



Q1 2008 Email Threats Trend Report

Zombies Depend on the Kindness (and IT Resources) of Others

April 7, 2008

Spammers and malware distributors are continuously seeking new techniques to bypass email filtering engines, and throughout the first quarter of 2008, the primary trend was to leverage legitimate content and sites for their own purposes. Spammers and malware distributors utilized various items to give their messages the appearance of legitimacy, including embedding images served from valid sites like Flickr, hiding their malware URLs in search result links, and injecting spam or malware links into transactional Hotmail content. Each of these techniques was designed to ensure that their messages pass through traditional automatic email defense filters.

In addition to these emerging techniques, several more "traditional" email fraud methods were on display throughout the quarter, including PDF attachment spam, ecard scams, and holiday- and event-based spam and malware messages.

Q1 2008 Highlights

- Spam levels ranged from 60 to 94 percent of all email throughout the quarter
- Malware distributors and spammers hid their unwanted messages within legitimate or legitimate-appearing web sites and messages
- Mortgage refinancing spam jumped to 10% of all spam in January
- Holidays continued to be celebrated in spam and malware
- On average, 355,000 zombies were newly activated each day for the purpose of malicious activity

Spammers, Fraudsters and Malware Writers Hide within Third-Party Sites and Senders

Hotmail Welcome Letters Camouflage Pharma Spam

A massive outbreak of pharmaceutical spam in January had spammers sending more than 250 million spam messages per hour during its peak. The unusual feature of this outbreak was that spammers hid their spam within the body of a legitimate Hotmail welcome message, a trick designed to make the messages appear to be legitimate to traditional content-filtering email filtering technologies, and bypass them.

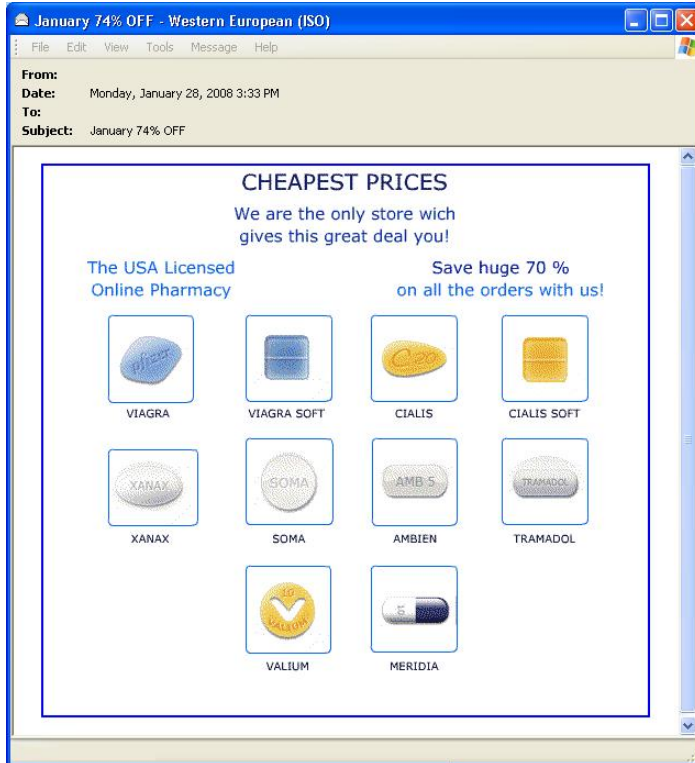
Recipients of the spam messages would see only pharmaceutical image spam. However if one views the HTML source of the message, the Hotmail content is immediately apparent.

In this outbreak, the spammers added another obfuscation trick, replacing the MSN image URLs with dozens of random web domains.



Sample Pharma Spam Message

Hidden within legitimate hotmail welcome message



More than 250 million spam messages per hour were sent during the peak of the Hotmail pharmaceutical spam outbreak

Source: Commtouch Labs

Message html source showing hotmail message content

```

: //gfx1.njtzo.com/mail/v2/ltr/welcomeletter/header-left-WL-Hotmail.jpg' width=339
ght=111 alt=""></td>
</tr>
<tr>
<td><table width="100%" border=0 cellspacing=0 cellpadding=0>
<tr>
<td><img border=0 height=1 src=
: //gfx2.rmene.com/mail/v2/ltr/welcomeletter/spacer.gif" alt="" width=16</td>
<td><font size=4 color="#0099ff">Hello and Welcome to
ms Live Hotmail<span style="font-size:10px;vertical-align:super">@</span><br>
</font>
<img border=0 height=5 src=
: //gfx2.pdjzo.com/mail/v2/ltr/welcomeletter/spacer.gif" alt="" width=1<br>
<font color="#000000">
Congratulations! The next generation of MSH® Hotmail is
ur hands - fast, simple, and safer than ever before.<br>+ Bookmark this link to
to your <a href="http://mail.kihhj.com" target="_blank">Windows Live Hotmail</a>
</font></td>
</tr>
</table></td>
</tr>
</table>
</td>
<td valign=top><img src=
: //gfx1.cnrwl.com/mail/v2/ltr/welcomeletter/header-right.jpg" width=211 height=
: /td>

```

Source: Commtouch Labs



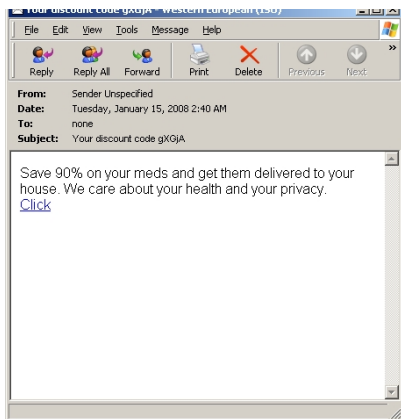
Spammers Cloak Site-links in Search Result URLs

Spam and malware have the same considerations as marketers: how to persuade their audience to respond to their call-to-action, which is typically to click on a URL. However URLs that are obviously linked to a spam site, or to a fast-flux domain, will often be filtered out before the user's inbox, so these malicious messages need new techniques to embed URLs that will not be recognized for what they are.

