Internet Threats Trend Report
July 2012

commtouch®

Internet Threats Trend Report – July 2012

In This Report

Q2 2012 Highlights

▼ **91 billion**

Average daily spam/phishing emails sent

Page 6

▲ **303,000 Zombies**

Daily turnover

Page 12

▼ **Streaming media**

Most popular blog topic on user-generated content sites

Page 13

▲ **Pharmacy ads**

Most popular spam topic (41.2% of spam)

Page 8

▲ **India**

Country with the most zombies (21%)

Page 12

▲ **Education**

Website category most likely to contain malware

Page 10

Overview

Distributors of malware, spam and phishing attacks are relying more and more on compromised websites. This tactic is designed to outwit email security and Web security systems that consider a site's reputation before blocking it. Legitimate websites with positive online reputations but with deficient plugins and known vulnerabilities were harvested en masse in the second quarter of 2012 to host redirects, malware, pharmacy sites and phony login pages.

The hacked websites were combined with effective social engineering that exploited multiple well-known brands to draw in victims. Similar branding tricks were used to distributed malware via email attachments. The popular file synchronization and sharing site Dropbox was also used as a malware distribution point in an attack promising free movie tickets. -

Malware trends

Blended attacks mix brands and malware

Malware gangs worked through a series of well-known brands during the 2nd quarter of 2012 in multiple email campaigns with links to malware. The attacks all included similar characteristics:

- Well-crafted emails matching those of known companies which were sent out in large volumes.
- The emails included links to multiple compromised websites which then redirected to the malware hosting websites.
- The compromised websites were often based on the WordPress content management system.
- The malware itself was mostly hosted on various .ru domains.
- The malware pages showed simple messages such as "Please Wait – Loading" (black text on white).

Webpage content while malware is downloaded

Source: Commtouch

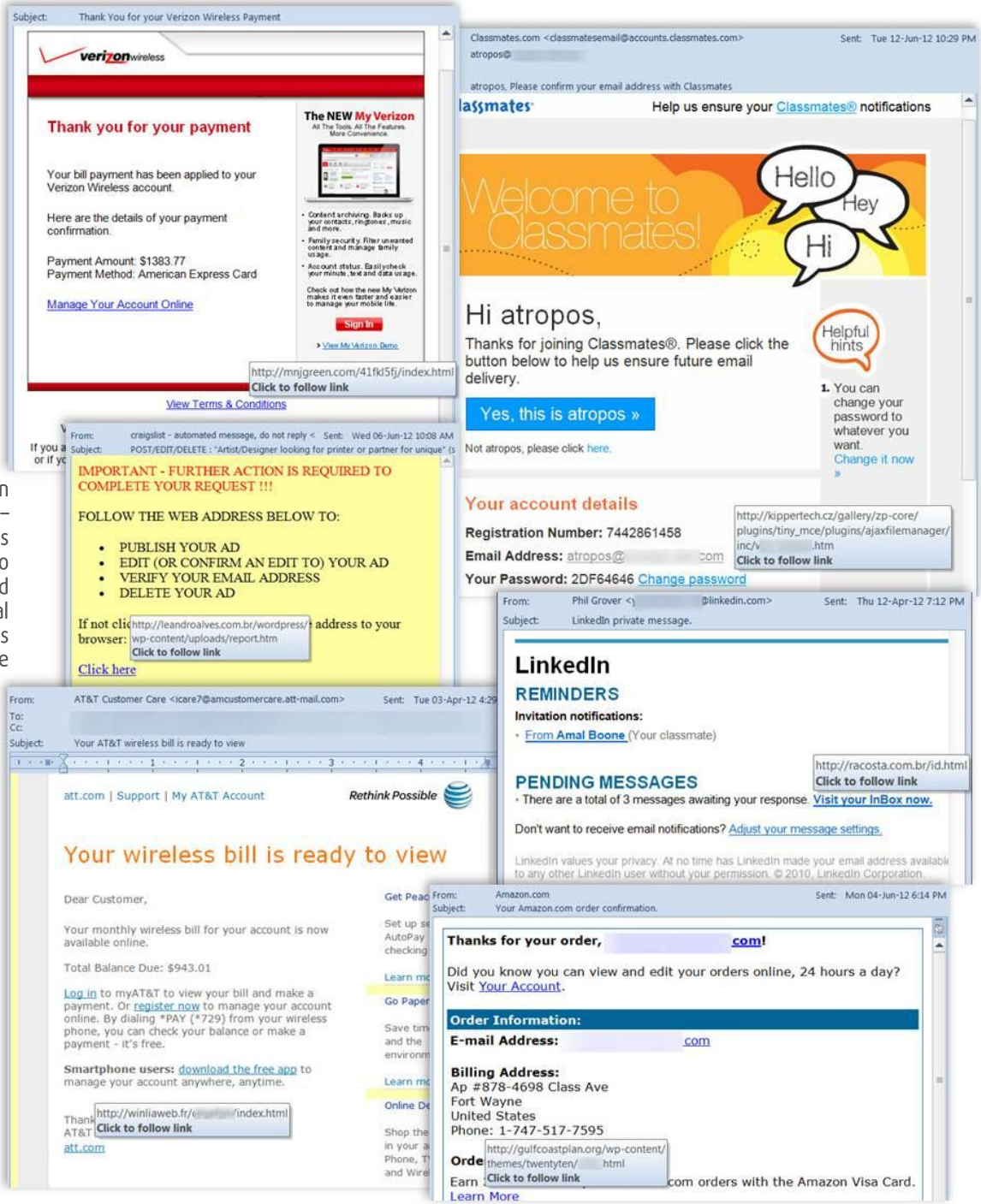
- The same Flash and Adobe Reader exploits were used in most of the malware.

