

Internet Threats Trend Report Q1 2010



In This Report

- SpamAssassin Y2K10 Bug:** SpamAssassin users started the quarter and the new decade with numerous false positives due to a bug in the open source software **Page 1**
- Analyzing Spam Templates:** We observe some of the techniques used by spammers and review new research published this quarter **Page 1**
- CNN redirect used by scammers:** An ad-serving HTML tag was exploited, directing unsuspecting users to a work-from-home scam **Page 4**
- Service Providers must deal with Zombies:** A proposed Internet Industry code of conduct raises the issue of outbound spam **Page 5**
- How much spam comes from gmail.com?** - The Gmail domain is the most abused by spammers who fake the "from" field in spam emails - but real Gmail accounts are also being used to send spam **Page 6**
- How phishers get free Web hosting:** A look at the Web categories most likely to be hosting a hidden phishing page **Page 8**
- Delivery invoices and etickets:** An analysis of the most common subjects used in emails carrying malware as well as common malware functionality **Page 10**

Q1 2010 Highlights

▲ 183 billion

Average daily spam/phishing emails sent
Page 6

▼ 305,000 Zombies

Daily turnover
Page 11

▲ Entertainment

Most popular blog topic on user generated content sites
Page 9

▼ 838 variants

Of Mal/Bredo malware emailed
Page 10

▲ Pharmacy ads

Most popular spam topic (81% of spam)
Page 6

▼ Brazil

Country with the most Zombies (14% of world's zombies)
Page 11

▲ Pornography

Website category most likely to be compromised with malware
Page 8

SpamAssassin Y2K10 Bug Causes False Positives Worldwide

A glitch in the most widely-used free Anti-Spam software – SpamAssassin – at the beginning of 2010 resulted in false positives and rejection of legitimate mail. SpamAssassin is widely used by xSPs, organizations, universities, and also vendors who integrate it into their own detection engines.

Each rule within SpamAssassin's engine searches for specific characteristics within an email and provides a score. The combined scores provide a spam probability rating. The bug was caused by a specific rule which checked to see if a message was sent from the future, which could be an indicator of a compromised computer. The buggy parameter in the rule, clearly created many years ago, stated that messages from 2010 were "from the far future," inappropriately adding an additional 3.2 points to each message, significantly increasing the message combined score, and thus raising the false positive ratio by as much as 20%.

The contributors fixed the problem at noon on January 1, 2010 but administrators were required to perform updates in order for the fix to take effect. The fix updated the rule to give mail received after 2020 the additional 3.2 points.



The Apache SpamAssassin Project
The Powerful #1 Open-Source Spam Filter

[SpamAssassin Home](#) | [Home](#) | [News](#) | [Wiki](#) | [Download](#) | [FAQ](#) | [Docs](#) | [Lists](#) | [Tests](#) | [Bugs](#) | [Credits](#)

2010-01-01: Y2K10 Rule Bug - Update Your Rules Now!

Versions of the **FH_DATE_PAST_20XX** rule released with versions of Apache SpamAssassin 3.2.0 thru 3.2.5 will trigger on most mail with a Date header that includes the year 2010 or later. The rule will add a score of up to 3.6 towards the spam classification of all email. You should take corrective action immediately; there are two easy ways to correct the problem:

- If your system is configured to use **sa-update** run **sa-update now**. An update is available that will correct the rule. No further action is necessary (other than restarting spamd or any service that uses SpamAssassin directly).
- Add "score FH_DATE_PAST_20XX 0" without the quotes to the end of your local.cf file to disable the rule.

If you require help updating your rules to correct this issue you are encouraged to ask for assistance on the Apache SpamAssassin Users' list. [Users' mailing list info is here](#).

On behalf of the Apache SpamAssassin project I apologize for this error and the grief it may have caused you.

Regards,

Daryl C. W. O'Shea

VP, Apache SpamAssassin

Source: Commtouch

Analyzing Spam Templates

Spammers and phishers continued to show creativity throughout the quarter in their attempts to create emails that lure recipients into clicking on the embedded links. The quarter also saw publication of new research into methods for determining the spam or phishing templates used.

Spam template research

An article in the January issue of *The New Scientist*, published in January, entitled "To beat spam, turn its own weapons against it," describes the work done by a team of academics to find a more effective way to filter spam. The team, from ICSI Berkeley and UC San Diego, has come up with a way of analyzing the spam email messages sent by a 'captured' zombie PC. After watching the zombie's spam outpourings for about 10 minutes, they managed to reconstruct the underlying template used to create the numerous variations of a particular spam message. This allowed them to successfully instruct spam filters to watch out for messages that match the template.