Embedding spam or malware URLs within legitimate URLs created from search results is one such method of hiding the true destination from the email filter.

Within the example below, the word "Click" is hyperlinked to a URL that is similar to a Yahoo! search result. (The actual spam site has been replaced with the words "SPAMMERSITE"): http://rds.yahoo.com/_ylt=3DA0geu4_1hZ9HkDIA7WdXNyoA/SIG=3D=119ei8plu/EXP=3D1201723253/*http%3a//SPAMMERSITE.com/ The link redirects to a pharmaceutical site, also shown below.

Sample message with search result URL, and the pharmaceutical site to which the URL leads



Source: Commtouch Labs

Every person who clicks on that spammer's link is routed through Yahoo's servers. It is ingenious from the spammers' perspective, since the Yahoo domain and its associated URLs are typically viewed as legitimate.

Within a legitimate search, it is not easy to swap out the target site URL with a different target URL. A simple swap of "SPAMMERSITE.com" will automatically redirect to a page that says:

This link is not authorized by Yahoo!

If you would like to continue to this link's intended destination *at your own risk*, click [here](#).

There are two methods spammers may use to implement this method successfully:



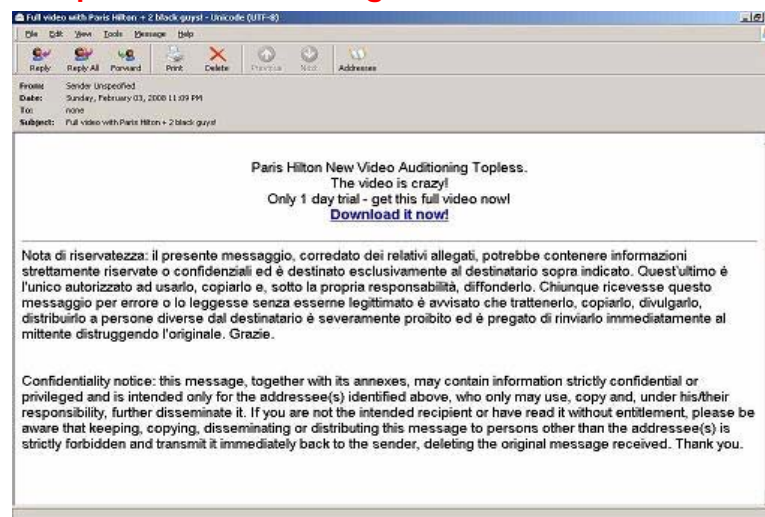
- 1) The spammers create a search in Yahoo displaying their site in the results and copy the Yahoo-generated URL from the search results. This is awkward as most of the spammer sites in this outbreak do not appear in search results, often because the sites themselves are so new. A “backward links” search for the URL in the sample message resulted in no links to that page.
- 2) Spammers may also use the Yahoo! search API to create links recognized by Yahoo, which could have far-reaching consequences for those protected by automatic spam filters depending mainly on white lists.

Google Redirects to Porn Malware Site

Yahoo! is not alone in having its legitimate code hijacked by fraudsters. In early February, pornography-focused spam email messages include a Google hyperlink, <http://www.google.com/pagead/iclk?sa=l&ai=trailhead&num=69803&adurl=http://...>

Upon arrival, the site automatically downloaded a Trojan malware called “trailer.exe.”

Sample malware message with embedded search URL



Source: Commtouch Labs



Spammer Uses Flickr to Host Spam Images

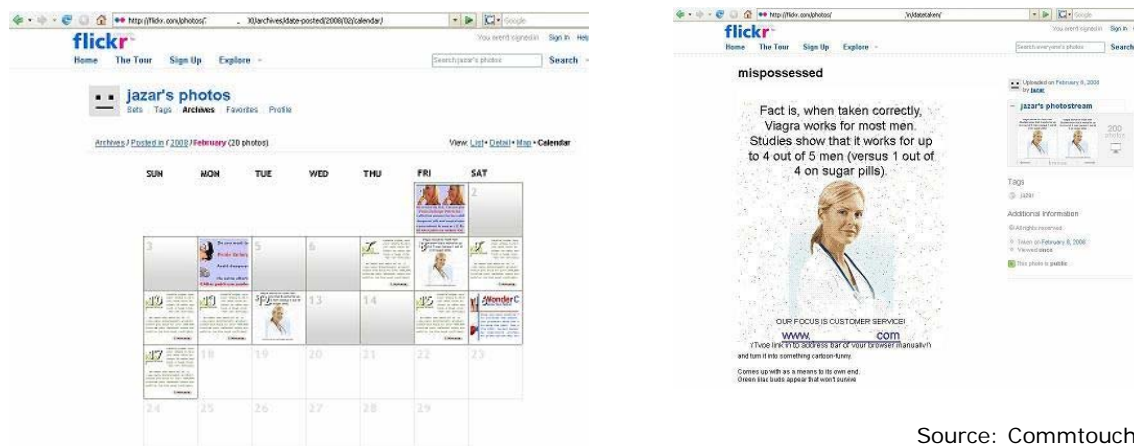
Not only are spammers generating their own legitimate-appearing links to disguise their malicious content, but they are also using legitimate sites to store their spam images. They are replacing their embedded image-based spam with image references within the HTML. Thus, the source code of the message pulls an image from a remote server when the message is opened, assuming the reader is connected to the Internet.

While images are generally stored within zombie-hosted or hacked sites, spammers also make use of Flickr and other legitimate sites to store images, ensuring the html-image references make it through automatic filtering.

Spammers take advantage of dormant Flickr sites and compromise them or simply create their own Flickr sites.

