



Internet Threats Trend Report Q2 2010

In This Report

Multi-stage attacks: This report delves into some of the techniques used by cybercriminals combining messaging, Web elements, and social engineering.

Reset your Twitter password: A wave of emails from "postmaster.twitter.com" lead users to malware infested websites.

What is "enhancement" spam? Analysis of the most popular spam topics and a closer look at one of the stranger products marketed by spammers this quarter.

How phishers get free Web hosting: An analysis of the Web categories most likely to be hosting a hidden phishing page, including some examples.

Greeting cards and MS® Outlook updates: This quarter's favored email-borne virus attachments.

Outbound spam and zombies: New research into outbound spam highlights the link to zombies and looks at the responsibility of service providers.

Q2 2010 Highlights

▼ 179 billion

Average daily spam/phishing emails sent

▲ 307,000 Zombies

Daily turnover

▲ Streaming media/ Downloads

Most popular blog topic on user-generated content sites

▲ 1811 variants

Of Mal/Bredo malware emailed

▼ Pharmacy ads

Most popular spam topic (64.4% of spam)

▲ India

Country with the most zombies (13%)

▲ Pornography/ Sexually Explicit

Website category most likely to be compromised with malware

Perfecting the multi-stage attack

This quarter saw further examples of multi-stage attacks. These are often referred to as blended attacks as they may combine messaging and Web elements.

- The first stage involves an email designed to entice or convince a user to click on the embedded link or respond to the 419 scam. Alternatively, this stage might originate on the Web with SEO poisoning – where cybercriminals manipulate popular search engine results to make their links appear higher than legitimate results. When users search for related terms, the infected links appear near the top of the search results, generating a high number of visits to malware-infested pages.
- In the second stage, the user reaches the destination website which hosts spam advertising, malware or phishing.
- A further third stage aims at getting a user to install malware, complete a phishing form or submit personal information for marketing or identification theft purposes.

Spammers and malware writers continue to come up with new ways to implement multi-stage attacks that trap users while attempting to bypass messaging and Web defenses. In fact these attacks highlight the importance of a defense strategy that includes both messaging and Web components.

Stage 1: Open this email!

This is the first social engineering stage where users must be convinced to take action based on a received email. Malicious senders continue to use three proven methods for getting recipients to open emails and follow the included links:

- Including current events or upcoming calendar events/holidays in the email content
- Using well-known brands
- Sending the email from a trusted source

Emails with current and calendar events

A sample of some of the events abused in the second quarter of 2010 is presented below. April saw extensive worldwide coverage of flight cancellations caused by the eruption of Iceland's Eyjafjallajökull volcano. Related spam combined volcano subjects with automatically generated random words.

- fears volcano chaos will continue abasedly
- iceland volcano disrupts flights actuate
- sport left grounded by volcano accommodated
- volcano ash affects air travel abfarad
- volcanic ash causes travel chaos abiotrophy
- volcanic ash cloud causes flight chaos alcholemlia
- volcanic ash grounds flights abashlessly

Volcano related text was also used in pharmacy spam as shown below. The use of random topical text in this way is designed to fool rule-based anti-spam engines that may interpret the emails as legitimate.



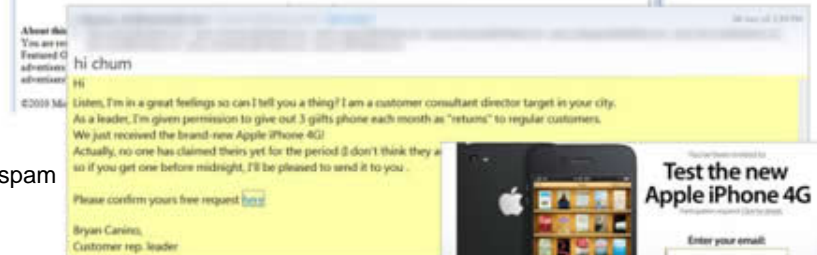
Source: Commtouch

Apple was also a favorite email topic as the iPad passed one million sales in May, followed by the launch in June of the iPhone 4. The iPhone 4 email (shown below) lured users to a maze of affiliate marketing links that targeted users with US IP addresses. Unsuspecting users hoping to actually receive the “free iPhone 4” may also have provided too much personal information, making them vulnerable to identity theft. Non-US IP addresses were directed a lottery scam site.