A similar pattern identification concept is part of Commtouch's patented Recurrent Pattern Detection process. The particular approach proposed by the academics would require several improvements that already exist in the Commtouch solution:

- The 10 minute period to derive the template would in practice allow a botnet to deliver millions of spam messages before detection – detection is required within seconds.
- Analysis of a few zombies would not be enough. A widely distributed system of millions of nodes all around the Internet is required in order to quickly capture sufficient breadth of data, all of which would need to be efficiently and quickly processed to create spam signatures for filters to match against. This would also resolve the issue of templates that change very frequently.

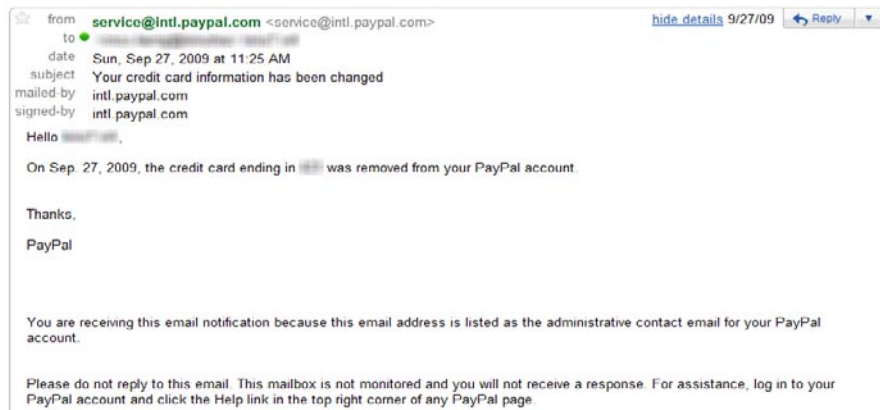
Better phishing templates target Blogger/Google users

In February a phishing attack directed at Blogger and Google users was based on a template which used two techniques that effectively downplayed the “phishy” nature of the email. The received emails cloned the following sample:



Source: Commtouch

1. The very bare text style is similar to the kind of email that a reputable service would actually use. Phishing-aware services such as PayPal, Facebook, and Blogger tend to use text-only emails with no links or images when contacting account owners – since anti-spam engines may remove hyperlinks and images on received messages. This is a real message recently received from PayPal (note that it contains only text and no images):



Source: Commtouch

2. The link is “fully displayed”. Phishing-aware users have learned to mouse-over underlined text (“click here”) or simple domain names in order to see

Q1 2010 Internet Threats Trend Report

the full URL. The “exposed” complex URL in the phishing email above gives the impression that mousing-over is unnecessary. The link naturally hides one of many URLs that look something like:

blogger.com.erdca.or.kr/update/VE.php?c=9883246018300591978521084101021546437&email=user@place.com&service=blogger

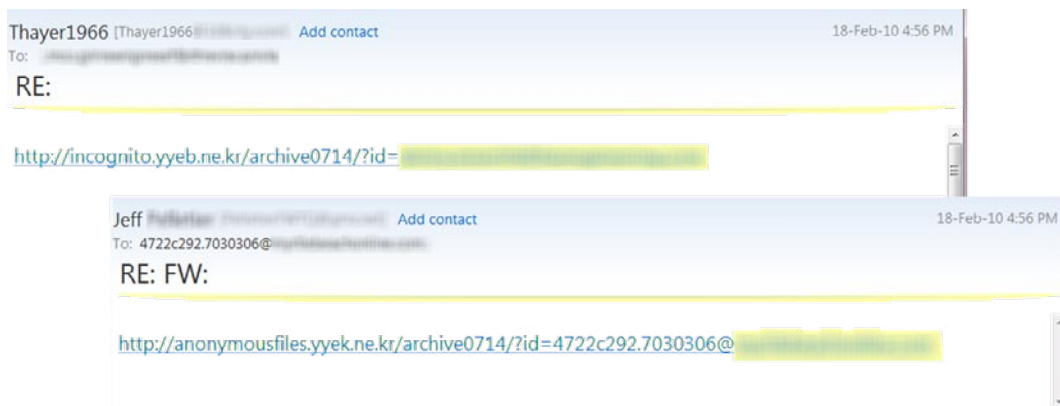
Clicking on the link reached a reasonably well-copied Blogger/Google password entry page. Unsuspecting users entering their correct account data would have compromised their Blogger or Gmail accounts. See page 5 for Commtouch’s analysis of spam emanating from compromised Gmail accounts.