The well-known brands that were abused in the various emails included the following (and other companies):

- LinkedIn – emails mixed pending LinkedIn invitations with messages awaiting response
- AT&T wireless – wireless bill summaries mentioned large account balances (over $900) with invitations to log in, register, or download apps. In some examples up to 9 links were included – all of them directing to separate compromised accounts.

- Verizon Wireless – Following the AT&T outbreak, similar emails claimed to be Verizon Wireless accounts (also with large balances).
- Classmates.com – the email thanks the recipient for joining and provides links to confirm the user or make corrections.

Well-known brands abused – links in emails are all to compromised sites – final destination loads malware



Source: Commtouch

- Amazon order confirmation – the well-crafted emails do not describe the merchandise supposedly ordered – only providing a balance with links to get more information or visit "your account".
- Citi – offering the ability to view "your Citi credit card online" with balances of several thousand dollars.
- Craigslist – the email subjects were varied and described a range of plausible sounding Craigslist posts. Links in the email promised to help complete the posting of the ad, or assist with other activities such as editing or deleting the ad.

Movie ticket hoax hides malware on Dropbox

A further example of a blended email/Web malware attack made use of well-known storage/sharing network Dropbox. The Spanish emails offered free movie tickets.

Free movie ticket offer leads to malware hidden on Dropbox

En este mes ven al cine gratis!!

Ven al cine con claro y un acompa◆ante gratis solo por este mes

Descarga tu entrada para ingresar Aqui

Se tiene que llevar la entrada impresa descargada de aqui. al centro de atencion al cliente

Condiciones de la oferta

Se ha de traer la entrada adjunta en este correo electronico impresa

Source: Commtouch

The text more or less translates to:

This month come to the cinema for free!

Come to the movies with clear and free companion only for this month

Download your entry to enter here

You have to bring the printed ticket downloaded from here. the customer service center

Offer conditions

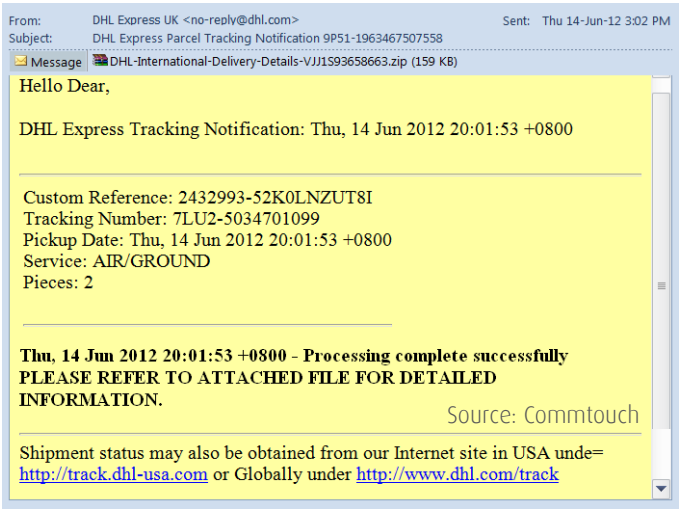
It is to bring the entry enclosed in this email print

Clicking on the links leads to several redirects and scripts, followed by the automatic download of the file "entrada_cine.zip" from the following link: https://dl.dropbox.com/u/689--025/bts/entrada_cine.zip. One of Dropbox's features allows users to create publicly available folders, which basically turns Dropbox into a free hosting site. The use of the popular service in this way provides a powerful platform for malware distribution. The downloads were eventually stopped with the following reason provided on screen – "This account's public links are generating too much traffic and have been temporarily disabled!" The file unzips an executable file of the same name with very little coverage by major antivirus engines.

Email malware

Levels of email attached malware increased in the second quarter of 2012. Attached-malware distributors once again stuck to the usual themes such as DHL/UPS delivery notices. Many attacks from this quarter featured new malware or variants of malware with very low detection rates by most AV engines at the time of the outbreak. For example, the "DHL tracking" malware attachment shown below was detected by 6 out of 42 antivirus engines shortly after the mass of emails was released.