Millionth iPad spam



iPhone 4 spam



iPhone 4 destination site

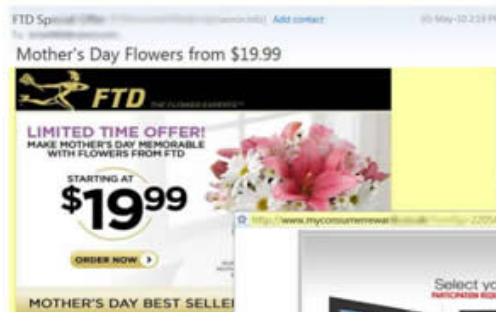


Source: Commtouch

An example of a calendar event abused this quarter was Mother's day. Here again, Mother's Day subjects were combined with random words that appeared to be emails selling flowers. The FTD brand was used within the body to add authenticity to the emails. In this case the links led to a "free TV" site with extensive affiliate marketing links and possible identity theft motives.

- alan\$20 off mother's day flowers – today only!
- albert\$20 off mother's day flowers – today only!
- alex\$20 off mother's day flowers – today only!
- Mother's Day Exclusive – roses starting at only \$19.99
- Mother's Day Flowers from \$19.99
- Mother's Day Exclusive! roses from \$19.99

Mother's Day spam emails



Links lead to "Free TV" site



Source: Commtouch

Finally, the biggest event of the quarter was the 2010 Football/Soccer World Cup. The World Cup was predictably used in every kind of multi-stage attack from pharmacy spam to lottery scams (see sample below).

