



Q1 2009 Internet Threats Trend Report

Conficker Worm Infects Millions Around the World

April 14, 2009

Introduction

The major news of the first quarter was the rapid propagation of the Conficker worm. Research indicates its three variations have infected more than 15 million computers, weaving a massive zombie botnet, since appearing on the scene in November 2008. The botnet lay dormant for weeks, leaving computer users nervous and vulnerable; and only in the last days leading up to the publication of this report did it begin to be activated for malicious purposes.

Throughout the quarter, spammers and malware distributors continued to exploit legitimate sites to bypass traditional content filtering technologies. Recent tactics include the targeting of ISPs and the borrowing of images from legitimate, well-known hosts to use in e-mail messages.

Another growing trend is the use of social networking sites (e.g. Facebook, Twitter) for phishing schemes. By pulling on the heartstrings of networks of friends, unknowing users have fallen victim to money-making and password-stealing schemes.

Q1 2009 Highlights

- The Conficker worm infected more than 15 million computers since its first appearance last Fall.
- Loan spam jumped to the top of the list of top spam topics, with 28% this quarter.
- Users of social networking sites fell victim to new, more complex phishing attacks.
- Computers/Technology sites and Search engines/Portals are among the top 10 Web site categories infected with malware and/or manipulated by phishing.
- Brazil continues to lead in zombie computer activity, producing nearly 14% of zombies for the quarter.
- Spam levels averaged 72% of all email traffic throughout the quarter and peaked at 96% in early January. It then bottomed out at 65% in February.
- Spammers attacked large groups of an ISP's users and moved to the next ISP in a targeted spam outbreak.
- An average of 302,000 zombies were activated each day for the purpose of malicious activity.



Conficker Worm Weaves its Way Around the World

The Conficker phenomenon has become one of the most widespread computer worms ever, and the end is nowhere in sight. With its first appearance in November, Conficker A exploits a vulnerability in Microsoft Windows, worming its way into a system and then generating a list of 250 random domains. The infected system then communicates with the domains until it finds the one that has been set up with a payload with further instructions. An advanced URL filtering solution should be able to prevent the communication of the worm to the generated domains by blocking suspicious URLs before a connection could be established.



- Conficker A generated 250 domains per day.
- Conficker C generates 50,000 per day.

Early in the first quarter of 2009, Conficker B appeared. This variant passed from computer to computer via network shares and USB devices. The latest iteration, Conficker C, shuts down security services (e.g. anti-virus software) and blocks security update Web sites, making it more difficult to contain. Adding to the complexity, instead of 250 random domains, Conficker C generates 50,000 each day.

All three variations of the worm have infected approximately 15 million computers around the world and its ultimate purpose has been unclear. The worm lay dormant for weeks, awaiting further instructions from the downloaded payloads. In the few days prior to this report's publication, it has started to be used for sending spam; and if the owner of this worm arranges for all of the infected machines to "awaken" at the same time and work as one huge spamming botnet, there is potential for a meaningful rise in spam counts for the second quarter.



Spam

Companies around the world continue to send millions of unsolicited emails, clogging inboxes and decreasing productivity. After the fall of McColo in Q4 2008 and the subsequent drop in the amount of spam being transmitted, the levels have slowly returned to the levels they were before the incident.

Spammers Target ISPs

A new tactic that emerged in the first quarter of 2009 for spammers avoiding detection and blacklisting is the targeted spamming of ISPs. Through trial and error, spammers have seen that sending large numbers of emails raises red flags in the Internet security community. Legitimate organizations and ISPs monitor Internet activity and band together to identify and blacklist senders to prevent further attacks.

To circumvent this, spammers are beginning to attack ISPs one at a time. A general purpose attack email is sent to a list of users on one ISP; the spammer then moves to the next list, targeting users of a different ISP, and may change its messaging server to delay detection. In general, spammers are harder to identify and detect when they employ this method of sending large numbers to one ISP as opposed to randomly sending large batches of email.