Below is an example of one spammer's Flickr account and a close-up of one of the images:

Sample Flickr account used by spammers to store images, with a close up of one of the spam images



Source: Commtouch Labs

419 Scams & Spearphishing Use Google & Yahoo! Calendar Standards

Thieves offering easy money and those seeking to defraud individuals have started using calendar-update messages generated from legitimate sites, such as Google and Yahoo!, and one such outbreak was identified during the month of March.

The calendar attachments are ICS files, a standard format for storing calendar information within a text file on the Internet. It is used in programs including iCal on the Macintosh, Microsoft Outlook 2003 and higher, the Mozilla Calendar project, Lotus Notes, and Yahoo! and Google calendars.

When opened in Outlook, the calendar-update message includes the usual "Accept" "Tentative" and "Decline" buttons, just like a regular calendar invitation.

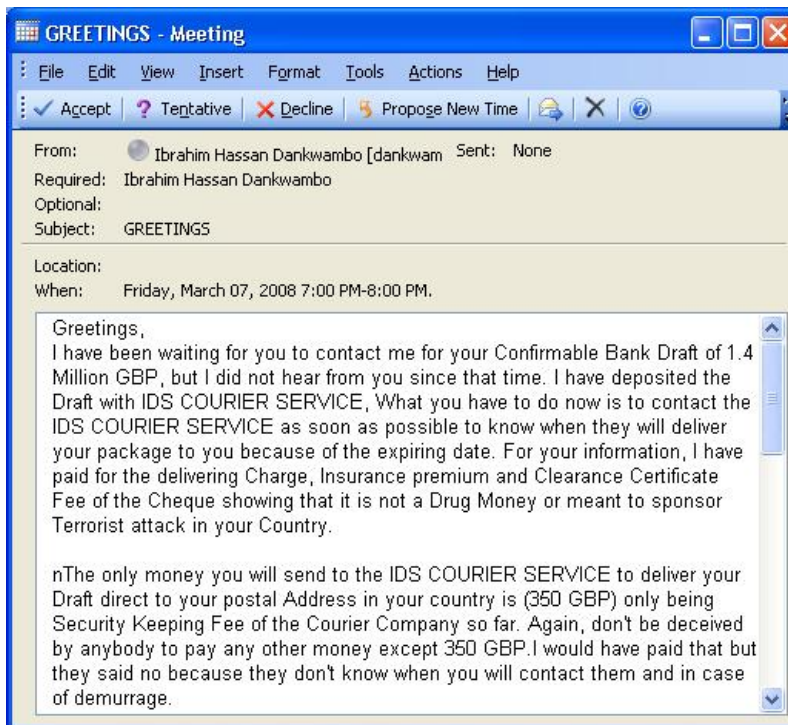


Generally, traditional anti-spam engines do not block ICS or Google or Yahoo messages because it would cause an unacceptably high level of false positives. By using ICS files and Google, Yahoo!, and other legitimate service providers, the fraudsters get extra “anti-filtering” protection.

The sample messages below are calendar messages generated from Google and Yahoo!

New Attachment Spam:

ICS Calendar attachments used by spammers



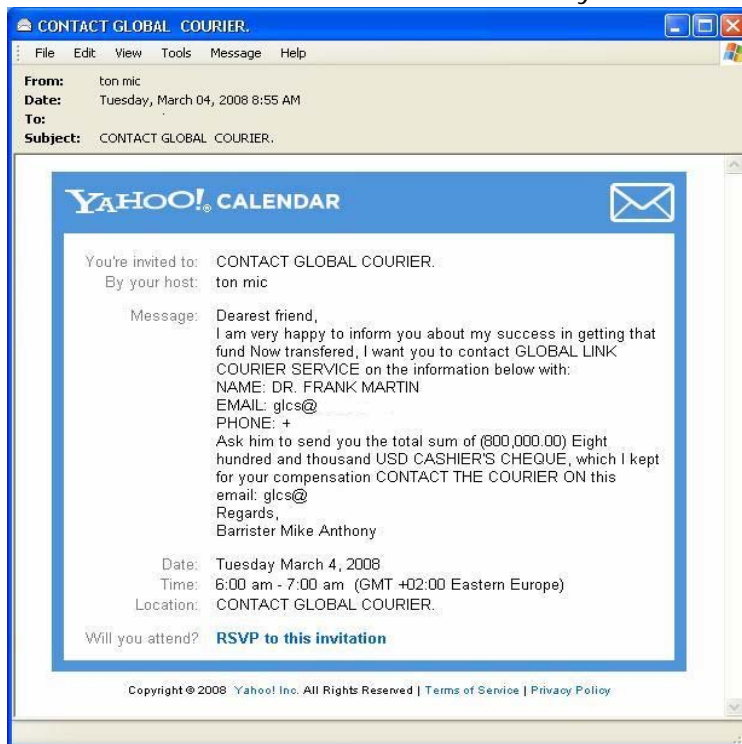
Blocking all ICS calendar messages would lead to numerous false positives

Source: Commtouch Labs



Sample Yahoo! Calendar Spam Message

ICS attachments latest mechanism used by fraudsters



Source: Commtouch Labs

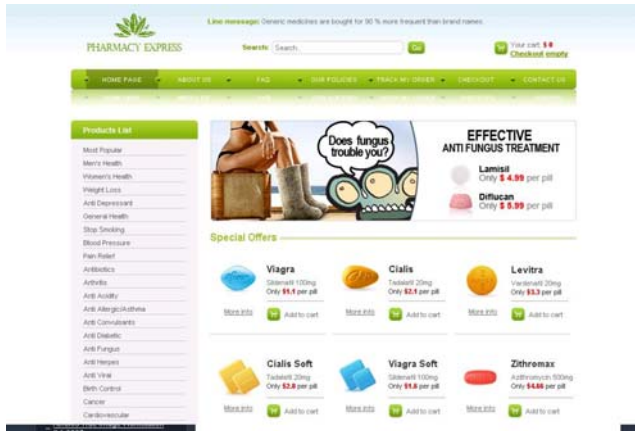
Blogspot Redirects to Malware Sites

For at least a year, Google's blogspot has been known to be a hotbed of spam activity, used by spammers to re-direct to their web sites. However in late-Q1, these popular blog sites started to redirect to sites that automatically download malware. During a three week period in March, thousands of new spam-related blogspot domains were identified each day by the Commtouch Detection Center appearing in spam messages, some directing to malware. When the user clicks the blogspot link within an email message, he or she is redirected automatically to a different site, unrelated to blogspot. Spammers use sites like blogspot to bypass traditional email filtering techniques, since it is impossible to block all blogspot addresses without creating a large number of false positives or errors.