Lottery scam email

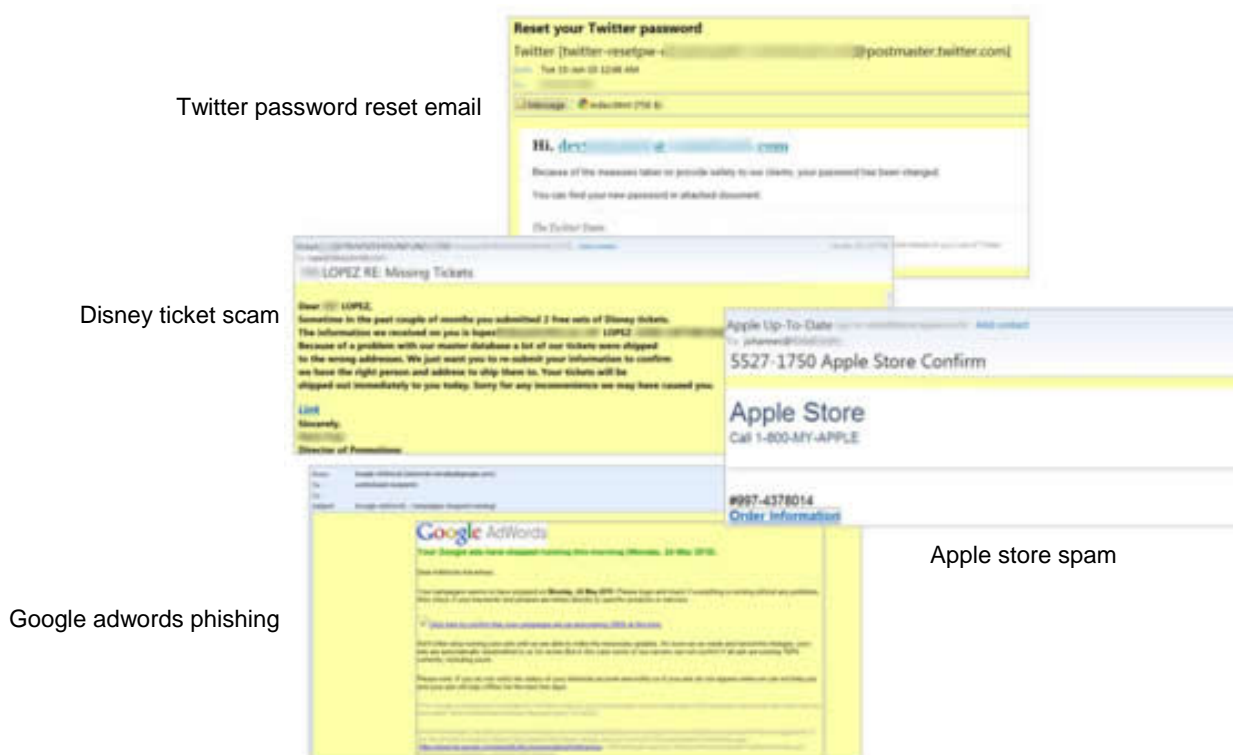


Source: Commtouch

Emails abusing well-known brands

Emails claiming to originate from well-known brands directed recipients to a range of malicious and spam sites. Some examples from the last three months:

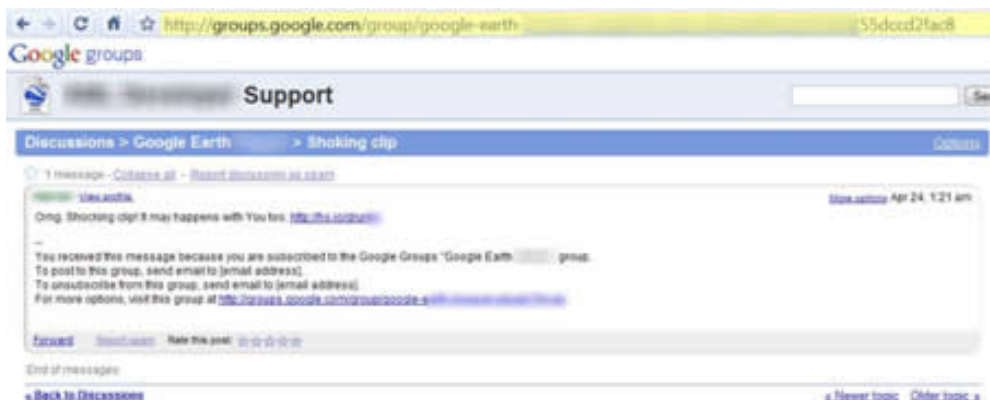
- “Reset your twitter password” – malware
- “Apple store confirmation” – pharmacy spam
- “Reset Google adwords account” – phishing
- “Google 12th birthday giveaway” – 419 scam
- “Free Disney tickets” – identity theft



Source: Commtouch

Emails from trusted sources

In these cases, the source domain of the email is genuine and verifiable, causing recipients to be less suspicious about opening the email or clicking embedded links. In May, Commtouch Labs described an attack directed at users of Google Groups. The message subject sent out to multiple groups was “Shoking clip” (sic) and the body simply stated “Omg – shocking clip! It may happen to you too.” Those following the link would arrive at a malware video player website similar to those described in “Stage three” below.



Source: Commtouch

The source domain, Google Groups in this case, helps the messages bypass content filtering engines as well as suspicious users' defenses.

Stage 2: Reputable destinations

In many cases the destination domain of the second stage is set up temporarily, but in an effort to gain legitimacy, the initiators of the multi-stage attack have used well-known Web properties to either host their destination sites or as redirect points to their sites. Shown here are two examples from the second quarter: Google Sites and Wedding Wire. In Google's words "Google Sites is a free and easy way to create and share webpages." It therefore represents a useful platform for hosting pharmacy advertising as shown below.

Spam with link to Google Sites



Pharmacy site within Google Sites

Source: Commtouch

A June outbreak included links to WeddingWire – a wedding planning site. Pharmacy spammers had created “wedding” pages and embedded redirect scripts into the page content.

- `<meta http-equiv="refresh" content="0;url=http://bestpharmace.com">`
- `<script type="text/javascript"> <!-- window.location = "http://bestpharmace.com" //--> </script></div>`

Although the initial destination is a reputable site, the code placed here redirects within seconds to the pharmacy site.