Russian Spam Levels Increase

During the quarter, Commtouch labs noted a spike in the amount of Russian-language spam circulating the world. When comparing it to other types of spam messages, Russian spam is unique – it is usually sent from legitimate companies as part of a direct marketing plan. Where in most areas, unsolicited email sent in bulk is considered “spam,” Russian businesses often employ this inexpensive

Sample Russian-Language Spam Masking Telephone Number with Letters

<p>From: "Шейх-Раджаб Али" Date: Wednesday, 01 April, 2009 12:29 To: bulma.madefing@commtouch.com Subject: ваши документы</p> <p>ДЛЯ ИНОСТРАНЦЕВ ДЕЛАЕМ ВСЁ:</p> <p>Разрешения на работу (ближнее и дальнее зарубежье) Визовая поддержка (приглашения, телексы, турваучеры) для приезда в Россию для любой цели Постановка иностранцев на миграционный учет в УФМС (быв. ПВУ или УВИР) Юридическое сопровождение обращений в УФМС (подготовка, подача, ускорение) Регистрация автомобилей и прохождение ТО для иностранцев</p> <p>Тел. (495) 650-1740, 8-915-764-56-45 info@com.dobro.ru</p> <p>Шейх-Раджаб Али</p>
--

Source: Commtouch Labs



tactic as part of their marketing plan because this behavior is not widely prosecuted or even socially unacceptable in Russia.

Additionally, Russian spam can be unique in form. Unlike spam in other languages which publicize URLs and hide the business phone numbers and addresses, Russian-language spam does not typically contain Web site links. The emails often contain actual phone numbers for recipients to call, albeit the phone numbers are generally masked using spam tricks to bypass traditional content filtering systems. As seen in the example below (an advertisement for services tourist and immigrants, including help obtaining visas or driver's licenses), the phone number contains letters in place of some of the numbers (i.e. an "O" in place of a zero and a Cyrillic letter in place of the number four).

ZDNet exploited via Google Docs

Google Docs, a free online suite of applications, has provided a fruitful breeding ground for new outbreaks during last several quarters.

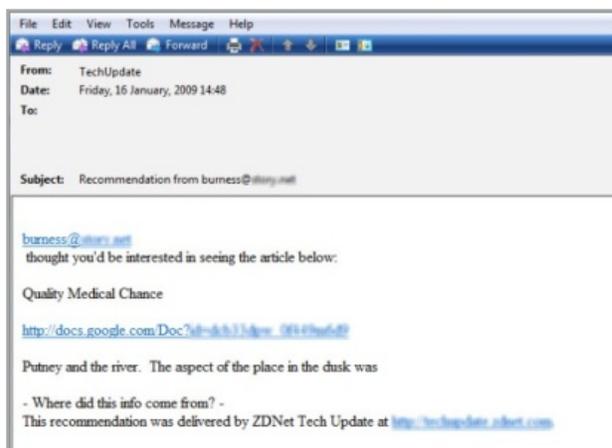
An attack at the beginning of the first quarter of 2009 exploited the popular tech site, ZDNet, by stating that a Google docs document had been recommended by their Tech Update service.

As seen in the example, a recipient could have easily been tricked into believing that the message was a legitimate technology article recommended by someone in the community; both the "Sender" and the closing line refer to the Tech Update service.

The hyperlink within the email message, however, leads to an advertisement for International Rx, hosted on Google Docs.

ZDNet read the Commtouch blog post about this outbreak and immediately looked into the issue. When they found that an old ZDNet server had been compromised, they took measures to lock it down, to ensure the problem would not occur again.

