the same Canadian Pharmacy that is notorious for sending spam in English with messages like "Impress your girlfriend;" apparently spammers are segmenting their target markets with different messages just like legitimate marketers.

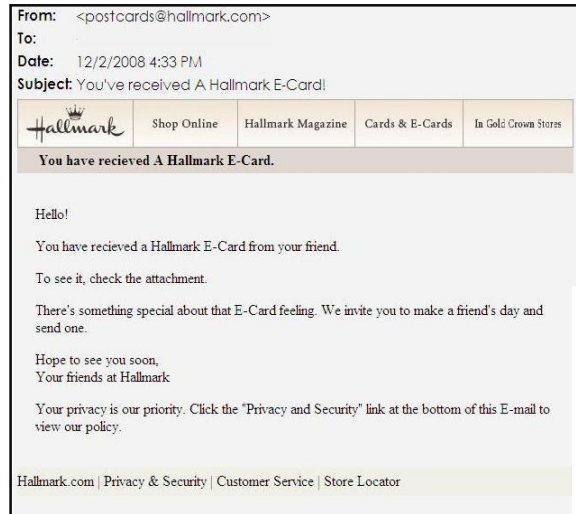


Source: Commtouch Labs



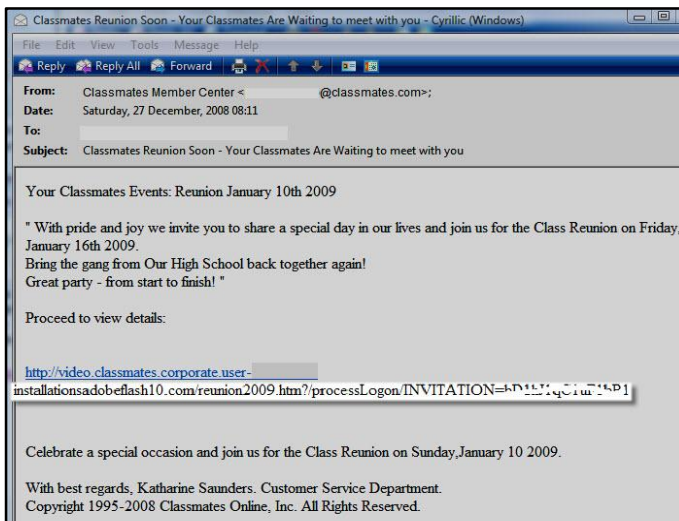
Spammers Continue to Exploit Legitimate Sites

Electronic cards containing malware have become an annual holiday tradition just like sugar plum fairies and the partridge in a pear tree. The latest trend amongst malicious code writers is a plain text or very simple email that appears to have been sent from a legitimate e-card source. When an unsuspecting recipient clicks on the link, Trojan software is downloaded onto the computer. Sometimes a user may be prompted to download a plug-in to receive the holiday greeting, or the link may simply lead to a site that downloads the Trojan automatically.



Source: Commtouch Labs

Note the prompt to open an attachment on the above example of a fake e-card greeting.



Source: Commtouch Labs

Another site that has been targeted is the popular Classmates.com. An outbreak in December enticed recipients to download a plug-in with the promise of seeing a video montage of their graduating class. Like the fake Hallmark emails, these "plug-ins" are actually Trojans.

Many content-based filters do not block messages that appear to come from legitimate sites in order to avoid blocking valid messages (i.e. false positives).



Web Threat Trends: Malware and Phishing Sites

During the fourth quarter of 2008, Commtouch analyzed which categories of Web sites were most likely to contain malware or phishing. Internet users may not be surprised to find that adware and prescription drug sites may be infected with malware or phishing schemes, especially if they have reached these sites via spam messages. What may be more surprising is that many Web-based email sites, search engines and sites promoting the use of tobacco and alcohol are also in the top ten lists of infected sites.