Page on WeddingWire

Redirect to pharmacy site

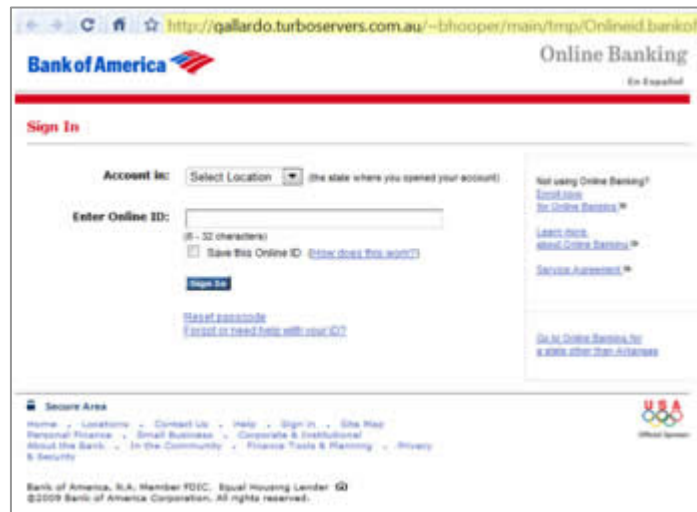


Source: Commtouch

Stage 3: One more click...

Here again the social engineering aspect is essential. These Web pages are carefully designed to ensure the completion of the multi-stage attack – each one focused on the particular desired outcome.

- In a phishing attack, the destination site must look as authentic as possible so that the phishing form will be completed and submitted. The sample below from Q2 2010 shows a Bank of America phishing page.



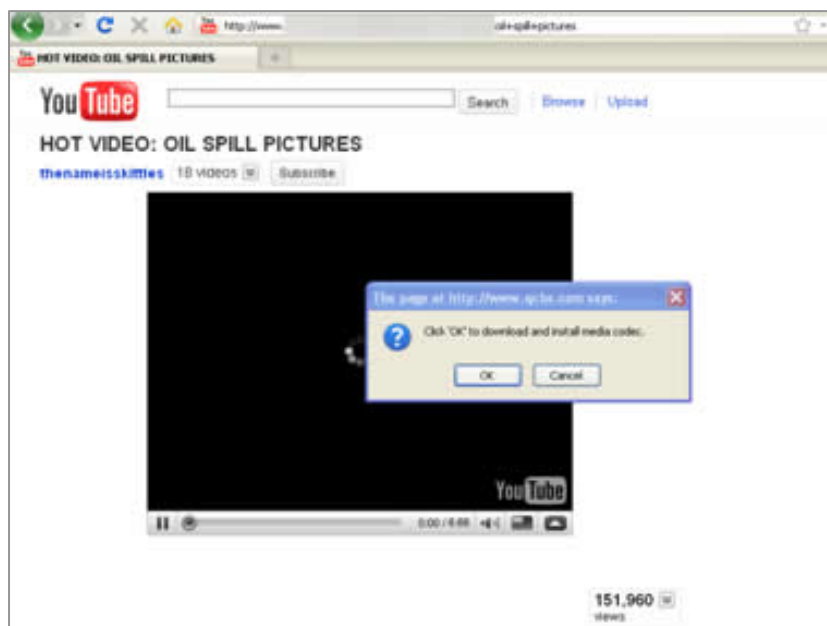
Source: Commtouch

- For marketing scams or identity theft, users must be motivated to supply their personal information. In the Apple iPhone 4 example described in Stage One above, respondents are promised that they are “one step away” from receiving a free iPhone. At each stage they will be providing more personal information or even paying online for several unrelated “offers.”