Sample Spam Message Using ZDNet's Tech Update Service



Source: Commtouch Labs

Sample Spam Landing Page Redirected from Google Docs



Source: Commtouch Labs



CBS and Pizza Hut now selling your favorite meds

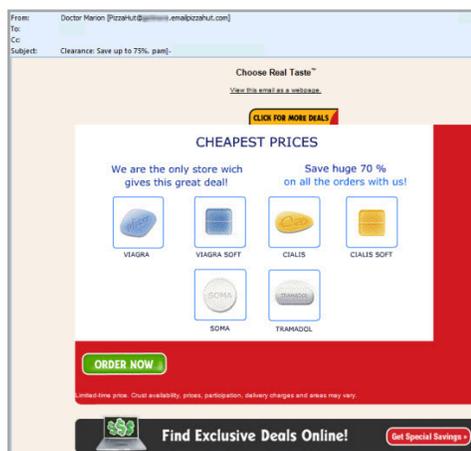
Spammers continued to exploit legitimate sites to host their materials during the first quarter of 2009. They also masked their e-mail addresses and most recently, they have “borrowed” images from legitimate, well-known hosts to use in e-mails in hopes of bypassing spam filters.

A January outbreak included a “News Summary” image in the header; that particular image is actually hosted on the legitimate CBS News site. Although boasting different URLs within the messages, the sites they linked to were all for a pharmaceutical spammer site.

Sample Spam Message with Images Borrowed from CBS News



Sample Spam message with Images Borrowed from Pizza Hut



Source: Commtouch Labs

In the example here (with the red frame), images from the legitimate Pizza Hut site were used by spammers within their unrelated spam messages to confuse traditional image scanning spam filters. In the example here, the green “Order Now” button and the “Find Exclusive Deals Online!” tab are both images hosted from the Pizza Hut site.

In this case, the spam provider also masked the sending address as *PizzaHut@____.emailpizzahut.com* to further confuse recipients and traditional content-based spam filters.



Social Networking and Phishing

Social Networking sites like Facebook, Twitter and MySpace have become targets for cyber-criminals looking to make money by tricking networks of friends or by stealing passwords for access to personal and financial accounts. As these sites gain in popularity and numbers of users, the types and severity of phishing attacks have also risen.

Facebook friend or foe? New phishing schemes target social networks

Back in early 2008, a Facebook phishing scheme circulated where some users received wall posts proclaiming that funny or scandalous pictures of them had surfaced. When a user clicked on the link, he or she was redirected to what looked like the Facebook login page, but which actually was an imposter site that collected usernames and passwords of unknowing users.



The newest occurrence that became widespread in the recent quarter is a bit more complex. Some users received what appear to be desperate messages from their "friends" who have found themselves in a financial bind. These messages have

arrived via Facebook chat, as a direct message to a user's inbox or as an updated status on the victim's profile proclaiming that the person urgently needs help.

Facebook's Online Reporting System



Source: Commtouch Labs

The messages are part of a new scam where cyber criminals try to steal money by testing the loyalty of friends.

Facebook has set up an online reporting system for victims who have either received or sent these kinds of messages and warns users to use caution when dealing with requests for money or personal information.



Targeting Twitter: A new wave of phishing

Web 2.0 applications are becoming more vulnerable to Internet security threats as culprits seek easier ways to reach large numbers of people. One of the latest targets is the microblogging service, Twitter.

The scam targeted Twitter users via direct messages; the direct messages proclaimed that a blog post had been written about them or that funny pictures of them had been located online.

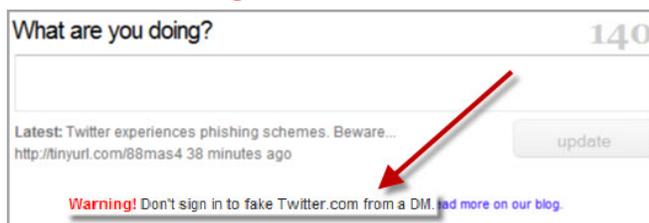
If a user clicked on the link provided in suspect messages, he or she was directed to a landing page that looks exactly like the Twitter home page. Upon closer inspection, however, the URL appeared to be a variation on the real Twitter URL, for example: *http://twitter.access-logins.com*. According to the Commtouch Data Center, this domain is classified as “fraud/phishing,” and the domain was set up to mock the appearance of Twitter in hopes of stealing user names and passwords from people who may not realize they have been tricked.

