Internet Threats Trend Report
October 2012

commtouch®

Internet Threats Trend Report – October 2012

In This Report

Q3 2012 Highlights

▼ **87 billion**

Average daily spam/phishing emails sent

Page 4

▲▼ **304,000 Zombies**

Daily turnover

Page 4

▲ **1.9 billion**

Average daily emails sent with attached malware

Page 3

▼ **Pharmacy ads**

Most popular spam topic (31.3% of spam)

Page 7

▼ **India**

Country with the most zombies (20%)

Page 10

▲ **Education**

Website category most likely to contain malware

Page 8

Overview

The third quarter of 2012 provided further proof of the growing menace of Android malware with attacks that exclusively targeted the Google OS. The convincingly named "update" app requires user installation but provided its distributors with a platform for a mobile Android botnet or a vehicle for theft of corporate data.

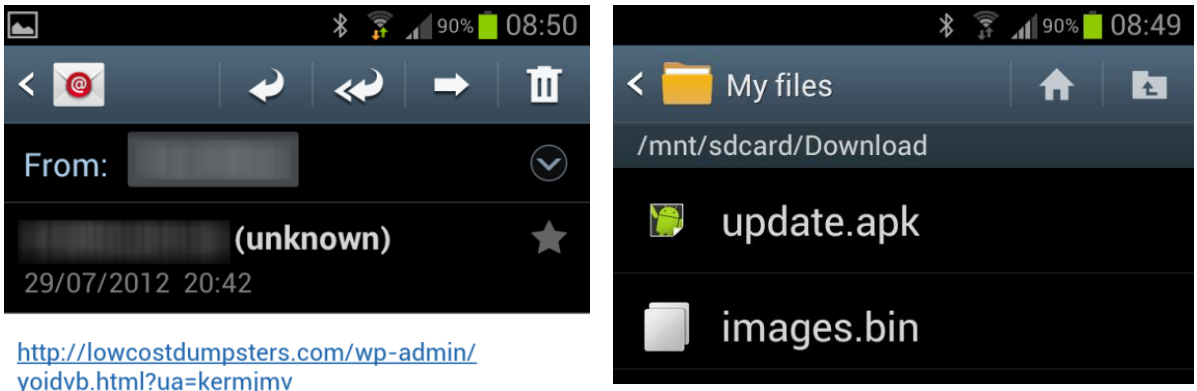
July provided yet another botnet takedown – this time the Grum spam botnet. Although spam and zombie levels appeared to drop, the effect proved to be temporary. Spammers rallied quickly to recruit new zombies and resume spam-sending operations within a matter of days.

This quarter's Trend Report also covers Olympic Games scams, careless spammers, and the "calling card" that one malware gang keeps using.

Malware Trends

Android malware

Android malware continues to grow – both in volume and in the number of variants of Trojans and viruses. Proof of Android's increasing popularity was a July attack that only targeted the Google OS. The attack made use of compromised email accounts to send simple one-link emails. In the past this method has been used to distribute links to spam products (pharmaceuticals, replicas) or links to drive-by malware downloads. In this case the malware URLs only worked for Android devices.



(Left) Email from compromised Yahoo account, and (right) download folder on Android device after clicking on email link. "update.apk" has been downloaded

Source: Commtouch

The destination Web server checked for browsers sending an Android User-agent string. The server then returned an android application, causing the Android browser to automatically download the file. Any other browser (e.g.: from Windows) would be shown a blank page or a "page not found" message.

The downloaded file "update.apk" (.apk is a packaged Android app) does not install automatically, but rather requires the user to activate the installation by touching on the filename. The file is shown in the download folder above. The filename "update.apk" is generic enough to fool many users, especially since Android routinely downloads and updates many of the apps on the device.