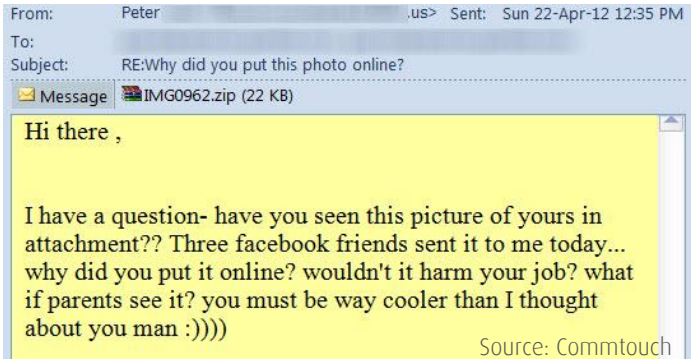
DHL tracking file unzips exe with limited AV detection



In April, a series of emails alerted the recipient about a picture of themselves (or an ex-girlfriend) that has been circulated online. Sample text from three of the messages:

> *Sorry to disturb you , – I have a question- have you seen this picture of yours in attachment?? Three facebook friends sent it to me today... why did you put it online? wouldn't it harm your job? what if parents see it? you must be way cooler than I thought about you man*

Attached malware masquerading as image file



> *Hi there ,But I really need to ask you – is it you at this picture in attachment? I can't tell you where I got this picture it doesn't actually matter...The question is is it really you???.*
>
> *Sorry to disturb you , – I got to show you this picture in attachment. I can't tell who gave it to me sorry but this chick looks a lot like your ex-gf. But who's that dude??.*

The "image" was attached to the emails for convenience and the filename in all samples was identical: "IMG0962.zip". The unzipped file displayed a PDF icon – designed to confuse

recipients whose computers do not display file extensions (the extension in this case was exe).

Top 10 Malware

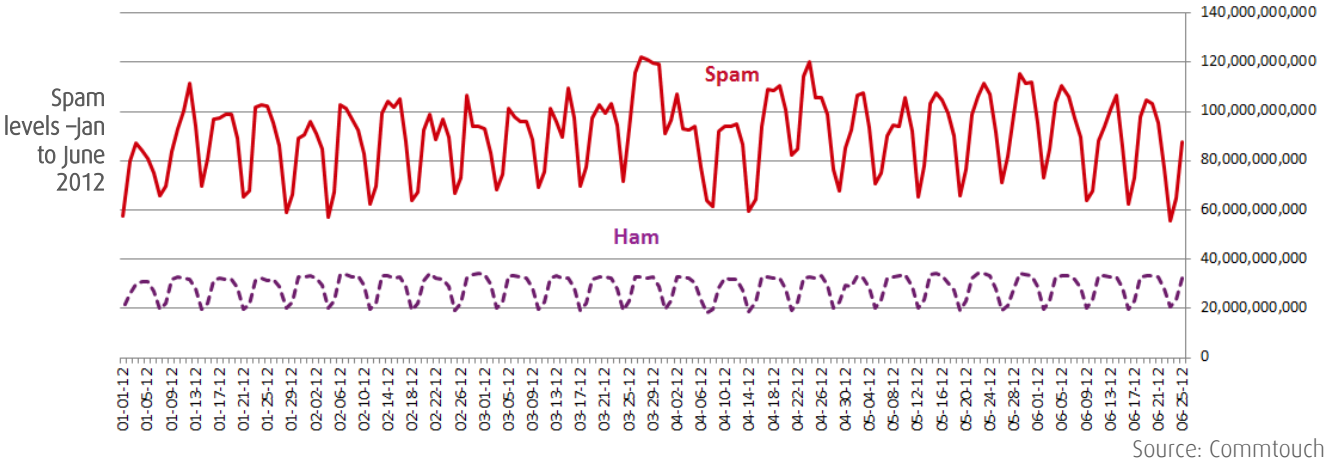
The table below presents the top 10 most detected malware during the second quarter of 2012 as compiled by Commtouch's Antivirus Lab.

Top 10 Detected Malware			
Rank	Malware name	Rank	Malware name
1	W32/RLPacked.A.gen!Eldorado	6	W32/Sality.gen2
2	W32/InstallCore.A2.gen!Eldorado	7	W32/RAHack.A.gen!Eldorado
3	W32/Sality.C.gen!Eldorado	8	W32/OnlineGames.FL.gen!Eldorado
4	W32/HotBar.L.gen!Eldorado	9	W32/Vobfus.AD.gen!Eldorado
5	W32/Heuristic-210!Eldorado	10	JS/Pdfka.EV.gen