When logged into the legitimate Twitter service, users received a warning like the one pictured here. In the case where an account was compromised and used to perpetuate the scheme, the real Twitter “proactively reset the passwords of the accounts” and offered the option for users to change their own passwords.

While this was a phishing scam, plain and simple, using familiar techniques from spam and IM schemes, there are other Web security holes inherent in the Twitter platform. Because of the nature of twitter, condensing thoughts into 140 character snippets, URLs are often automatically condensed using a service like tinyurl, which redirects to longer addresses, making them easier to use with a smaller number of characters.

As seen above (just under the text box), if a URL is condensed using tinyurl on Twitter, there is no way to know where it leads before it is clicked, except in the case of some twitter add-ons such as Power Twitter that “expand” the URL. In an attempt to overcome this issue, Twitter added an “expanded URL” feature to its search page so savvy users can see what URL they will be going to (even if they do not know if that URL is safe or not), but this feature is still not available on individual tweets from the regular Twitter site.

Twitter Status Update Page with Warning



Source: Commtouch Labs



Blended Threats

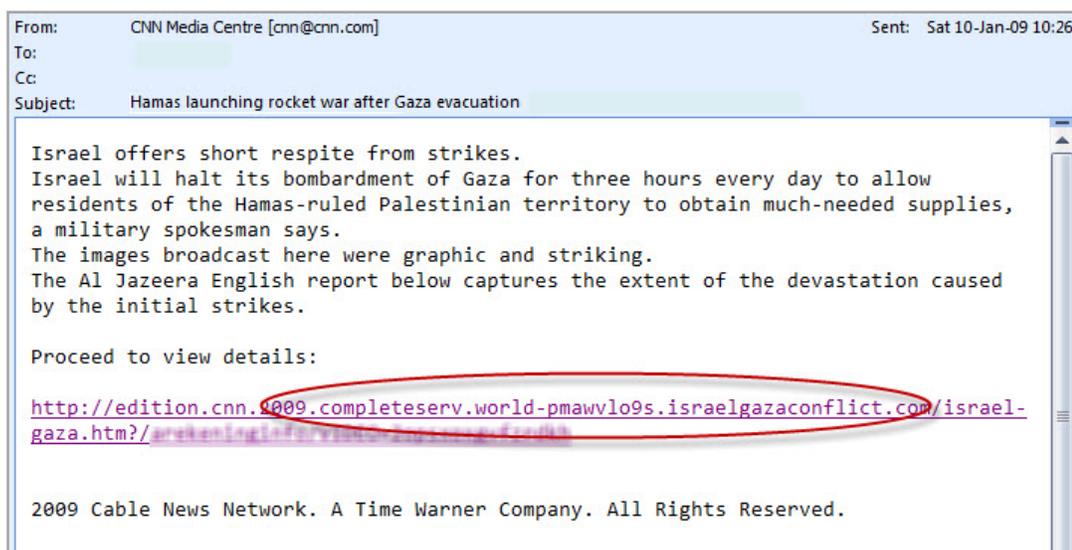
Blended threats are attacks that use multiple paths to reach their goals; sometimes an email will lead to malware downloads or phishing schemes. Cyber criminals are becoming more advanced in their attacks and blended threats are becoming more sophisticated with near perfect site duplications and official looking emails.

CNN Falls Victim to Conflict in Gaza

The unrest in the Middle East earlier this year, was used as fodder for spammers looking to entice unknowing victims into downloading malware. As demonstrated in previous outbreaks, spammers use current events (e.g., the financial crisis, elections, major international events) to ensnare recipients. By masking the origin and tricking users into believing they are legitimate sources, the chances of successfully distributing malware increase.

As seen below, one outbreak during the first quarter appeared to have been sent from CNN, taking advantage of the timely hostilities in Gaza with subject lines such as "israel's war on hamas: a dozen thoughts," "hamas goads israel into war," "israel vows war on hamas in gaza" and "hamas launching rocket war after gaza evacuation." The actual Web link within the email, however, was not from CNN; it appeared to point to the legitimate "edition.cnn" but the actual domain was a hoax site.