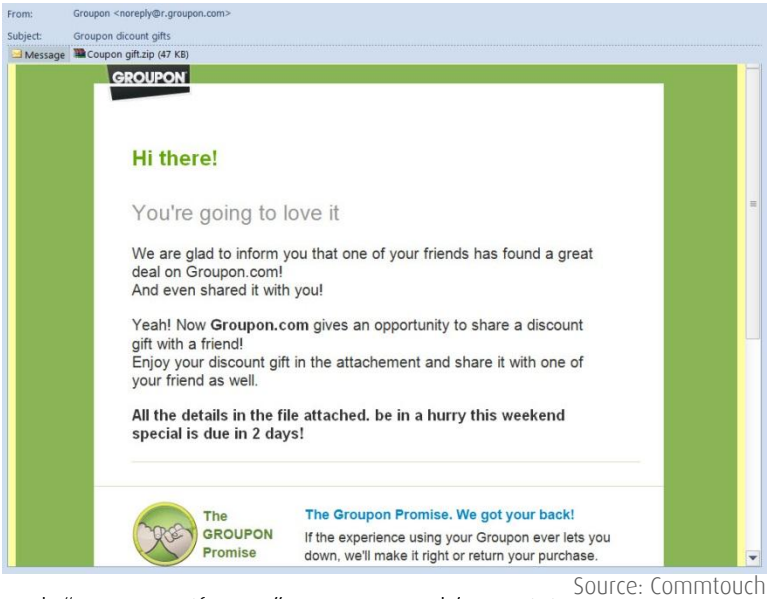
The malware only requested network permissions, so the intention was not to collect contact details, SMSs, email and other personal details. The actual functions of the Trojan were not

immediately clear – but the network permissions would have allowed it to work as a proxy to steal data from devices on corporate VPNs. Alternatively, the network access would allow communication with botnet command and control servers.

Groupon malware deals

A collection of malware emails sent out in July borrows heavily from authentic mailings sent out by Groupon and LinkedIn. The outbreak is different from the blended attacks that have featured regularly in the last few months since it relies on attached malware as opposed to a link to drive-by malware. Using email templates modeled on Groupon and LinkedIn increases the chances that recipients will consider the attachment genuine and worth opening. The example below shows a Groupon "deal" found by a friend. Recipients are invited to open the attachment to view the gift details and also to forward it on to friends. All the links within the "offer" point to genuine Groupon sites (and not drive-by malware).

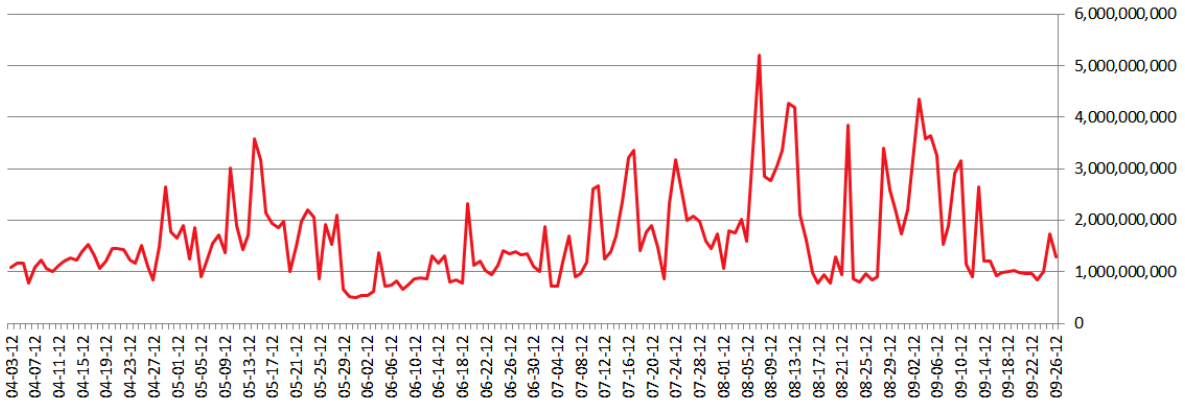
Phony Groupon offer with Attached Malware



Source: Commtouch

The attached zip file unpacks to a file named "Coupon gift.exe." Commtouch's Antivirus identifies the malware as W32/Trojan3.DWY. The malware attempts to download and install files from several remote servers. Only 30% of the 41 engines on VirusTotal detected the malware within a few hours of the attack.

Attached Malware levels – Apr to Sept 2012



Source: Commtouch

Levels of email attached malware increased in the third quarter of 2012. The average per day was around 1.9 billion emails. Attached-malware distributors generally stuck to the usual themes such as DHL/UPS delivery notices.