Below are some examples of sites that were promoted by spammers through blogspot redirects in the last few weeks of the quarter.



Sample spam sites redirected to from blogspot
Blogspot used by spammers to redirect to unrelated websites



Source: Commtouch Labs

Spammers Leverage Latest News & Events

Like any news publication, spammers, malware writers, and fraudsters need to stay current to keep their message relevant and obtain top readership levels.

Mortgage Spam Jumps in Response to U.S. Federal Reserve Rate Cut

When the U.S. Federal Reserve cut interest rates in late January in response to the mortgage crisis, millions of U.S. mortgages became eligible for refinancing. Spammers immediately set out to capitalize on the new awareness of mortgages, and pumped out huge quantities of mortgage refinancing spam, which jumped to 10% of all spam. For comparison's sake, this type of spam was 2% of all spam in Q4 2007 and overall average in Q1 2008.

Mortgage spam jumped to 10% of all spam when the US Federal Reserve cut interest rates in January 2008.

The burst in mortgage spam had a flip-side: email correspondence between banks and their customers in some cases was delayed or blocked by content-filtering technologies that cannot differentiate between valid mortgage-related mail and the mortgage-related spam.

Of course, the spammers' offers may have been better than the legitimate offers. Their mortgage "specials" included:

- Save over 50% on your monthly mortgage payments by refinancing!
- 30 seconds could save you money on your mortgage
- Are you paying too much for your mortgage?
- Mortgage rates are crashing - see if your zip code qualifies
- Calculate your new mortgage payment
- Debt consolidation mortgage loan



- Debt consolidation remortgages
- Breaking mortgage news - fed drops rates to 4.50%
- Is your mortgage payment too high?
- Low mortgage rates are still available. Refinance now!
- Online mortgage loan quote

Malicious Content Preys on Human Nature

Taking advantage of the Internet's easy way to express love and friendship, malware writers sent infected ecards, Valentines and postcards.

New Storm Ecard Blended Threat

Storm is one of the most menacing malware threats active today. Its infected zombie computers enable it to easily outmaneuver real-time blacklists (RBLs) by quickly jumping among a seemingly endless network of dynamic IP addresses.

One recent Storm outbreak in March was disguised as an ecard with a horoscope header and a "funny postcard" body, inviting readers to click the link to see their own card. Clicking the link showed the image below and automatically downloaded the Nuwar (aka Storm) malware to the unsuspecting user's computer.

What makes Storm especially dangerous is that most end users are likely unaware that they have been infected – symptoms are not especially noticeable, and their computers continue to function as usual.

All the while, the Storm botmaster can use the hijacked computing power to generate and send spam and malware, host fraudulent websites and malware, and even perform DDoS attacks. This botnet is so nimble and dynamic that researchers are unable to estimate how many infected PCs it contains. Traditional IP blocking technologies such as RBLs are unable to keep pace with the dynamic activation and deactivation of the dynamic IPs.

Sample of "funny postcard" used to distribute Storm malware



Your download will start in 5 seconds.
If your download does not start, [click here](#)

©2000-2008 FunnyPostCard.com - All rights reserved.

Source: Commtouch Labs



Malware Writers Send Their Signs of Love

In mid-January, malware writers took pre-Valentine's Day advantage of people's romantic vulnerabilities by launching a love-themed blended attack generated by zombies. The very tiny messages (around 2k) had a love-oriented subject and a short love-oriented message in the body, with a link to a malware site.

The hyperlink was an IP address, not a domain name, which tends to indicate that it was a zombie-attack. The subject lines may have been just romantic enough to inspire potential victims to see what the messages contained. Upon opening the messages, the victim romantics were sent to innocent-looking sites containing malware, such as the example here.

Sample subject lines included:

- | | | |
|-----------------------|---------------------------|-----------------------|
| ■ A Dream is a Wish | ■ I Would Dream | ■ Sending You My Love |
| ■ A Is For Attitude | ■ If Loving You | ■ Sent with Love |
| ■ A Kiss So Gentle | ■ Inside My Heart | ■ Special Romance |
| ■ A Rose | ■ Love Is... | ■ Surrounded by Love |
| ■ A Rose for My Love | ■ Love Remains | ■ The Dance of Love |
| ■ A Toast My Love | ■ Magic Power Of Love | ■ The Miracle of Love |
| ■ A Token of My Love | ■ Memories of You | ■ The Mood for Love |
| ■ Come Dance with Me | ■ Miracle of Love | ■ The Moon & Stars |
| ■ Come Relax with Me | ■ My Love | ■ The Time for Love |
| ■ Dream of You | ■ Our Journey | ■ When I'm With You |
| ■ Eternal Love | ■ Our Love is Free | ■ Why I Love You |
| ■ For You...My Love | ■ Our Love is Strong | ■ Words in my Heart |
| ■ Heavenly Love | ■ Our Love Nest | ■ You're in my Soul |
| ■ Hugging My Pillow | ■ Our Love Will Last | ■ You're my Dream |
| ■ I Dream of you | ■ Pages from My Heart | ■ You're the One |
| ■ I Love Thee | ■ Path We Share | ■ You... In My Dreams |
| ■ I Love You Because | ■ Sending You All My Love | |
| ■ I Love You Soo Much | | |