Sample Spam Message Masquerading as a Message from CNN



Source: Commtouch Labs



Victims of the scam believed they were receiving legitimate news covering the war, and were taken to a Web site that closely resembled CNN. When they attempted to click on the link to watch the video, they were pulled into a complicated web of download screens prompting them to update Adobe Acrobat or Flash player software. The only way out of the loop was to end the browsing session. Users that accidentally accepted the software download installed a Trojan which opened communication for the download of further malware from a remote location.

Masking the origin of emails tricks users into believing they are legitimate sources and increase the chances of distributing malware.

Adobe was aware of the problem and has seen numerous attacks in the past which exploit their name and trick people into downloading malware. Last summer, a similar outbreak claiming to originate from CNN was distributed. On the Adobe security blog, a post dated August 4, 2008 warns users not to download software claiming to be Adobe unless it is done directly from the Adobe download site.

CNN also became aware of the scam and their "Behind the Scenes" blog proactively warned CNN readers not to download any software pertaining to the Gaza conflict.

New phishing scheme targets Italian Credit Card Company

Spam and phishing attacks in non-English languages are not uncommon, and Italians were among the victims during the quarter. A phishing scheme surfaced in February with a nearly immaculate Web site duplication. CartaSi, a well-known Italian credit card company, was the target.

Sample CartaSi Phishing Scheme Email



Source: Commtouch Labs



The circulating email alerts CartaSi customers that their account statements are available online and encourages them to log-in to “view it, print it and save it to your personal files on your PC.” The link was written to appear as a CartaSi URL but when a user clicked it, the page was redirected to a page hosted on *ns1.druti.net*, which is classified in the Commtouch Data Center as “Reported Web Forgery.” Unknowing users were tricked into supplying their account information to the cyber-criminals who could then use the information to gain access to financial statements.

The fake landing page is a near perfect replica of the legitimate CartaSi Web site as seen below.



Source: Commtouch Labs



Source: Commtouch Labs

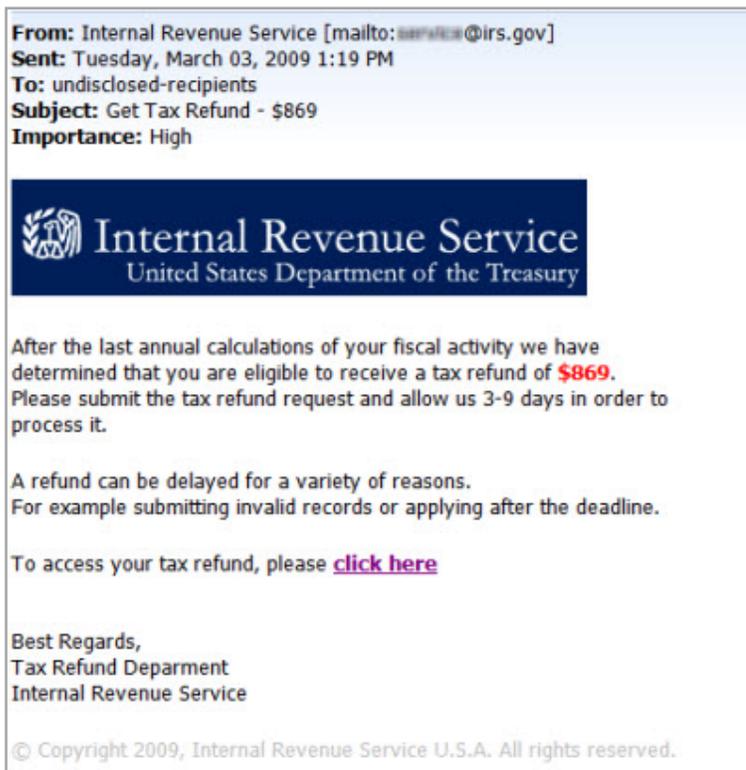
Phishing schemes are becoming more elaborate and cyber-criminals are taking more time to develop very believable fake sites to trick unassuming users.