Source: Commtouch

The “curious recipient” template

A more spartan template was employed in another outbreak that took place in February. The emails (samples below) have no subject (other than RE: or FW:), no text telling recipients why they should click on the link, no URLs hidden behind on-screen hyperlinks, and no images. It would seem that the social engineering concept relies on curious users who will click on the link “because it’s there.” In this case the links lead to sites requiring “the latest version of Macromedia Flash Player.” Simply visiting the site or installing the “update” starts a process of compromising the recipient’s computer, making it part of a botnet.



Source: Commtouch

CNN redirect exploited by scammers

A spam outbreak at the beginning of March featured familiar promises of work-from-home riches. The subjects were typically bold and the emails featured short one-liners and single links offering more information.



The links lead to a "career digest" as shown below.

Source: Commtouch

The links in the email exploit the redirect functionality supported by CNN's ad servers. The links are structured as follows:

<http://ads.cnn.com/event.ng/Type=click&Redirect=http://bit.ly/cP--XW>

Clicking on the link sends a request to CNN which instructs the browser to send a second request to the redirect URL – in this case the shortened <http://bit.ly/cP--XW>. The host site would not be aware of the misuse – the spammer is simply abusing legitimate ad-serving functionality.

Source: Commtouch

This technique provides several advantages to the spammer:

1. The URL from cnn.com might give the impression that there was a genuine CNN-worthy story to be found
2. The reputable site name would allay fears of anything malicious lurking at the end of the click
3. Most URL filtering solutions would not block the initial request to cnn.com (although reputable solutions would have been updated in real time about the follow on link which would be blocked)

In addition, the shortened bit.ly URL further obfuscates the final destination (the newspaper shown above). All 24 links on the page point users in the direction of a recognized "Auction Listing Agent" scam. Since the outbreak began the links' destination alternated (depending on the day and week) to a download page for a toolbar which is advertised as avatar creation software, but includes a search tool which is generally regarded as spyware.

Proposed code of conduct targets zombies

The Australian and *ZDNet* both reported this quarter about a new initiative of the Internet Industry Association (IIA)- whose members include major internet service providers Optus, Telstra, Vodafone, AAPT, Virgin and Hutchison 3G, as well as industry giants Facebook, Google and Microsoft – to prepare a new industry code of conduct that will come into force this year.

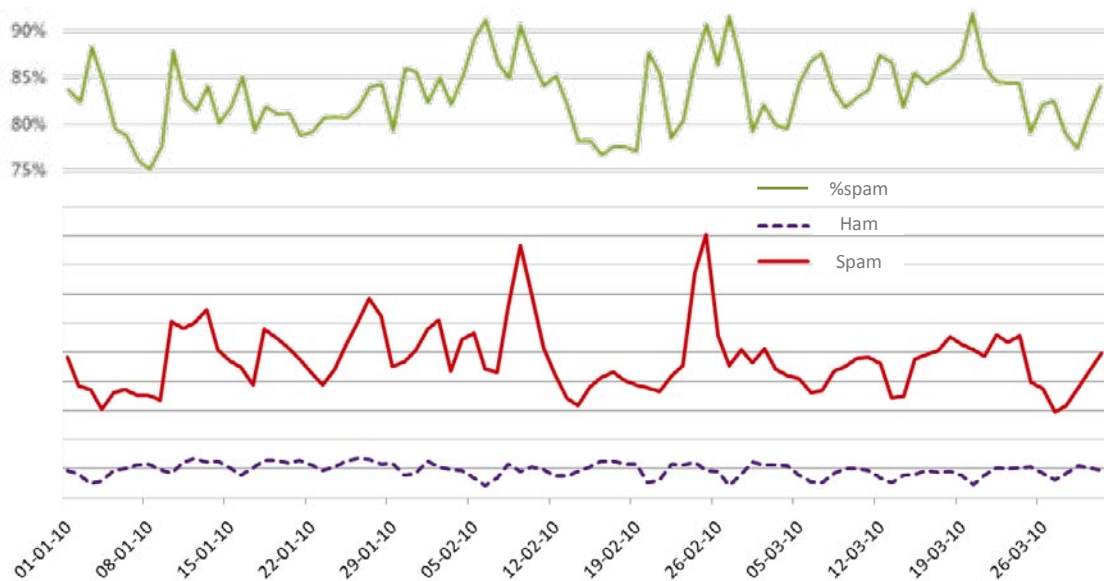
The code will require service providers to deal with zombie computers within their networks that are responsible for outgoing spam, virus and phishing attacks. Service providers will have to identify and then notify the users of compromised computers. They could also place the users in a quarantined or walled garden status until the malware is removed from their PCs.