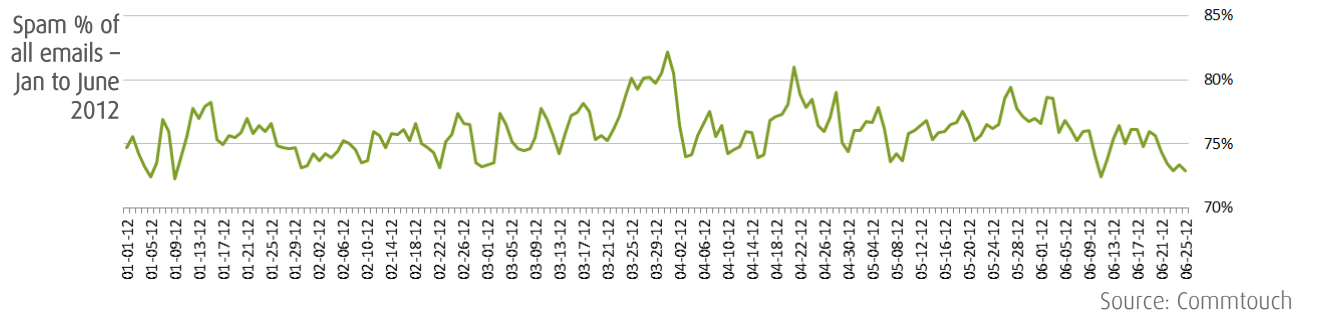
Source: Commtouch

Spam trends

Spam levels remained stable in the second quarter of 2012. The average daily level dropped slightly to 91 billion spam and phishing emails per day. Spam averaged 76% of all emails sent during the quarter, an increase of only 1% from Q1. Average levels are 20% less than the same period last year.



Source: Commtouch



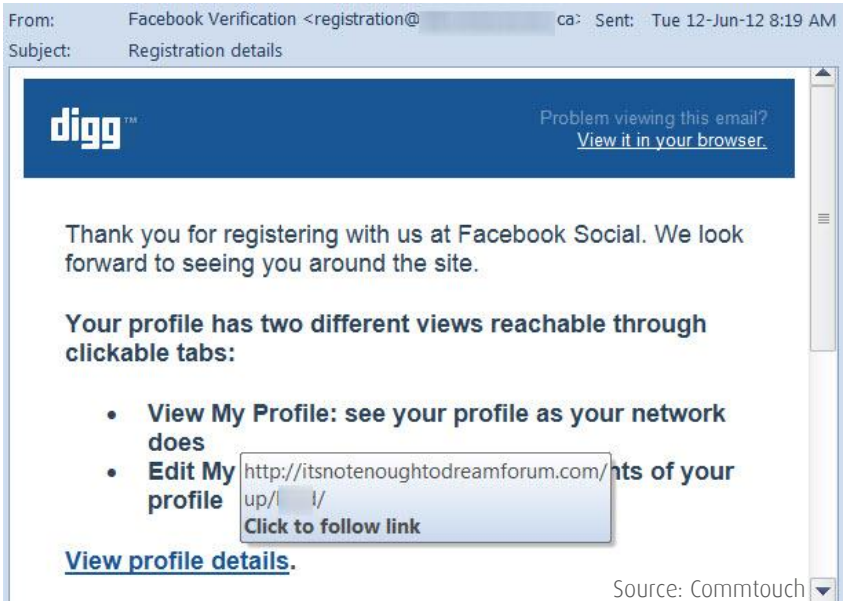
Source: Commtouch

Facebook and MySpace draw users to online pharmacies

The "spam topics" section below features the Commtouch "spam subject cloud" which shows that most spam messages are quite direct i.e.: those marketing Viagra simply include the word "Viagra" in the subject line. In order to draw other would-be customers to online pharmacy sites, spammers often resort to phony emails that trick users into clicking using clever social engineering.

In this quarter spammers created a new Facebook/Digg application called "Facebook Social". There is actually a "Facebook Social Reader" for Digg, but "Facebook Social" is a neatly confusing invention of pharmacy spammers designed to draw recipients to an online pharmacy. The description of the new service seems to have been lifted more or less from the description of the Reader. The email welcomes users to the new service and invites them to "view profile details":

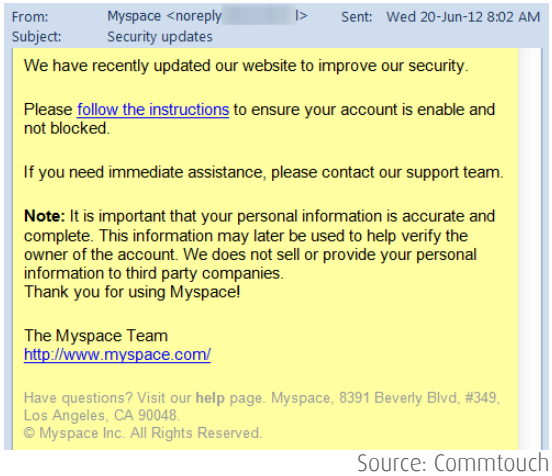
Spammers invent "Facebook Social" – links lead to pharmacy pages