IRS Phishing Schemes...just in time for tax season

As US tax season approached, the numbers of IRS and tax-related spam and phishing outbreaks rose. In the example pictured here, the outbreak appears to be an official email, complete with an *@irs.gov* email address, an IRS logo across the top and a copyright statement at the bottom.

Sample IRS Phishing Scheme Email



Source: Commtouch Labs

Most US taxpayers would be excited to receive an email promising a refund of any kind. In this case, however, unknowing recipients followed the link in the email and found themselves on a page set up by cyber criminals to look identical to the actual IRS Web site. Recipients were prompted to fill out a form providing personal information like social security number, address and sometimes even an ATM card number and its PIN. Once submitted, the cyber criminals gained direct access to the victims' financial accounts.

The IRS is aware of these schemes and has set up an informational page for people who feel they have been targeted.



Web Security

The Internet has become an indispensable part of everyday life and work, yet the massive growth of data coupled with a rapid increase in the number of individuals with Web access has introduced a variety of security issues.

This site may harm your computer...or not...

On Saturday, January 31 between 6:30 a.m. and 7:25 a.m. (Pacific Standard Time), Internet users searching using the popular Google search engine received a message stating "This site may harm your computer" for every query. According to the official Google blog, the problem was caused by human error and the company worked as quickly as they could to reverse the issue once it had been discovered.

Typical Internet users may need a third party to warn them if a site is potentially malicious.

Google works closely with StopBadware.org to establish criteria for maintaining a list of possibly malicious sites in order to protect Google users from malware or other online threats. In this case, human error caused every indexed site to be categorized as malicious.

In their blog, Google documented the incident as such:

Unfortunately (and here's the human error), the URL of '/' was mistakenly checked in as a value to the file and '/' expands to all URLs. Fortunately, our on-call site reliability team found the problem quickly and reverted the file. Since we push these updates in a staggered and rolling fashion, the errors began appearing between 6:27 a.m. and 6:40 a.m. and began disappearing between 7:10 and 7:25 a.m., so the duration of the problem for any particular user was approximately 40 minutes.

Typical Internet users may need guidance to keep their computers and networks safe; sometimes a third party is needed to warn them if a site is potentially malicious. In this case, the third party was Google, a trusted resource for millions of users who would most likely believe any message they received.

Google employs automatic algorithms that are manually checked to ensure individual computers are safe. Humans developed computers to help automate processes, but as demonstrated in the case with Google, humans still need to go back to make sure the computers are working properly.



Web Threat Trends: Malware and Phishing Sites

During the first quarter of 2009, Commtouch analyzed which categories of Web sites were most likely to contain malware or phishing. As expected, pornographic and sexually explicit sites topped the list of sites infected with malware, but the less expected job search sites also made an appearance, albeit further down the list. Criminal activity sites fell from first place last quarter to sixth place this quarter.

On the list of Web categories manipulated by phishing, download sites and social networks continue to fall victim to new schemes. Newcomers to the list include the number one category – Health and Medicine, plus chat sites and Web-based email.

Top 10 Web Categories Infected with Malware	
Rank	Category
1	Pornography & Sexually Explicit
2	Computers & Technology
3	Streaming Media & Downloads
4	Business
5	Search Engines & Portals
6	Criminal Activity
7	Shopping
8	Health & Medicine
9	Job Search
10	Education

Source: Commtouch Labs

Top 10 Web Categories Manipulated by Phishing	
Rank	Category
1	Health & Medicine
2	Web-based Email
3	Finance
4	Computers & Technology
5	Chat
6	Search Engines & Portals
7	Social Networking
8	Personal Sites
9	Download Sites
10	Politics