The code is being pushed by the Australian federal Department of Broadband, Communications and the Digital Economy. The department has told a parliamentary inquiry into cyber-crime that the voluntary code is faster than introducing legislation.

"We've always said that if this does not work then government will have to consider firmer options" said Keith Besgrove, the first assistant secretary of the digital economy services division. "This is damn dangerous and we've got to do something about it."

Spam Trends

Spam levels averaged 83% of all email traffic throughout the quarter, peaking at nearly 92% near the end of March and bottoming out at 75% at the start of the year. Assuming worldwide email traffic of around 220 billion emails per day this would equate to an average of around 183 billion spam messages per day.



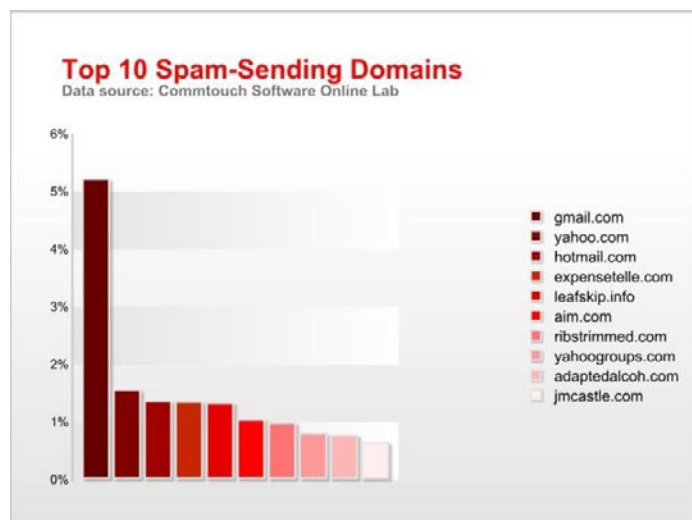
Source: Commtouch

NOTE: Reported global spam levels are based on 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.

Spam from gmail.com?

As part of Commtouch's analysis of spam trends Commtouch Labs monitors the domains that are used by spammers in the "from" field of the spam emails. Naturally the addresses are typically faked in order to fool anti-spam systems and to give the impression of a reputable, genuine source. Occasionally spammers will use a company name, for example, UPS – particularly when sending malware disguised as "UPS delivery information" (see Malware Trends on page 10). The domain that is most often faked however is gmail.com.

This quarter Commtouch Labs asked the question – How much spam from gmail.com actually emanates from real Gmail accounts and how much is faked. The analysis was based on the following methodology:



Q1 2010 Internet Threats Trend Report

1. Get a list of the IP addresses authorized to send mail from gmail.com (using SPF)
2. Examine the from fields for gmail.com senders as well as the actual source IP addresses from a representative sample of Q1 traffic
3. Divide the emails into those actually sent from Gmail accounts (which match the IP addresses from step 1) and the remainder from faked Gmail senders
4. Divide these emails into legitimate and spam
5. Compare the percentage of spam coming from the genuine and faked accounts