Top 10 Web Categories Infected with Malware

Rank	Category
1	Criminal activity
2	Advertisements & pop-ups
3	Phishing & fraud
4	Web-based email
5	Spam sites
6	Health & medicine
7	Download sites
8	Search engines & portals
9	Gambling
10	Sex education

Source: Commtouch Labs

Top 10 Web Categories Manipulated by Phishing

Rank	Category
1	Criminal activity
2	Advertisements & pop-ups
3	Hate & Intolerance
4	Illegal drugs
5	Violence
6	Alcohol & tobacco
7	Job search
8	Social networking
9	Download sites
10	Gambling

Source: Commtouch Labs

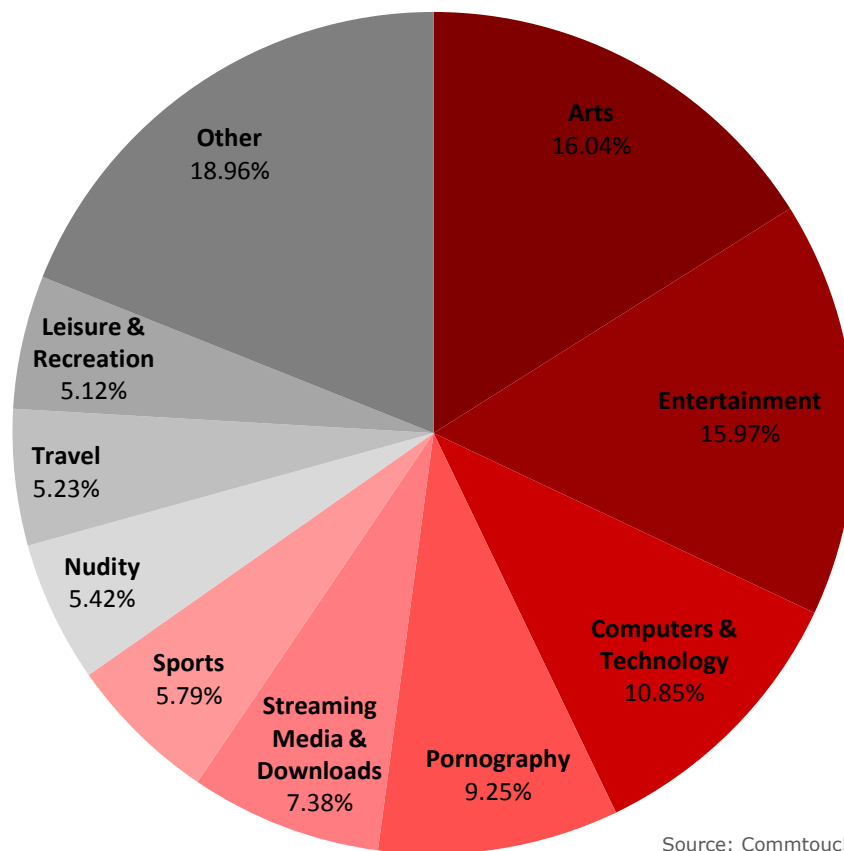


Web 2.0 Trends

In an analysis of six of the most popular user generated content hosts, art was the most popular subject covering more than 16 percent of the content being generated. Following closely behind was entertainment (16 percent) and computers and technology (11 percent). Pornography and sexually explicit content placed fourth with 9 percent.

When evaluating user generated content in relation to malware and phishing, some of the most popular categories appear on both lists. Streaming media and downloads, for instance, are among the top 10 Web site categories infected with malware and/or manipulated by phishing. They are also two of the most popular categories within user generated content sites.