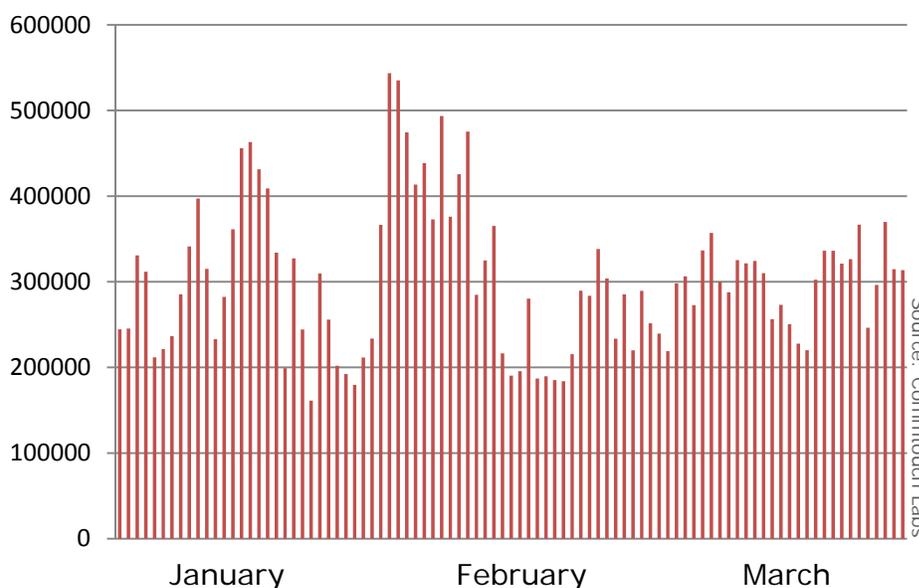
Source: Commtouch Labs



Newly Active Zombies

The lifespan of zombies is very short, and according to Commtouch Labs, the first quarter saw an average turnover of 302,000 zombies each day. The graph below shows the newly active zombies each day throughout the quarter; because the Conficker botnet had not yet been activated by the end of the first quarter, it is not reflected in this graph.

Q1 2009 Newly Active Zombies



Zombie Hot Spots

Absent last quarter, verizon.net returned to bump 163.data.co.cn off the top 10 list. TpNet from Poland moved from third place in Q4 2008 to first place this quarter.

Brazil continues to produce the most zombies, responsible for nearly 14% of global zombie activity according to Commtouch Labs.

Top 10 Zombie Hot Spots – Average Per Day		
Rank	Category	# Zombies
1	tpnet.pl	34,480
2	veloxzon.com.br	33,714
3	ttnet.net.tr	33,105
4	telesp.net.nr	27,451
5	brasiltelecom.net.br	22,714
6	asianet.co.th	21,609
7	ukrtel.net	21,146
8	telecomitalia.it	20,793
9	verizon.net	16,088
10	airtelbroadband.in	14,857

Source: Commtouch Labs



Top Spam Topics

Loan spam jumped from 3% of all spam messages in Q4 2008 to first place, with 28% of all spam messages this quarter, possibly reflective of the global economic situation. Pharmacy spam fell from the number one spot at 42% last quarter to third place with 19% this quarter.

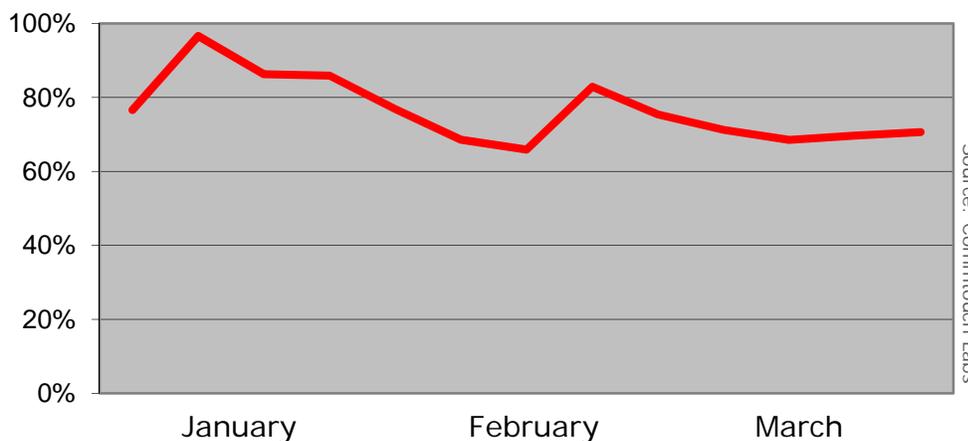
Topics of Spam Email Q1 2009	
Loans – 28%	Dating – 6%
Replicas – 20%	Degrees – 4%
Pharmacy – 19%	Software – 1%
Enhancers – 11%	Other – 4.6%
Weight Loss – 7%	