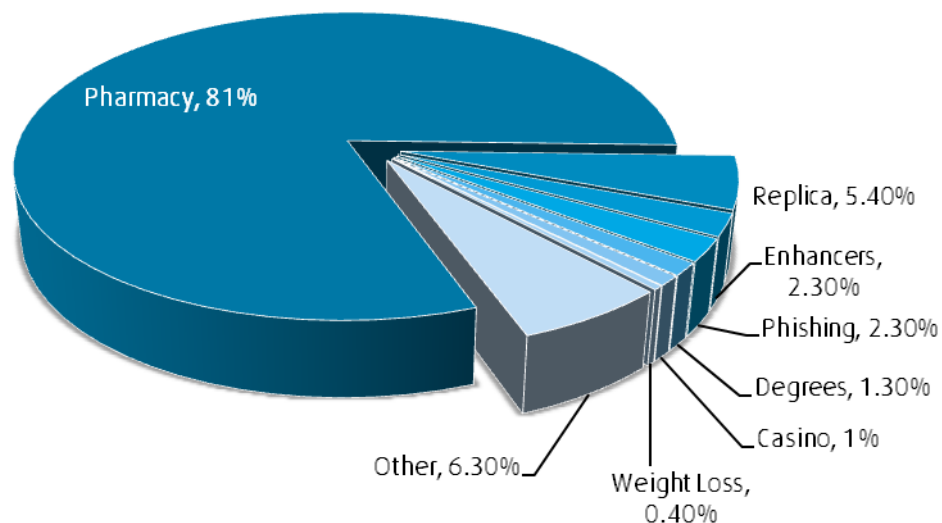
The results for all emails in the analysis period from gmail.com are presented below.

- % of genuine Gmail senders 59%
- % of fake Gmail senders 41%
- % of emails classified as spam 42%
- % of spam emails sent by genuine Gmail accounts 1%

As shown, 1% of spam “from” gmail.com is actually from gmail.com. This small percentage is likely to represent a mix of spammers and compromised Gmail accounts. On page 2 of this report we describe a phishing outbreak aimed at obtaining the credentials of Gmail users.

Spam Topics

Pharmacy spam remained in the top spot with 81% of all spam messages; slightly increased from last quarter. Replicas remained in the #2 spot, with 5.4%.



Source: Commtouch

Compromised Web Sites

During the first quarter of 2010, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware or phishing. As expected and in line with the last several quarters, pornographic and sexually explicit sites ranked highest in the categories infected with malware.

On the list of Web categories likely to be hosting hidden phishing pages, sites related to sex education ranked highest. These are followed by socially oriented sites such as games, chat and social networking which are easier targets for posting hidden phishing pages.

Categories infected with Malware	
Rank	Category
1	Pornography/Sexually Explicit
2	Business
3	Computers & Technology
4	Forums & Newsgroups
5	Education
6	Health & Medicine
7	Transportation
8	Travel
9	Streaming Media & Downloads
10	Finance

Categories infected with phishing	
Rank	Category
1	Sex Education
2	Games
3	Chat
4	Social Networking
5	Health & Medicine
6	Personal sites
7	Education
8	Real Estate
9	Computers & Technology
10	Business

Source: Commtouch

The sites infected with phishing are generally not changed in any obvious way. The phishing page is added by a hacker and the link to the page is then inserted into phishing emails. A PayPal phishing link might look like this:

<http://infected-site.com/paypal.com/ndex.php>

Phishers gain several advantages from this ploy:

- The legitimate site name lends legitimacy to the link
- The phishing page is hosted for free
- It usually takes several days or more to detect and remove the page

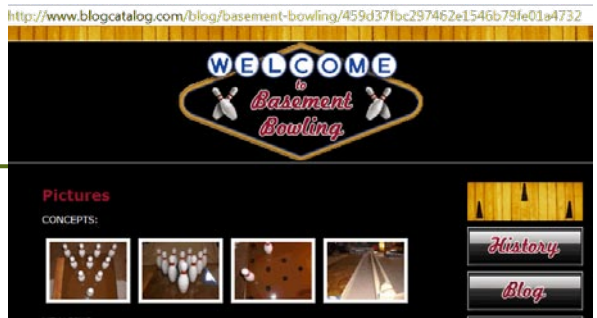
Web 2.0 Trends

In an analysis of nine of the most popular user generated content sites, entertainment continued to be the most popular blog or page topic, covering 13% of the generated content. Following closely behind were shopping (12%) streaming media and downloads (10%), computers and technology (7%) and pornography and sexually explicit content (6%). 4% of blog pages analyzed have been adopted by spammers as the destinations for their pharmaceutical or replica campaigns.

Entertainment blogs typically cover television, movies, and music as well as hosting celebrity fan sites and entertainment news. The streaming media & downloads category includes blogs with streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Examples of these and other categories are depicted below.

Rank	Category	Percentage
1	Entertainment	13%
2	Shopping	12%
3	Streaming Media & Downloads	10%
4	Computers & Technology	7%
5	Pornography/Sexually Explicit	6%
6	Arts	5%
7	Spam Sites	4%
8	Education	4%
9	Sports	4%
10	Religion	3%
11	Health & Medicine	3%
12	Leisure & Recreation	3%
13	Finance	2%
14	Travel	2%
15	Politics	2%

Source: Commtouch



Malware Trends

The names of the most widely distributed malwares during the quarter are shown in the figure opposite (larger size indicates higher distribution).