Most Popular User Generated Content



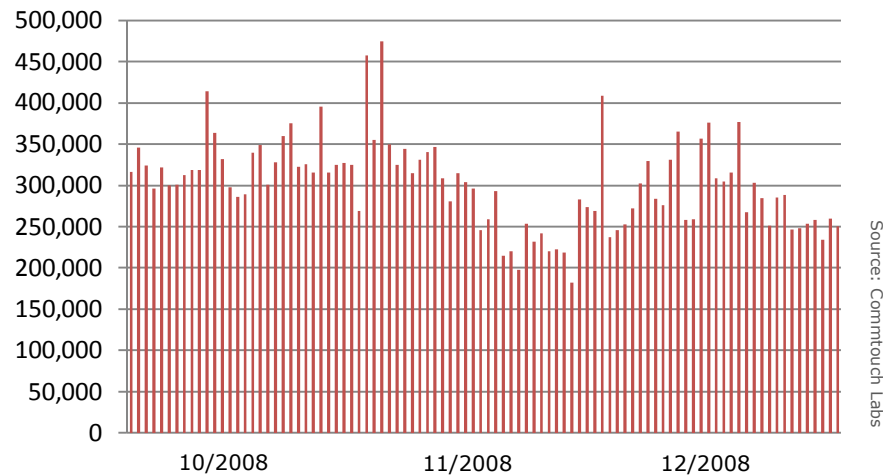
Source: Commtouch Labs



Newly Active Zombies

The lifespan of zombies is very short, and according to Commtouch Labs, the fourth quarter saw an average turnover of 301,000 zombies that were newly activated each day. The graph below shows the *newly* active zombies each day throughout the quarter.

Q4 Newly Active Zombies



Zombie Hot Spots

Two newly added domains to the top ten zombie hot spots, both based in Brazil, are:

- brasiltelecom.net.br
- veloxzone.com.br

Those that slipped below the top ten ranking among zombie hot spots at the time of this report include:

- verizon.net
- mtu-net.ru

Top 10 Zombie Hot Spots – Average Per Day

Rank	Domain	# Zombies
1	telesp.net.br	27,211
2	163data.com.cn	26,016
3	tpnet.pl	22,624
4	brasiltelecom.net.br	20,953
5	ttnet.net.tr	20,315
6	telecomitalia.it	18,501
7	asianet.co.th	16,354
8	ukrtel.net	16,025
9	veloxzone.com.br	14,369
10	airtelbroadband.in	9,840

Source: Commtouch Labs



Three of the top ten zombie hot spots are Brazilian service providers and as a country, Brazil is responsible for more than 14% of the zombies produced globally according to the Commtouch Zombie Lab.

Top Spam Topics

In spam topics, pharmaceutical spam regained the number one spot with 42% of all spam, compared to the previous quarter, where it had temporarily dropped to 19%. Sexual enhancers fell from the number one slot, comprising 23% of all spam in the third quarter, to only 7% in the fourth quarter of 2008.

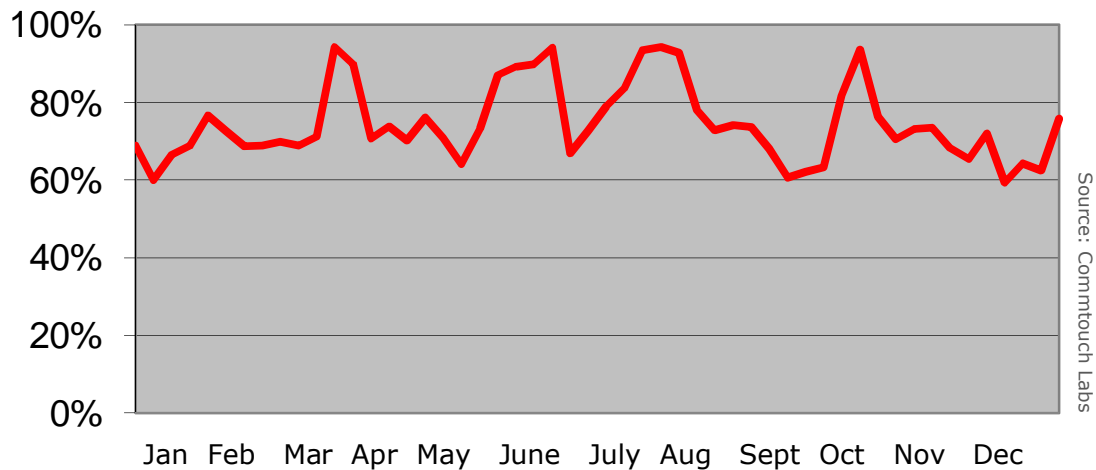
Topics of Spam Email Q4 2008	
Pharmacies – 42%	Enhancers – 7%
Replicas – 15%	Casino – 6%
Other – 14%	Mortgage/Loan – 3%
Pornography – 12%	Software – 1%