Source: Commtouch Labs

Spam Levels

Spam levels averaged 72% of all email traffic throughout the quarter and peaked at 96% in early January, and bottomed out at 65% in February.

Q1 2009 Spam Levels

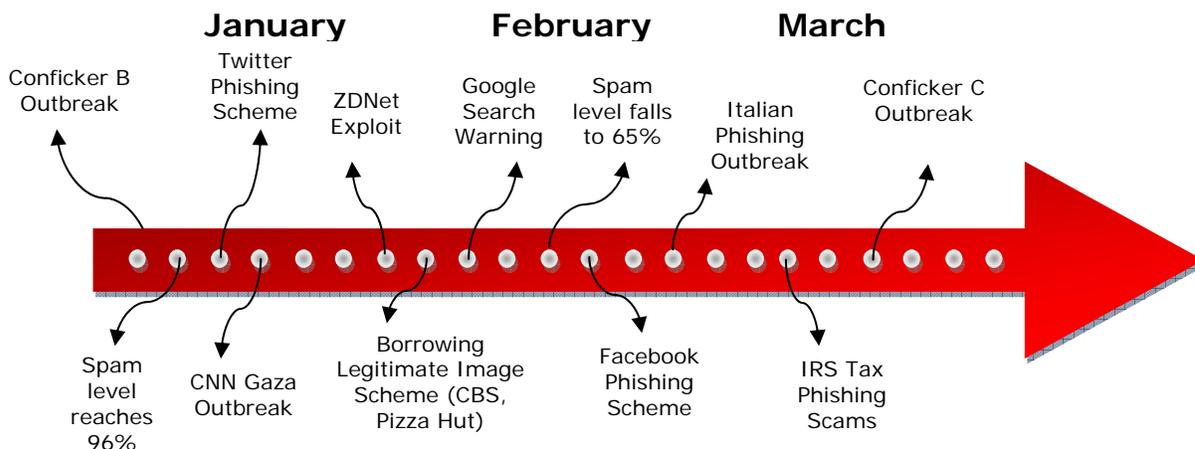


Source: Commtouch Labs

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 at the ISP level.



Q1 2009 Outbreaks in Review



About Commtouch

Commtouch[®] (NASDAQ: CTCH) provides proven messaging and Web security technology to more than 100 security companies and service providers for integration into their solutions. Commtouch's patented Recurrent Pattern Detection[™] (RPD[™]) and GlobalView[™] 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. Stay abreast of the latest messaging and Web threat 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 info@commtouch.com.

About Panda Security

Panda Security is one of the world's leading IT security providers, with millions of clients around the globe and products available in over twenty languages. Our mission is to keep our customers' information and IT assets safe from security threats, giving them the most effective protection with the minimum resource consumption. Every day, thousands of new malicious codes are created. To combat this threat, Panda Security has developed an innovative and unique security model which can automatically analyze and classify thousands of new malware samples. This model is collective intelligence and ensures that Panda Security solutions can protect against far more threats than the products of any other company. The exceptional detection capacity of collective intelligence can be put to the test at the Infected or Not website (<http://www.infectedornot.com>). For more information and evaluation versions of all Panda Security solutions, visit our website at: <http://www.pandasecurity.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.