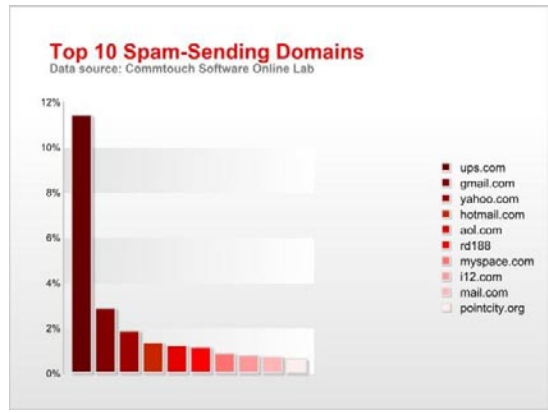


The functionality of the most distributed malware falls into one or both of the following categories:

1. Rogue security software that deceives or misleads users into paying for the fake or simulated removal of malware
2. Downloader malware that contacts a remote host to download and install additional malware – most commonly botnet related

Source: Commtouch

The attached files are mostly zipped executables. The most common email subjects for the distributed malware relate to mail or courier delivery invoices as well as travel “etickets”. During one of these outbreaks the ups.com domain surpassed gmail.com as the most faked domain used in mass-distributed emails. This is shown in the graph on the right.



The Mal/Bredo malware that has featured prominently in the last two quarters was distributed in far fewer numbers but had by far the most variants – totaling 838 for the quarter. The next most variants were of Mal/ZipMal which was emailed in 446 different varieties.

Detection time of major AV vendors

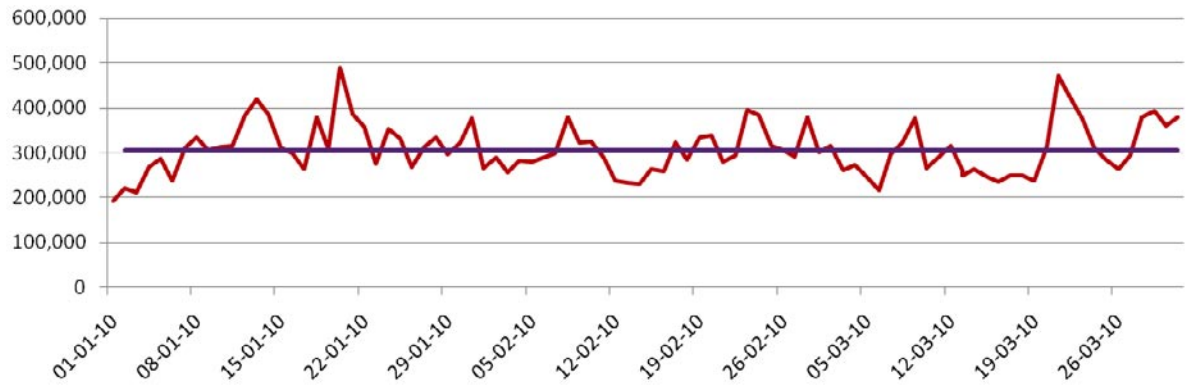
The table below compares the average detection times (in hours) of leading AV vendors for all variants of the five leading viruses of the quarter. These figures were calculated using AV engine detection times as reported by AV-Test.org compared to the zero-hour detection time of Commtouch. “No detection” indicates that the AV engine did not release a signature by the time the report from AV-Test was tallied; however it is possible that the AV engine released a signature after that time.

Top 5 malware	Symantec	Kaspersky	Trend Micro	Microsoft	CA
Mal/FakeAV-BW	11.98	21.4	20.48	30.88	29
Mal/FakeAV-BT	9.64	7.4	12.47	23.68	24.28
Mal/EncPk-NP	7.53	9.37	11.12	23.68	No Detection
Mal/EncPk-MP	23.49	6.87	No Detection	No Detection	59.27
Mal/EncPk-NS	11.98	23.36	15.3	13.95	12.74
Average	12.92	13.68	14.84	23.05	31.32