Source: Commtouch Labs

Spam Levels

Spam levels averaged 72% of all email traffic throughout the quarter and peaked at 94% in October, pre-McColo, then bottomed out at 59% in early December, post-McColo.

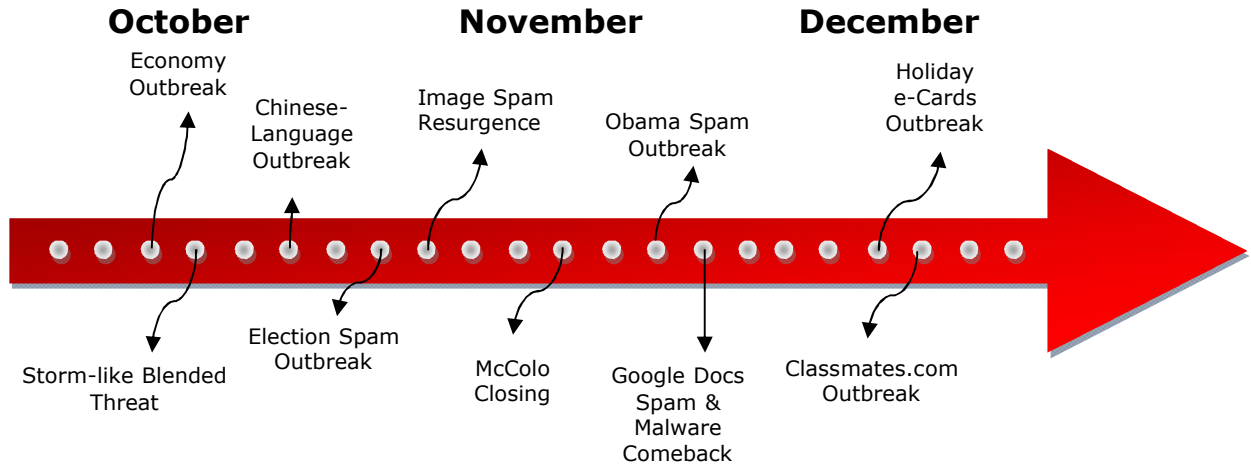
2008 Spam Levels



Source: Commtouch Labs



Q4 2008 Outbreaks in Review



About Commtouch

Commtouch® (NASDAQ: CTCH) is the source of proven messaging and Web security technology for scores of security companies and service providers, founded on a unique cloud-based datacenter approach. Commtouch's expertise in building efficient, massive-scale security services has resulted in its patented technology mitigating Internet threats for thousands of organizations and hundreds of millions of users in more than 100 countries.

Commtouch technology automatically analyzes billions of Internet transactions in real-time to identify new threats as they are initiated, protecting email infrastructures and enabling safe, compliant browsing. The unmatched suite of Commtouch security offerings is based on patented Recurrent Pattern Detection (RPD™) and GlobalView™ technologies, which work together in a comprehensive feedback loop and offer equally effective protection for all languages and formats.

In the past year, Commtouch was awarded Frost & Sullivan's European Messaging Security Technology Innovation of the Year Award and Deloitte's Fast 50 (Israel) and Fast 500 (EMEA) awards.

Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif.

Stay abreast of the latest trends all quarter long, at the Commtouch Café:

<http://blog.commtouch.com>. For more information about enhancing security offerings with Commtouch technology, see www.commtouch.com or write nospam@commtouch.com.

© Copyright 2009 Commtouch Software Ltd. All Rights Reserved. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.