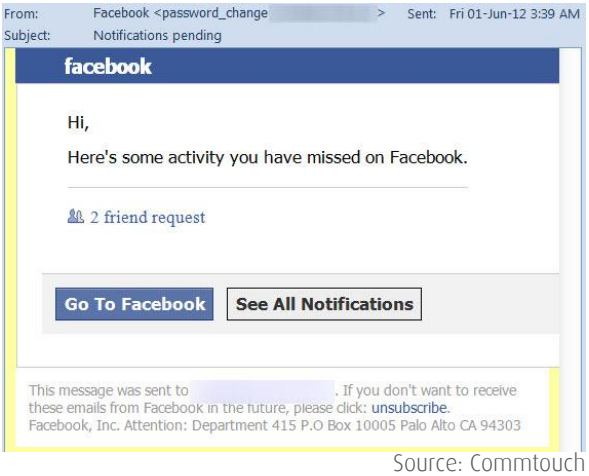
Source: Commtouch

The links in the email lead to compromised websites – in the sample above the site "itsnotenoughtodreamforum.com" has been hacked.

MySpace and Facebook notification emails lead to pharmacy websites



Source: Commtouch



Source: Commtouch

The same URL folder structure was used in a "Facebook notifications pending" outbreak, suggesting that the same spammer group was behind this attack (using the Facebook name obviously guarantees a good open-rate). The MySpace name was similarly abused to draw pharmacy clicks. Scripts hidden in the compromised sites redirect users to the destination "Wikipharmacy" or the more traditional "Toronto Drug Store"

The "Wikipharmacy" abuses well-known wiki template

Source: Commtouch

Spam Topics

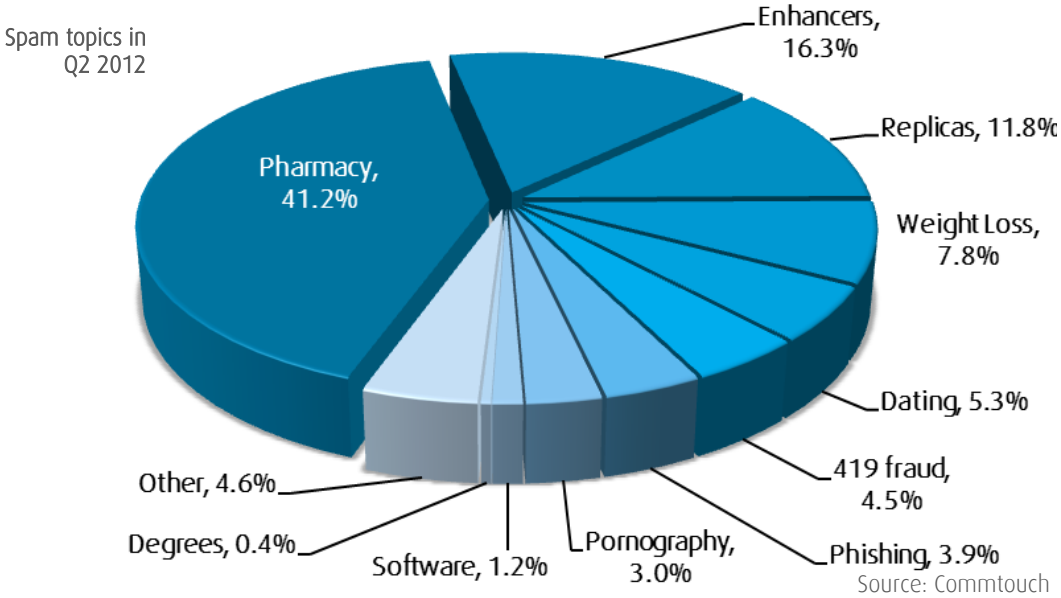
Commtouch's spam topics cloud tool samples thousands of spam messages at definable intervals and plots frequently occurring terms in proportionally larger text. Spam subjects that have been sent in massive quantities therefore become instantly distinguishable.