Source: Commtouch

Newly Active Zombies

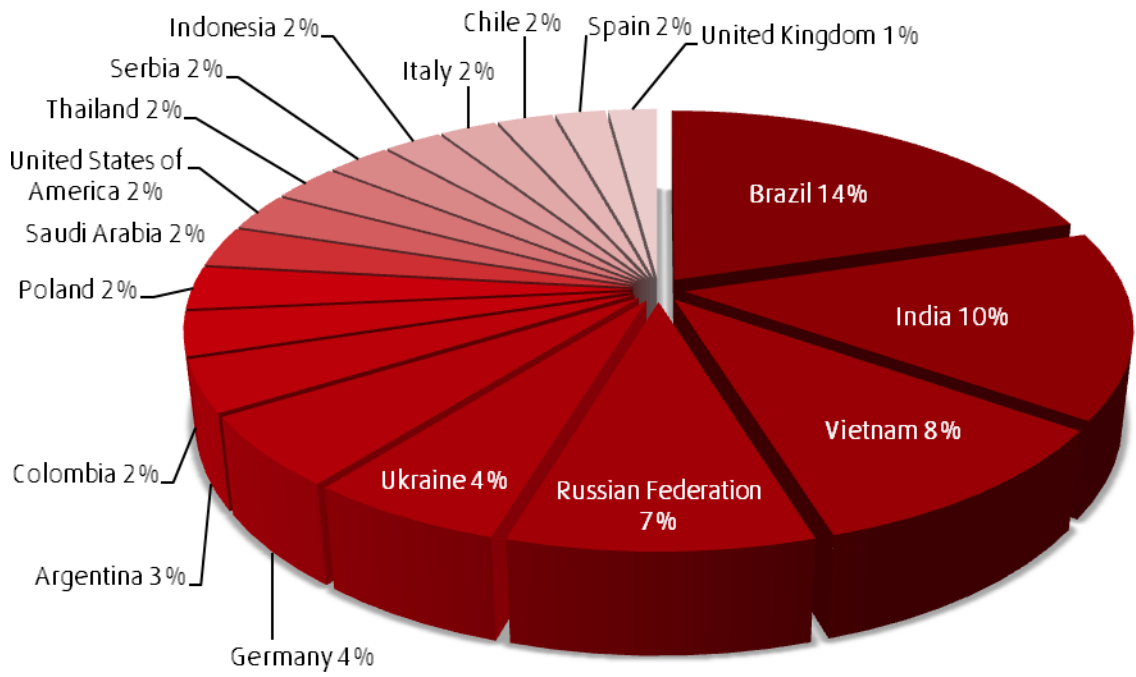
The lifespan of zombies is very short, and according to Commtouch Labs, the first quarter saw an average turnover of 305,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. This number is slightly lower than the 312,000 of Q4 2009. The graph below shows the newly active zombies each day throughout the quarter.



Source: Commtouch

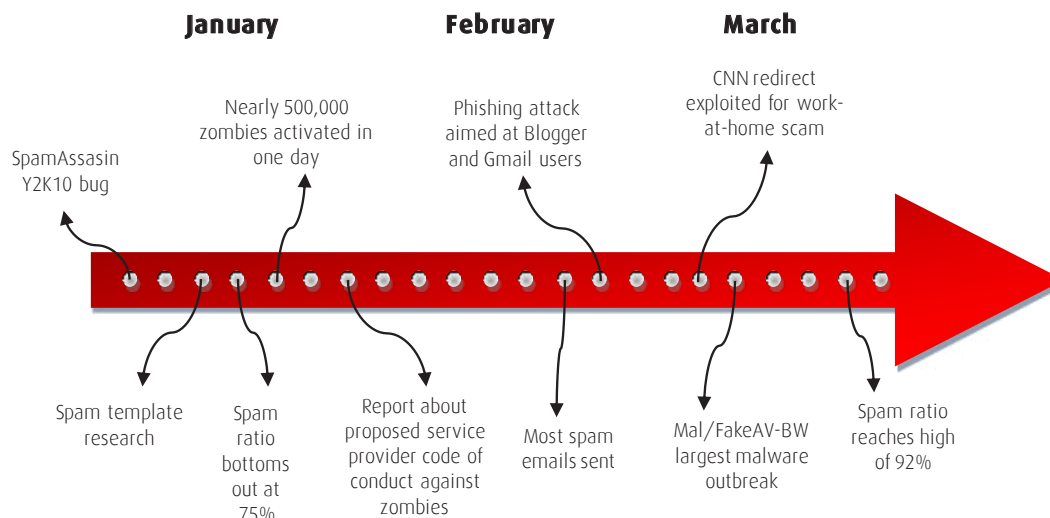
Zombie Hot Spots

Brazil continued to produce the most zombies but dropped from 20% last quarter to 14% this quarter.