Source: Commtouch

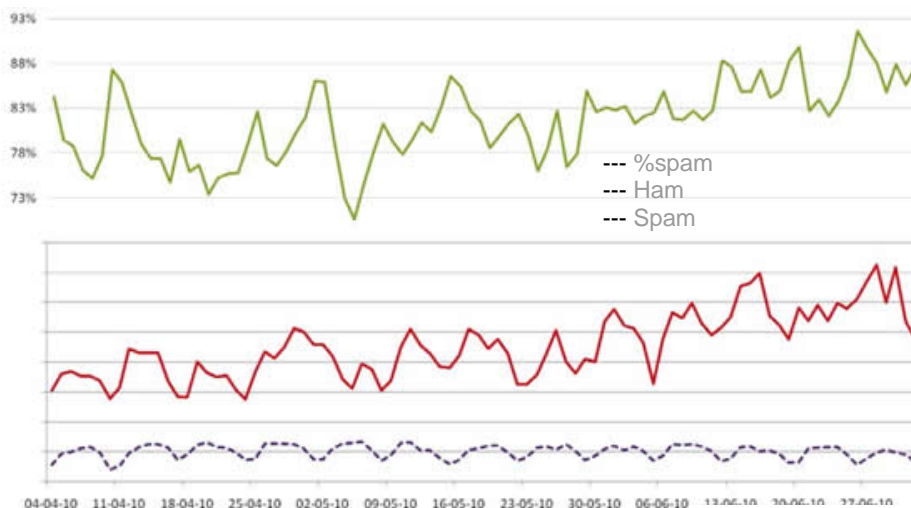
- For malware installation there needs to be some compelling reason to install a new software component. In June, Commtouch Security Alliance partner eSoft described well-crafted fake YouTube pages claiming to have a “Hot Video” associated with subjects ranging from the Gulf Oil Spill to the NBA Playoffs. Shown below is one of over 135,000 fake pages requiring installation of a “media codec” which is actually malware. In many cases user consent may not be necessary as the malware will use a browser exploit.



Source: eSoft (Commtouch Security Alliance Partner)

Spam Trends

Spam levels averaged 82% of all email traffic throughout the quarter, peaking at nearly 92% near the end of June and bottoming out at 71% at the start of May. These numbers are slightly lower than those detected in Q1 and equate to an average of around 179 billion spam messages per day.



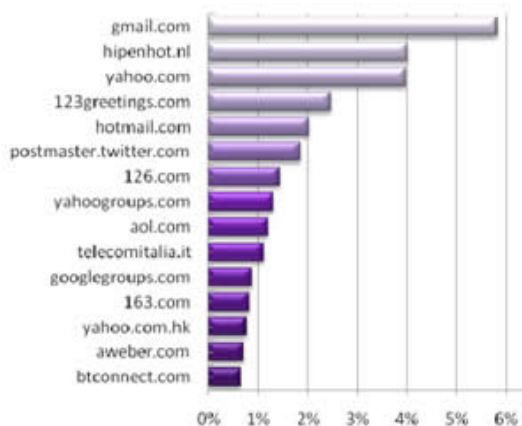
Source: Commtouch

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 sending domains

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. The addresses are typically faked in order to fool anti-spam systems and to give the impression of a reputable, genuine source.

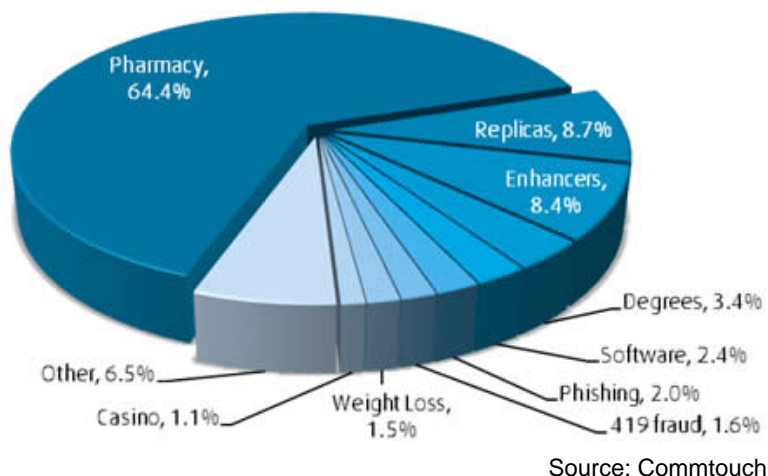
In the Q1 2010 trend report, Gmail.com held the top spot and a Commtouch analysis determined that only 1% of these emails actually came from Gmail. This quarter sees no change at the top, but sixth place is occupied by "postmaster.twitter.com". This is an indication of the large scale of the Twitter malware attack described on page 5 above.