Spam topics cloud for Q2 2012

Source: Commtouch

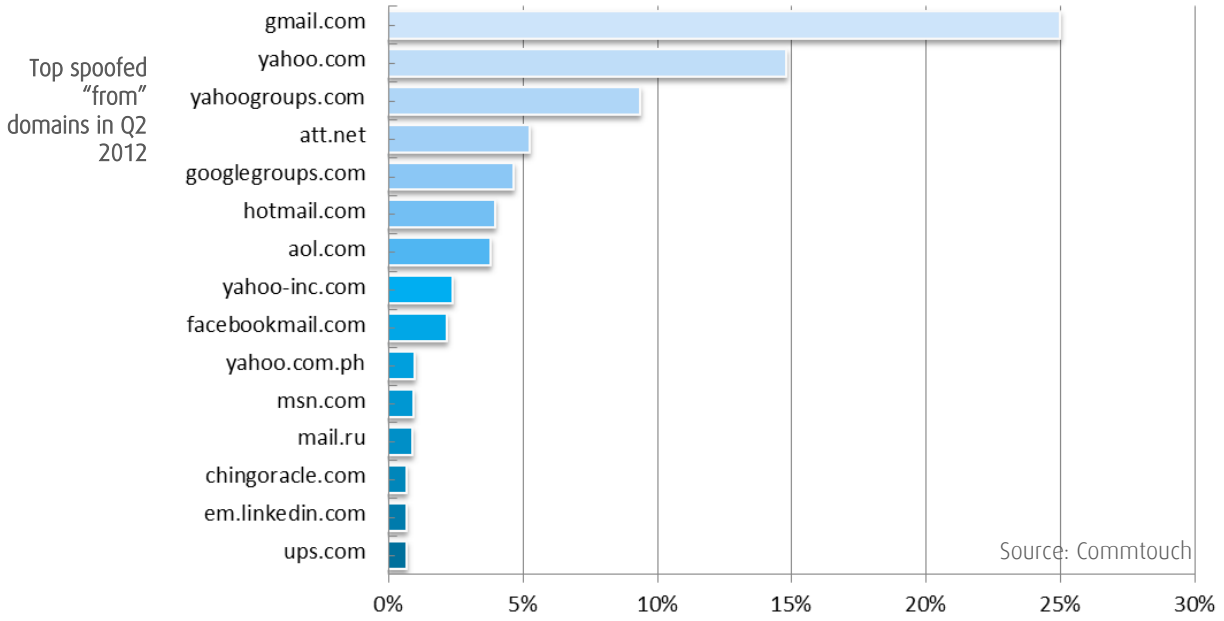
The spam cloud for the entire second quarter is shown above. Traditional spam topics such as pharmaceuticals, replicas and "enhancers" are clearly visible.

Pharmacy spam increased once again, as it has for the last few quarters, to reach over 41% of all spam (around 3% more than the previous quarter). Enhancer and diet-themed spam increased while replica spam dropped almost 8%.



Spam 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 give the impression of a reputable, genuine source.



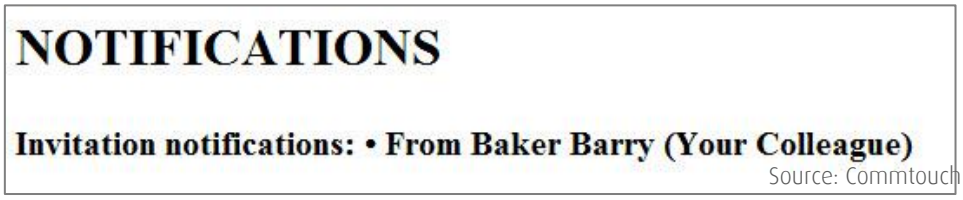
This quarter, gmail.com is once again the most spoofed domain. The top 15 features popular social networking and mail sites (AOL, Yahoo, Facebook, LinkedIn, MySpace) UPS – favored for email malware attachments – bumps DHL out of the top 15.

Web security

Compromised websites store malware

Compromised websites continued to be used extensively this quarter in many of the emails carrying malware and spam links. The hacked sites either hosted the actual spam or malware content or were used as a platform for redirection to common destination site. An example of one of the attacks is shown below. This is the screen that would be shown to anyone clicking on the links of the LinkedIn notification attacks (see page 2).

Compromised website used to host malware - message shown on screen while malware loads



Source: Commtouch

The malware loads in the background while this screen is shown. Meanwhile the host site continues to function normally.

Fully functional homepage of compromised website used to host malware

Source: Commtouch

During the second quarter of 2012, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware. Pornographic sites disappeared from the top 10 as many legitimate sites from different categories found themselves hacked and hosting malware. The ornamental plant site shown above is categorized as "business" (number 3 in this quarter up from number 9 in Q1).

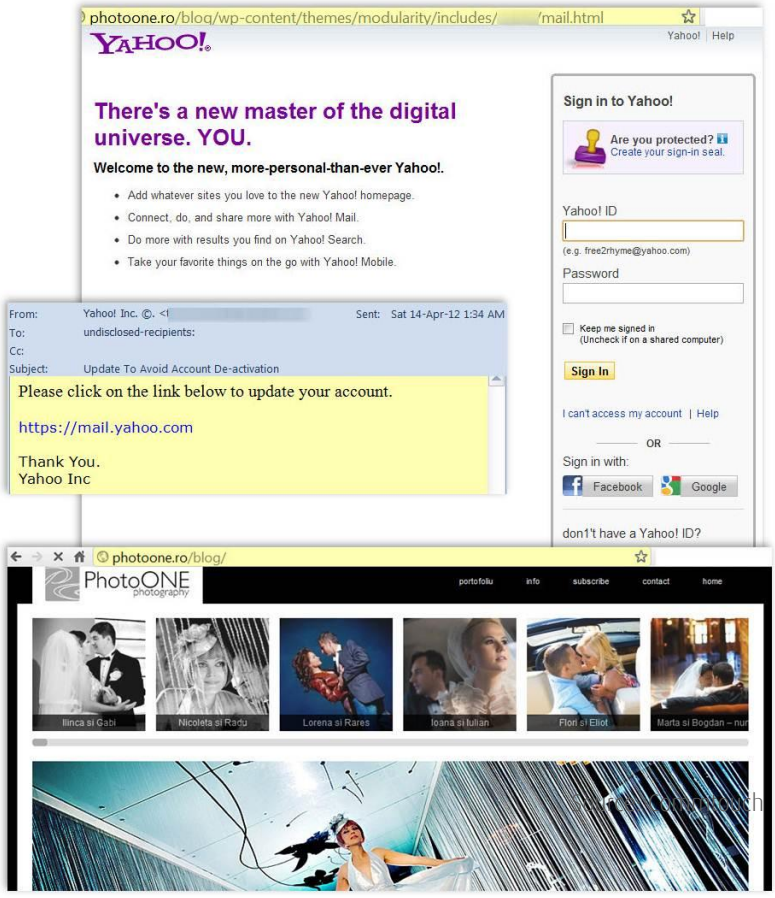
Website categories infected with malware				
Rank	Category		Rank	Category
1	Education		6	Sports
2	Travel		7	Leisure & Recreation
3	Business		8	Health & Medicine
4	Entertainment		9	Fashion and beauty
5	Restaurants and dining		10	Streaming media and downloads