Source: Commtouch

Q1 2010 in Review



Top 10 Most Ridiculous Spam Subjects

As a messaging and Web security company, Commtouch sees a fair share of spam while helping its customers get rid of theirs. Below is a collection of some of the most amusing spam subjects with a little bit of commentary from Commtouch Labs.

10. "Our watch will look great even on any loser" // Way to be blunt
9. "Jewelry, watches-the main things that show the man's significance" // Not according to the other spam I get
8. "Do your friends make you fat?" // Um...that's a better excuse than the cookies & the burger I just ate
7. "I want sale you rolex.. do yu want? 27" // Well, when you put it so eloquently...I'd like...27!
6. "You dont believe in ghosts" // But I *do* believe in spammers
5. "Out of my mind" // ...and into our spam folders!
4. "James bond prefers Swiss watches // We doubt he buys them from you
3. "Bed fail won't occur" // Don't you hate it when your bed fails?
2. "Vote for Mccane on our site" // It's a little too late for that
1. "Bash this site" // Don't tempt me..

Follow Commtouch on Twitter at <http://www.twitter.com/commtouch> for new silly spam subjects (search for #sillyspam) plus industry news, important company announcements and more.

About Commtouch

Commtouch® (NASDAQ: CTCH) provides proven messaging and Web security technology to more than 130 security companies and service providers for integration into their solutions. Commtouch's GlobalView™ and patented Recurrent Pattern Detection™ (RPD™) technologies are founded on a unique cloud-based approach, and work together in a comprehensive feedback loop to protect effectively in all languages and formats. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures and enabling safe, compliant browsing. The company's expertise in building efficient, massive-scale security services has resulted in mitigating Internet threats for thousands of organizations and hundreds of millions of users in 190 countries. Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif.

About Alt-N Technologies

Alt-N Technologies, a subsidiary of **Research in Motion** (Nasdaq: RIMM; TSX: RIM), develops affordable and secure messaging and collaboration solutions designed for, and trusted by, small-to-medium businesses in over 90 countries and 25 languages worldwide. The company's flagship solutions, the **MDaemon® Email Server for Windows** and the **SecurityGateway for Exchange/SMTP Servers**, install in minutes, include the latest email security technologies, and require minimal support and administration to operate and maintain. The company uses a network of global distributors and resellers for the sales and support of its products.

References and Notes

- <http://blog.commtouch.com/cafe/data-and-research/spamassassin-y2k10-bug/>
- <http://spamassassin.apache.org/news.html>
- <http://blog.commtouch.com/cafe/spam-favorites/spammers-have-given-up/>
- <http://blog.commtouch.com/cafe/data-and-research/an-academic-approach-to-anti-spam/>
- <http://www.newscientist.com/article/mg20527446.000-to-beat-spam-turn-its-own-weapons-against-it.html>
- <http://blog.commtouch.com/cafe/email-security-news/blogger-phishing-attack-uses-%e2%80%9cimproved%e2%80%9d-email-template/>
- <http://blog.commtouch.com/cafe/email-security-news/cnn-redirect-exploited-by-scammers/>
- <http://www.theaustralian.com.au/news/call-to-cut-net-link-on-virus-hit-computers/story-e6frg6n6-1225823060022>
- <http://www.zdnet.com.au/iinet-trial-clears-way-for-zombie-code-339301513.htm>
- Note on Malware names used (Page 10): The malware names used may differ from the names used by the different vendors but the AV-Test data is based on matching checksums.

commtouch®

Real Security. In Real Time.

© 2010 Alt-N Technologies, Ltd.
2550 SW Grapevine Parkway, Suite 150
Grapevine, Texas 76051

Phone: (817) 601-3222 Fax: (817) 601-3223

Alt-N Technologies is a Subsidiary of Research In Motion
MDaemon is a registered trademark of Alt-N Technologies.
All trademarks are property of their respective owners.
www.altn.com

© 2010 Commtouch Software Ltd.
bizdev@commtouch.com

Phone: 650-864-2114 (US) +972-9-863-6895 (International)
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.
www.blog.commtouch.com
www.commtouch.com