Source: Commtouch

Spam Topics

Pharmacy spam remained in the top spot but dropped over 15% this quarter to 64.4%. Replicas also remained second, but increased its share to around 8.7%.



Regularly featuring in the top five is a category called “enhancers,” which differentiates it from counterfeit pharmaceuticals. Enhancers increased from 2.3% in Q1 to 8.4%. This quarter provided an unusual example of an enhancement product as shown below.

Spam email

Links open this Web page

Source: Commtouch

Compromised Web Sites

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

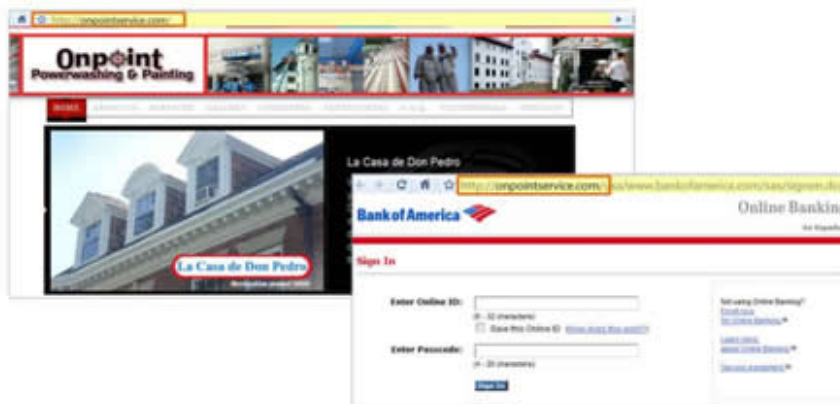
On the list of Web categories likely to be hosting hidden phishing pages, sites related to sex education again ranked highest. The “health & medicine” and “Computers & Technology” categories showed increased instances of embedded phishing pages compared to the first quarter of 2010. The sites infected 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.

Categories infected with Malware	
Rank	Category
1	Pornography/Sexually Explicit
2	Business
3	Education
4	Government
5	Parked Domains
6	Computers & Technology
7	Health & Medicine
8	Finance
9	Travel
10	Shopping

Categories infected with phishing	
Rank	Category
1	Sex Education
2	Games
3	Health & Medicine
4	Computers & Technology
5	Social Networking
6	Shopping
7	Pornography/Sexually Explicit
8	Education
9	Real Estate
10	Business

Source: Commtouch

The example below shows a home-service company unknowingly hosting a Bank of America phishing site.



Source: Commtouch

Two further examples from the second quarter are presented below. The first is a Swedish football fan club with an embedded Bank of America phishing page. The second example is a party supplies service with an embedded HSBC phishing page.



Source: Commtouch

Phishers gain several advantages from this ploy:

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

Web 2.0 Trends

Commtouch's GlobalView URL Filtering service includes highly granular categorization of Web 2.0 content. In addition to filtering accuracy, this provides insight into the most popular user generated content sites. In this quarter's analysis, streaming media and downloads surpassed entertainment (13%) as the most popular blog or page topic, covering 15% of the generated content. In ninth place is "Spam Sites" – these are the 3% of blog pages analyzed that have been adopted by spammers as the destinations for their pharmaceutical or replica campaigns.

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

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



Source: Commtouch



Source: Commtouch

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 TDSS.17 malware was distributed in emails either as a shipping label or as an update for MS Outlook. The TDSS-K virus was distributed as a “statement of fees”. As shown in the domain statistics on Page 9, 123greetings.com was used extensively during the quarter. The “you have received a greeting card” emails included malware attachments such as “setup.exe”.

Mal/Bredo malware was once again distributed with the most variants – totaling 811 for the quarter (1000 more than in Q1). The next most variants were of al/ZipMal which was emailed in 1021 different varieties (600 more than Q1).