Zombies generate love attack in time for Valentines Day



Your download should begin shortly. If your download does not start in 10-20 seconds, you can [click here](#) to launch the download and then press Run. **Enjoy!**

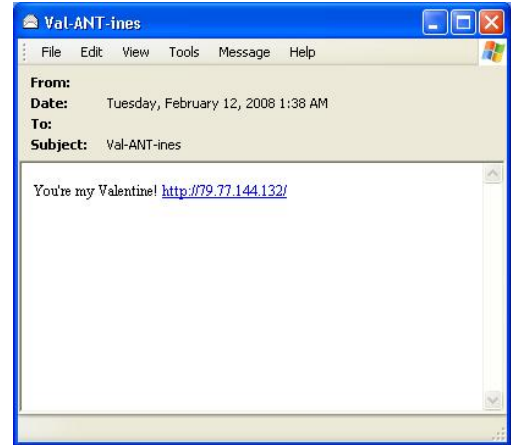
Source: Commtouch Labs

Artistic Valentines Featured in Malware Attack

As malware writers hone their expertise, they are increasing their focus on the packaging. Their Valentine’s Day malware email messages delivered in the few days leading up to the February 14 holiday featured simple text - a short message like “You’re my Valentine” or “A Hearty Wish” and a hyperlink to a specific IP address. The hyperlink went to a minimalist web page featuring intricate Valentine’s Day artwork.

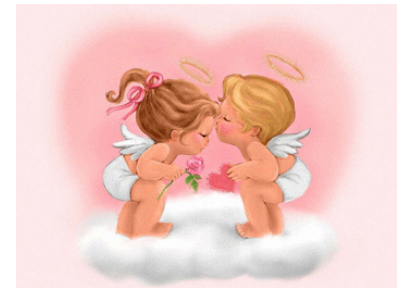
While the visitors admire the art, the site tries to automatically download a malware executable, valentine.exe. At the time of this outbreak, several standard, commercial AV engines were not yet detecting, let alone blocking, this particular code.

Sample of simple Valentines Day spam messages



Source: Commtouch Labs

Samples of Valentines Day artwork used to distract users while they unknowingly download malicious executable files



Source: Commtouch Labs



April Fools' Malware Messages Cap Off the Quarter

Similar to the holiday and ecard messages throughout the quarter, malware distributors took advantage of the atmosphere of April Fools' Day to send "jokes" linking to malware sites. The messages were short text messages, with a hyperlink to a web site hosted at an IP address (usually indicative of a zombie outbreak).

Subject lines included:

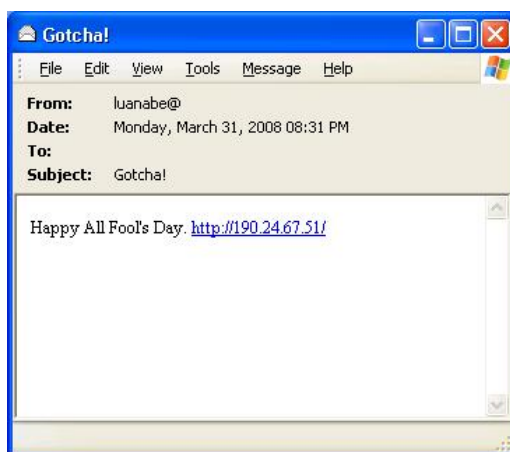
- All Fools' Day
- April Fools' Day
- Doh! All's Fool.
- Doh! April's Fool.
- Gotcha!
- Gotcha! All Fool!
- Gotcha! April Fool!
- Happy All Fools!
- Happy April Fools!
- Happy Fools Day!
- Surprise!
- Today's Joke!

At quarter's end, spammers unleashed a massive April Fools' outbreak with hundreds of different URLs associated with the outbreak each hour.

This outbreak began the day before April Fools', on March 31, and has been massive. The Commtouch Detection Center identified hundreds of new web links associated with the attack each hour.

The hyperlinks in the email linked to a web site that is similar to the earlier holiday greetings, both in terms of its appearance, and the fact that it attempts to automatically download malware.

Sample April Fools' Blended Threat Message and the site to which the message links



Your download will start in 5 seconds.
If your download does not start,
[click here](#) and then press "Run".

Source: Commtouch Labs

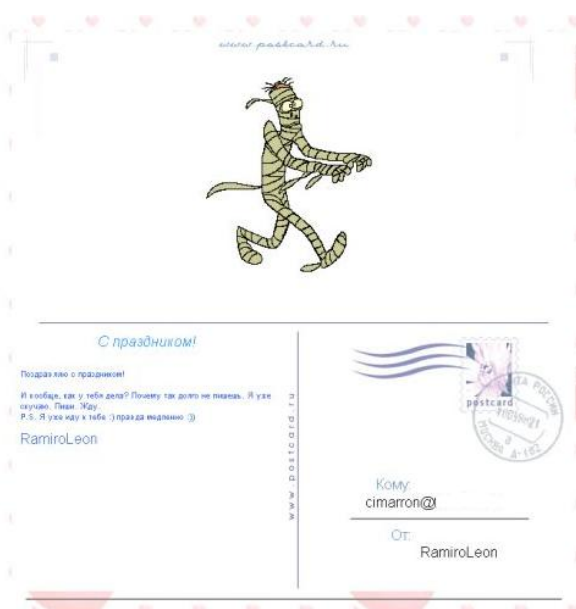
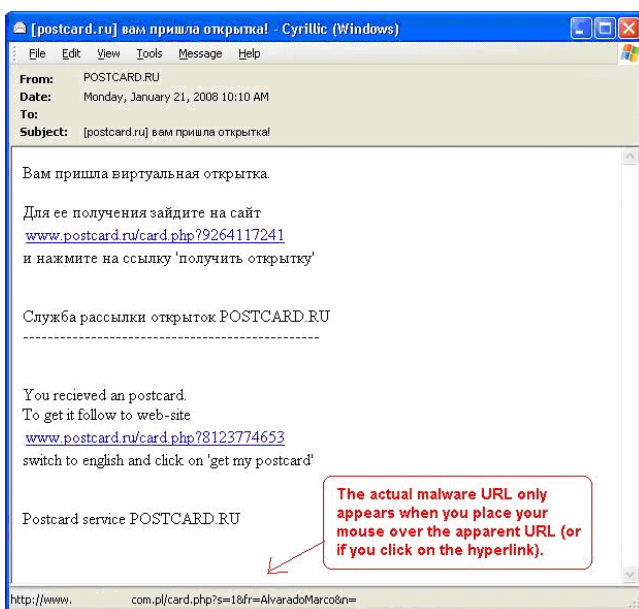