Source: Commtouch

Phishing Trends

This quarter featured the usual range of phishing attacks – and, as with malware and spam, most were based on compromised websites. In the example below, perfectly formed Yahoo login pages were hidden in hundreds of hacked WordPress websites. In such cases the phishers seek out a particular plugin with a known vulnerability that can be repeatedly exploited on many sites. In the example below a Romanian photographer's website continues to function normally while the phishing page is hidden in the blog section. Once users have entered their login details (which are collected by the phisher) on the fake page, they are redirected to Yahoo Mail.

Yahoo phishing attack - and compromised site



Source: Commtouch

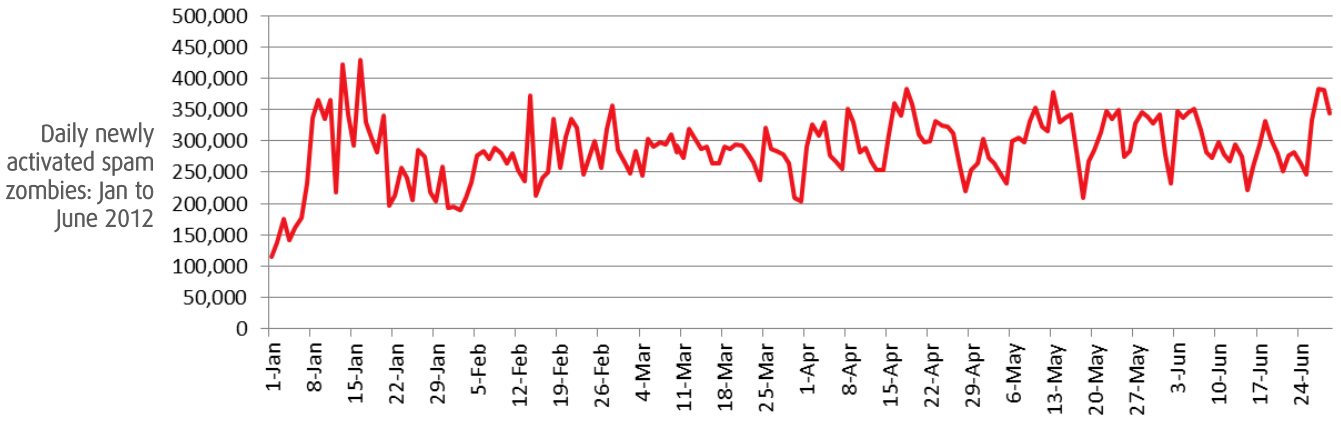
During the second quarter of 2012, Commtouch analyzed which categories of legitimate Web sites were most likely to be hiding phishing pages (as in the example above). Portals (offering free website hosting) remained at the highest position. The photography website shown above (used to host Yahoo phishing) is categorized as "business" and "arts".

Website categories infected with phishing				
Rank	Category		Rank	Category
1	Portals		6	Business
2	Fashion & Beauty		7	Arts
3	Sports		8	Streaming media and downloads
4	Shopping		9	Computers and technology
5	Education		10	Travel