Top 10 Malware

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

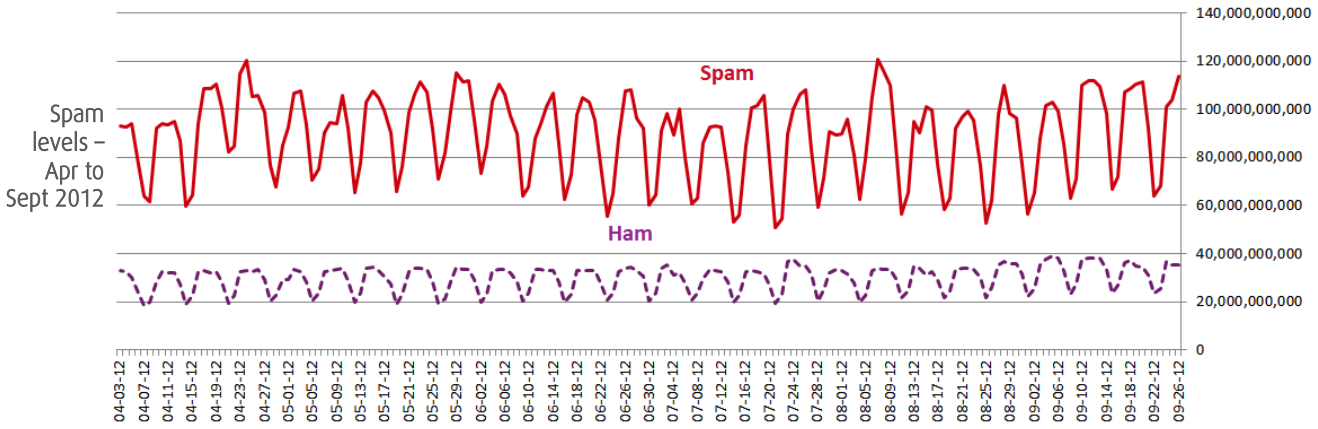
Top 10 Detected Malware			
Rank	Malware name	Rank	Malware name
1	SWF-malform-1	6	CVE-2010-3333
2	W32/Ramnit.Q	7	W32/MyWeb.D@adw
3	W32/Conficker!Generic	8	W32/Injector.A.gen!Eldorado
4	W32/Mabezat.A-2	9	W32/Mabezat.A-1
5	W32/Agent.PJ.gen!Eldorado	10	W32/Tenga.3666

Source: Commtouch

Spam Trends

Grum Botnet takedown

Near the end of July it was reported that the spam-sending Grum botnet had been taken offline. The takedown was the effort of FireEye assisted by Spamhaus, and other industry experts and network operators around the world. The takedown took around two weeks as command and control servers were taken offline and then replaced by the botnet owners. These remaining command and control servers in Russia and the Ukraine were the last to be shut down by the 22nd of the month.

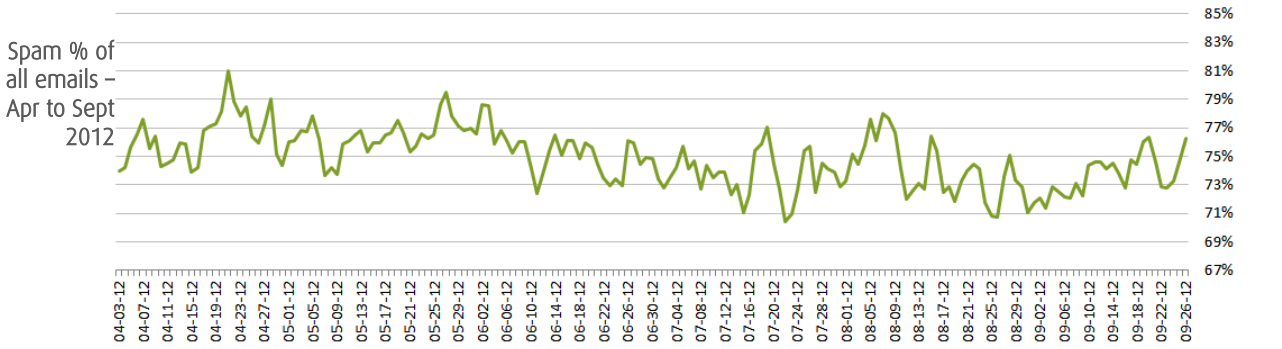


Source: Commtouch

Did the takedown have any effect on global spam levels? It is often worth waiting for one or two months before a clear trend emerges. This time period generally shows whether spammers have managed to resume their operations using other botnets. In the case of the