Malware Writers Leverage Multilingual Greetings

Malware writers believe in equal-opportunity fraud, as they attempt to infect people from all countries and language groups. One of the scams this quarter is a blended threat using emails in Russian and English, pretending to be a postcard from the popular site postcard.ru. The malware postcard does not look significantly different from postcard.ru's legitimate plain-text announcement. Mousing over the link to the postcard within the message reveals the malware URL.

The scam email links to a malware site that tries to download an .exe file to the user's computer. The fraudsters have made the extra effort to make the malware site look like a postcard, with the added "bonus" of an automatic download.

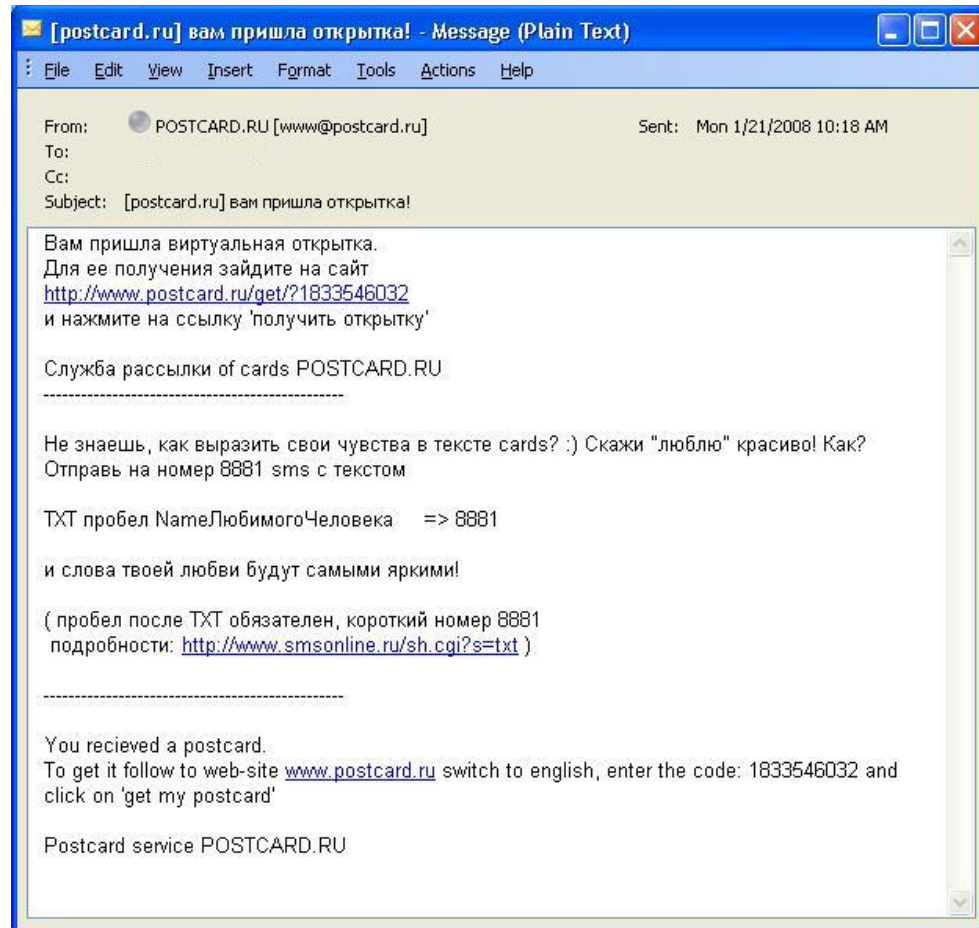
Sample messages based on postcard.ru with hidden links to malware sites; and the site to which the message links



Source: Commtouch Labs

Meanwhile, this is how a legitimate email from postcard.ru should appear:

Sample legitimate postcard.ru email message

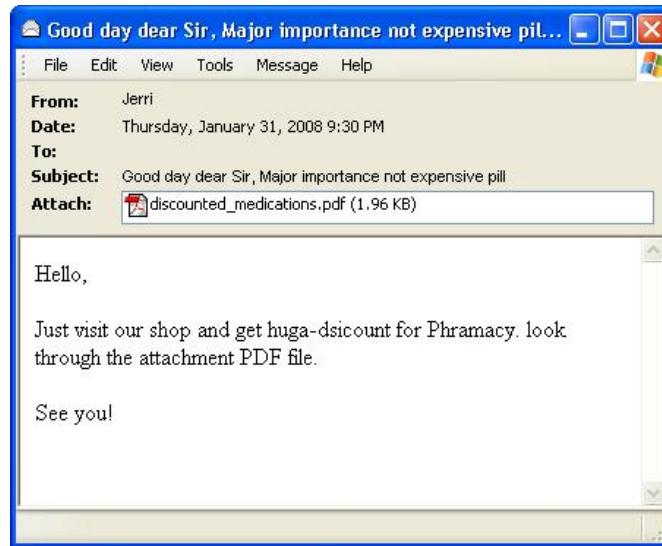


Source: Commtouch Labs

PDF Spam Continues, Slowly & Steadily

While PDF spam is no longer being sent at the high levels of 2007, it is still a steady presence. And its designers are still trying to get around Bayesian filters by adding Bayesian “poisoning text” at the bottom of the PDF.