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	Kaspersk	Trend Micro	Microsoft	CA
Gen:Variant.TDss.17	Zero Hour	13.3	Zero-	7.37	No Detection
Mal/TDSS-K	5.13	7.60	44.22	23.35	No Detection
Trojan.Downloader.JNDH	8.00	10.80	7.75	1.77	35.57
Troj/Agent-NRP	No Detection	No Detection	No Detection	No Detection	No Detection
Mal/Koobface-G	3.23	20.35	28.57	15.30	No Detection
Average (for detected)	4.09	13.01	20.13	11.94	35.57

Source: Commtouch

Newly Active Zombies

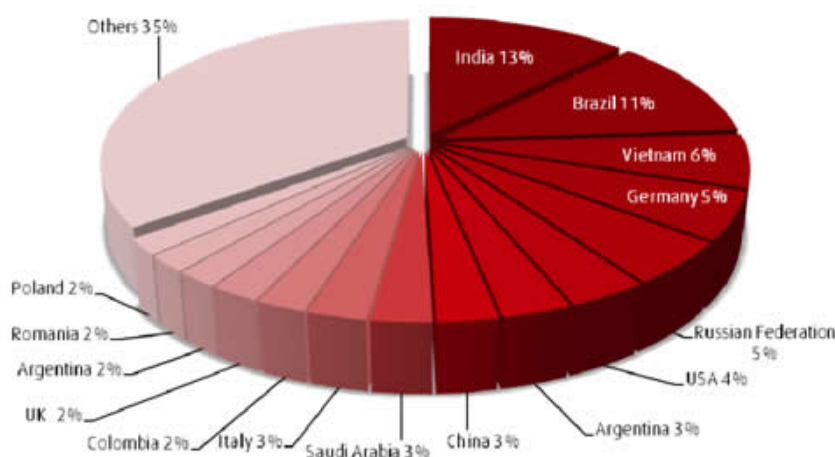
The lifespan of zombies is very short, and according to Commtouch Labs, the second quarter saw an average turnover of 307,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. This number is slightly increased over the 305,000 of the first quarter of 2010. The graph below shows the newly active zombies each day throughout the quarter.



The trend report of the first quarter described initiatives that require service providers to actively stop zombies within their networks. In the Osterman/Commtouch research report on outbound spam published in the second quarter of 2010, 87% of end users surveyed said that it is important or extremely important for email providers to actively eliminate zombies. The service providers polled estimated that 11.2% of their users had bots running on their PCs. The full report may be downloaded from the Commtouch website at <http://www.commtouch.com/outbound-spam-report>.

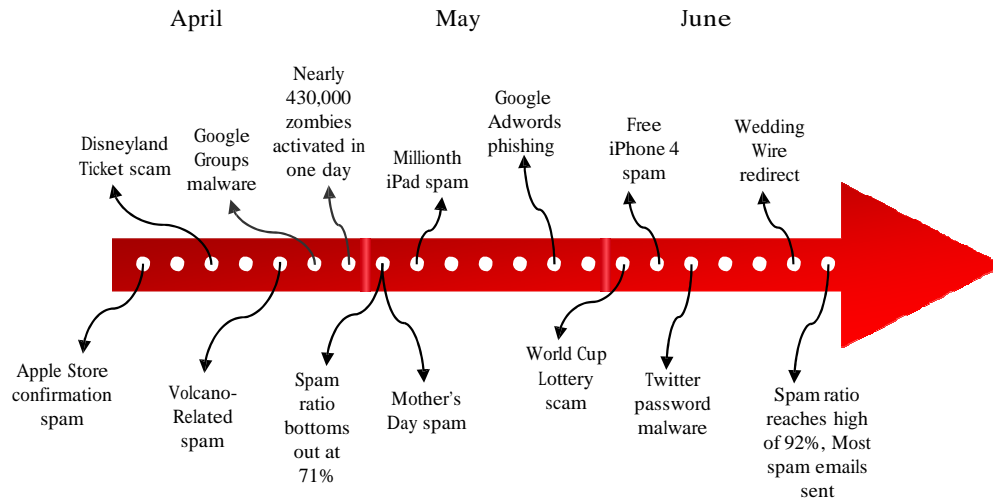
Zombie Hot Spots

India overtook Brazil this quarter to claim the top zombie producer title. Brazil dropped from 14% to 10%, Germany moved up into 4th place from last quarter's 6th place, and the US doubled its zombie percentage from only 2% last quarter.