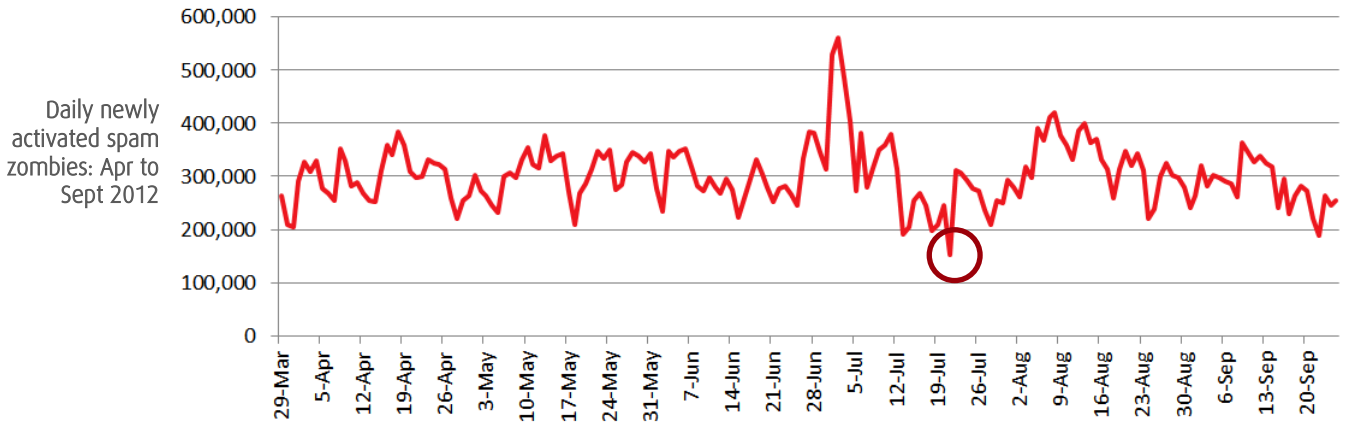
Rustock botnet takedown in March 2011, time has shown that the effects were permanent – and global spam decreased.

In the case of the Grum takedown the immediate effect was the lowest spam per single day in the last 3 years (near 51 billion messages). This effect, however, was very short-lived with spam levels returning to average numbers almost immediately. The effect of the takedown is barely visible on the daily spam levels graph (above). Spam averaged 74% of all emails sent during the quarter, a decrease of 2% from Q2.



Source: Commtouch

The effect of the takedown is visible in the daily spam zombie levels charted below. The daily zombies added on the reported day of the final takedown was the lowest of the quarter. Also visible is the ramp-up of zombies in the 2 weeks following the takedown – representing a rebuilding of botnet capabilities elsewhere.