PDF spam still exists, now with poisoned footnotes

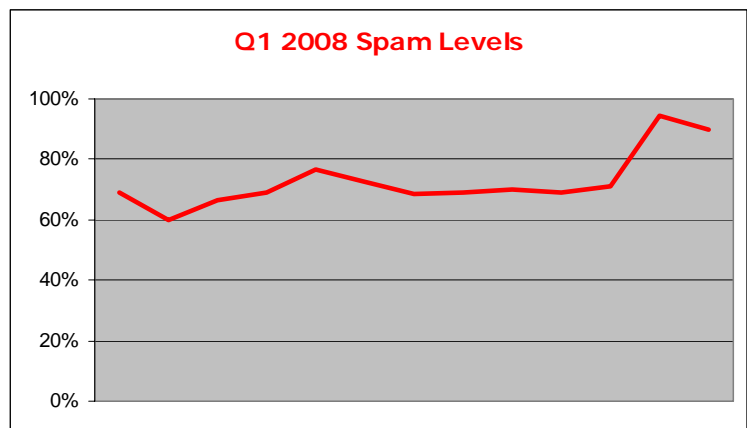


Source: Commtouch Labs

Spam and Zombie Levels

Spam levels during the quarter ranged between 60 and 94 percent of all email throughout the quarter.

Sexual enhancers remained the top topic of spam for the quarter, however decreased from Q4 2007's high of 70%, down to just 30% of spam messages in the first quarter.



Source: Commtouch Labs

NOTE: Reported global spam levels are the ratio of Internet email traffic as measured from unfiltered data streams, not including internal corporate traffic. Therefore global spam levels will differ from the quantities reaching end user inboxes, due to several possible layers of filtering at the ISP level.



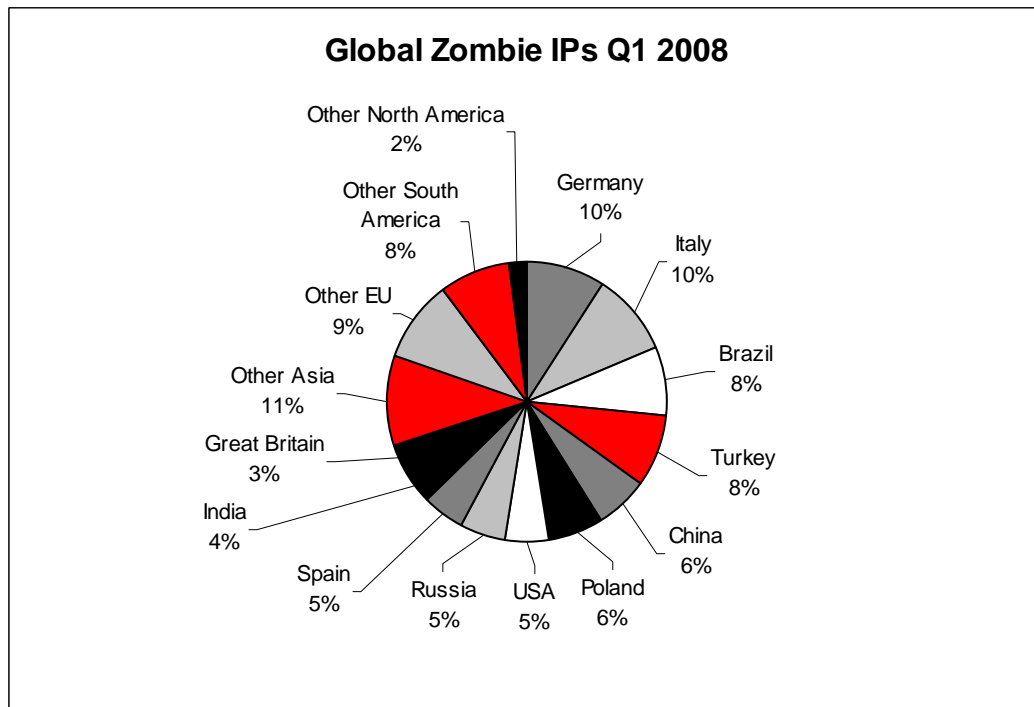
Topics of Spam Email

Sexual Enhancers 30%	Pornography 3%
Pharmacy 22%	Loans/ Mortgage 2%
Replicas 21%	Gambling 2%
Academic Degrees 5%	Other 13%
Software 3%	