Source: Commtouch

Zombie trends

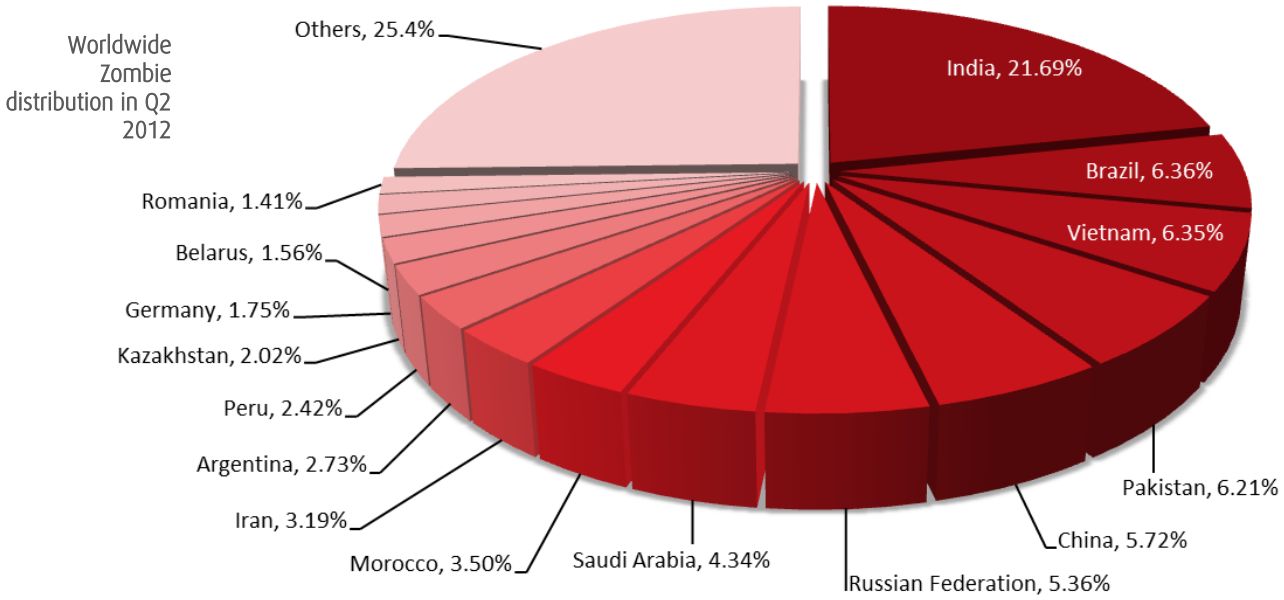
The first quarter saw an average turnover of 303,000 zombies each day that were newly activated for sending spam. This number is a slight increase over the 270,000 of the first quarter of 2012.



Source: Commtouch

Zombie Hot Spots

India again claimed the top zombie producer title, moving back over the 20% mark this quarter. Brazil, which in Q4 2011 showed some promise by dropping down to 6th place, once again holds the number 2 position. Poland, Italy, and Indonesia dropped out of the top 15, replaced by Saudi Arabia, Romania, and more surprisingly, Germany – which has stayed well out of the top 15 for over one and a half years. Almost zombie free status belongs to various Islands (Falklands, Comoros, Cook) and North Korea.



Source: Commtouch

Web 2.0 trends

Commtouch's GlobalView Cloud tracks billions of Web browsing sessions and URL requests, and its Web 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. Once again, "streaming media and downloads" was the most popular blog or page topic staying at 21%. The streaming media & downloads category includes sites with MP3 files or music related sites such as fan pages.

Most popular categories of user-generated content						
Rank	Category	Percentage		Rank	Category	Percentage
1	Streaming Media & Downloads	21%		8	Religion	4%
2	Computers & Technology	7%		9	Sports	4%
3	Entertainment	6%		10	Education	3%
4	Restaurants & Dining	5%		11	Leisure & Recreation	3%
5	Pornography/Sexually Explicit	5%		12	Health & Medicine	3%
6	Fashion & Beauty	5%		13	Games	2%
7	Arts	5%		14	Sex Education	2%

.

Source: Commtouch

About Commtouch

Commtouch® (NASDAQ: CTCH) safeguards the world's leading security companies and service providers with cloud-based Internet security services. Real-time threat intelligence from Commtouch's GlobalView™ Cloud powers Web security, email security and antivirus solutions, protecting thousands of organizations and hundreds of millions of users worldwide.

References and Notes

- 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 levels do not include emails with attached malware.
- http://blog.commtouch.com/cafe/anti-spam/spammers-invent-new-facebook-digg-application-facebook-social/
- http://blog.commtouch.com/cafe/malware/beware-the-phony-classmates-com-email/
- http://blog.commtouch.com/cafe/malware/284000-wordpress-sites-hacked-probably-not/
- http://blog.commtouch.com/cafe/anti-spam/reset-your-facebook-password-%e2%80%93-and-visit-wikipharmacy/
- http://blog.commtouch.com/cafe/email-security-news/yahoo-phishing-hides-in-compromised-wordpress-websites/
- http://blog.commtouch.com/cafe/email-security-news/have-you-seen-this-picture-of-yours-in-attachment-three-facebook-friends-sent-it-to-me-today/
- http://blog.commtouch.com/cafe/email-security-news/phony-linkedin-reminders-help-users-connect-with-malware-2/
- http://blog.commtouch.com/cafe/web-security/phony-verizon-wireless-emails-follow-att-wireless-emails-attack/
- http://blog.commtouch.com/cafe/web-security/your-att-wireless-bill-may-link-to-malware/

Visit us: www.commtouch.com and blog.commtouch.com
Email us: info@commtouch.com
Call us: 650 864 2000 (US) or +972 9 863 6888 (International)

commtouch®
Real Security. In Real Time.