Source: Commtouch

Q2 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. "Are you late for appointments and girls leave you?" // And I thought it was the aftershave!
9. "Our watches don't wear off like clothes" // but are they tumble-dryer safe?
8. "Make it longer than the Great China Wall!" // Don't you have something in a medium?
7. "Sold Out - LIMITED UNITS WATCHES!" // Sold out! - what a pity... I would have bought one
6. "Money for you. CONTACT: Demon, Russia" // Gee... that's tempting - but I'll pass
5. "Attack a greatpilule" // I'm against harming pilules, especially great ones
4. "Your wrist is screaming for a new watch" // My wrist should be more polite
3. "You would may never know" // I might could not understand
2. "contact Him now via e-mail/phone" // No need to go to church/synagogue then?
1. "Wanna enter?" // No!

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 Cyberoam

Cyberoam Identity-based UTM appliances offer comprehensive protection against existing and emerging Internet threats, including viruses, worms, Trojans, spyware, phishing, pharming and more. Cyberoam delivers the complete range of security features such as stateful inspection firewall, VPN, gateway anti-virus, gateway anti-malware, gateway anti-spam, intrusion prevention system, content filtering in addition to bandwidth management and multiple link management over a single platform. Cyberoam is certified by the West Coast Labs with CheckMark UTM Level 5 Certification, ICSA Lab, an independent division of Verizon Business, and the Virtual Private Network Consortium. Cyberoam has received the 2008 Emerging Vendor of the Year award by Frost & Sullivan, 2007 Global Excellence Awards for Integrated Security Appliance, Security Solution for Education and Unified Security, the 2007 Tomorrow's Technology Today Award for Unified Security was rated Positive by Gartner in its Marketscope for SMB multi-function firewalls. Cyberoam has offices in the Woburn, MA, USA and India. For more information, please visit <http://www.cyberoam.com>.

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.

References and Notes

- <http://www.commtouch.com/outbound-spam-report>
- <http://blog.commtouch.com/cafe/data-and-research/how-can-they-misuse-thee-google-%e2%80%93-let-us-count-the-ways-part-1/>
- <http://blog.commtouch.com/cafe/email-marketing/can-%e2%80%99t-wait-for-att-%e2%80%93-get-an-apple-iphone-4-for-free/>
- <http://blog.commtouch.com/cafe/email-security-news/reset-your-twitter-password-malware/>
- <http://blog.commtouch.com/cafe/spam-favorites/spammersmalware-writers-celebrate-world-cup-2010/>
- <http://threatcenter.blogspot.com/2010/06/135000-fake-youtube-pages-delivering.html>
- <http://blog.commtouch.com/cafe/spam-favorites/apple-itunes-ipad-imesd/>
- <http://blog.commtouch.com/cafe/phishing/google-adwords-phishing-attempt/>
- <http://blog.commtouch.com/cafe/spam-favorites/happy-mother-%e2%80%99s-day-%e2%80%93-have-some-spam/>
- <http://blog.commtouch.com/cafe/email-security-news/how-can-they-misuse-thee-google-%e2%80%93-let-us-count-the-ways-part-2/>
- <http://blog.commtouch.com/cafe/email-security-news/spammers-arent-tinkerbelle-identity-theft-takes-the-disney-magic-out-of-the-magic-kingdom/>
- <http://blog.commtouch.com/cafe/spam-favorites/volcanic-spam-chokes-inboxes/>
- Note on Malware names used (Page 14): The malware names used may differ from the names used by the different vendors but the AV-Test data is based on matching checksums.

Visit us: www.commtouch.com and blog.commtouch.com

Email us: bizdev@commtouch.com

Call us: 650-864-2114 (US) or +972-9-863-6895 (International)

Copyright© 2010 Commtouch Software Ltd. 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.

Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice.



Toll Free Numbers

USA : +1-877-777-0368 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958