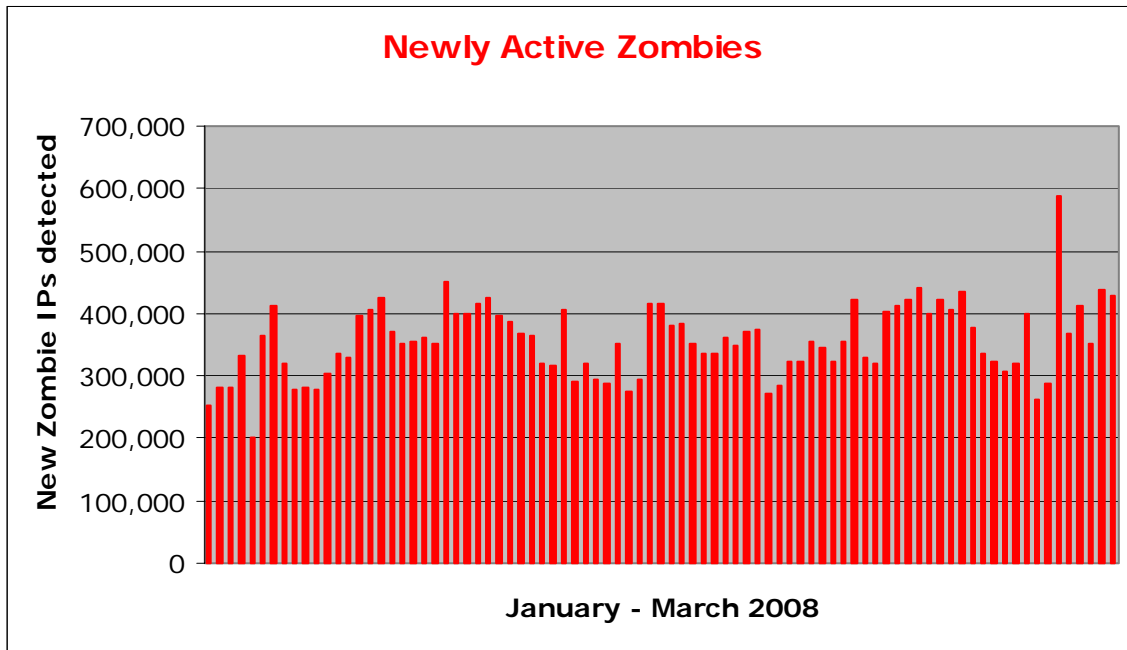
Source: Commtouch Labs

Newly active zombies averaged 355,000 per day, and were spread all over the globe.

Global Zombie IPs Q1 2008

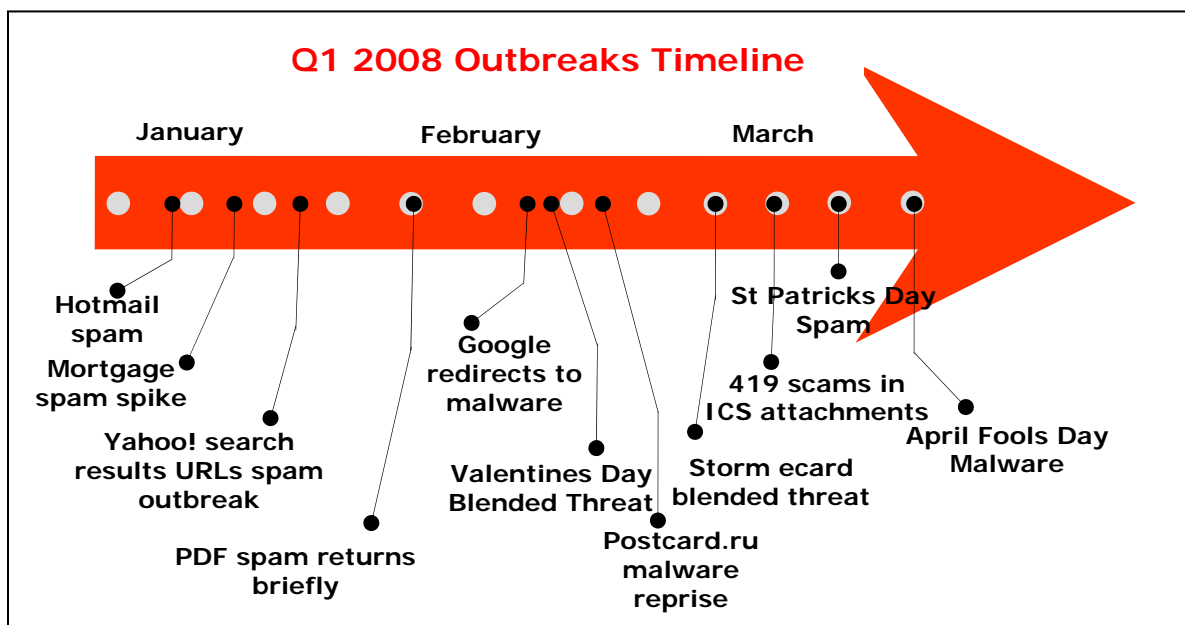


Source: Commtouch Labs



Source: Commtouch Labs

Q1 2008 Outbreaks in Review



Source: Commtouch Labs



About Commtouch

Commtouch® (NASDAQ: CTCH) is the source of proven messaging and web security technology for scores of security companies and service providers, enabling them to mitigate Internet threats and allowing them to focus on their business. Proven expertise in building efficient, massive-scale security services has resulted in Commtouch's unmatched suite of offerings that automatically process, learn and improve over time.

Stay abreast of the latest trends all quarter long, at the Commtouch Café:
blog.commtouch.com

The key services – Anti-Spam, Zero-Hour™ Virus Outbreak Protection, GlobalView™ Mail Reputation Services and GlobalView™ Zombie Intelligence – all provide information for each other in a comprehensive, self-learning feedback loop that learns locally as well as globally. Relying on Commtouch allows the company's licensing partners the freedom to focus on their own areas of expertise, secure in the knowledge that Commtouch is always well ahead of the latest email and web threats.

Commtouch's patented Recurrent Pattern Detection™ technology automatically analyzes billions of transactions weekly to identify new spam, malware and zombie outbreaks as they are initiated. Because RPD™ technology does not rely on any content-filters, it is equally effective for all languages and formats; it can identify outbreaks of any content- or attachment-type, and is highly effective at blocking spam in double-byte languages.

For more information about enhancing security offerings with Commtouch technology, see www.commtouch.com or write nospam@commtouch.com.

About Panda Security

Panda Security is one of the world's leading IT security providers, with millions of clients across more than 200 countries and products available in 23 languages.

Its mission is to develop and provide global solutions to keep clients' IT resources free from the damage inflicted by viruses and other computer threats, at the lowest possible total cost of ownership.

Panda Security proposes a new security model, designed to offer a robust solution to the latest cyber-crime techniques. This is manifest in the performance of the company's technology and products, with detection ratios well above average market standards and most importantly, providing greater security for its clients.

For more information and evaluation versions of all Panda Security solutions, visit our website at: <http://www.pandasecurity.com>

For more information: communication@pandasecurity.com

Tel. +34 91 806 37 00

© Copyright 2008 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.