Source: Commtouch

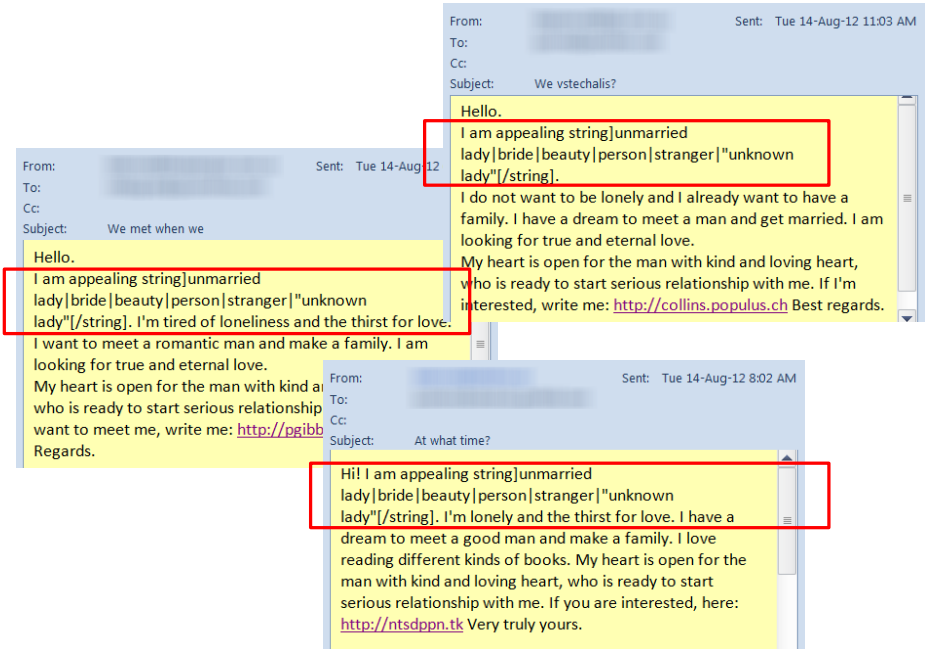
Spam Templates

Proving that spammers still work hard to outwit spam filters, a "dating" spam outbreak from August revealed how multiple emails are generated with slightly different wording. The spammers have mistakenly sent out the emails with the script language still visible. The language includes several options – the email sending bot was supposed to pick one per email:

string/ unmarried lady|bride|beauty|person|stranger|"unknown lady"/string

The remainder of the emails seems to have "worked" and includes variations of the "lonely lady" looking for a "man with a kind and loving heart."

Spammer error – email sent with template script still visible

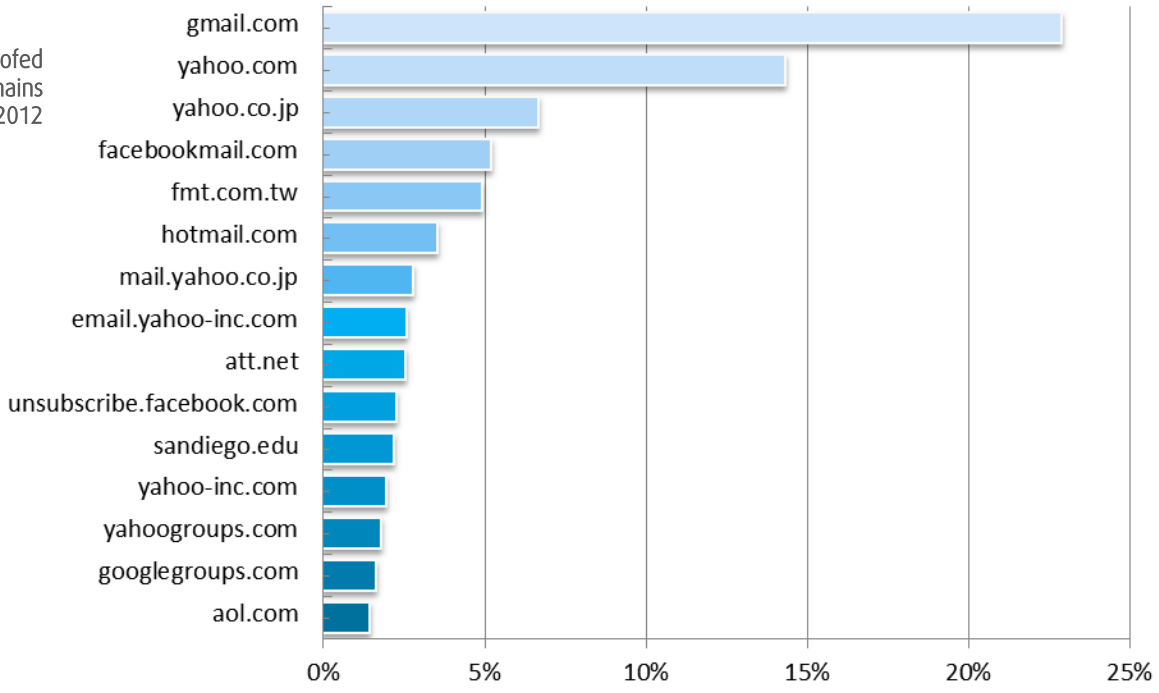


Source: Commtouch

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.

Top spoofed "from" domains in Q3 2012



Source: Commtouch

This quarter, gmail.com is once again the most spoofed domain. The top 15 features popular social networking and mail sites (AOL, Yahoo, and Facebook). Further down the list are variations of Google (google.com, google.org) and the ever-present ups.com and dhl.com still favored for attached malware attacks.

Spam Topics

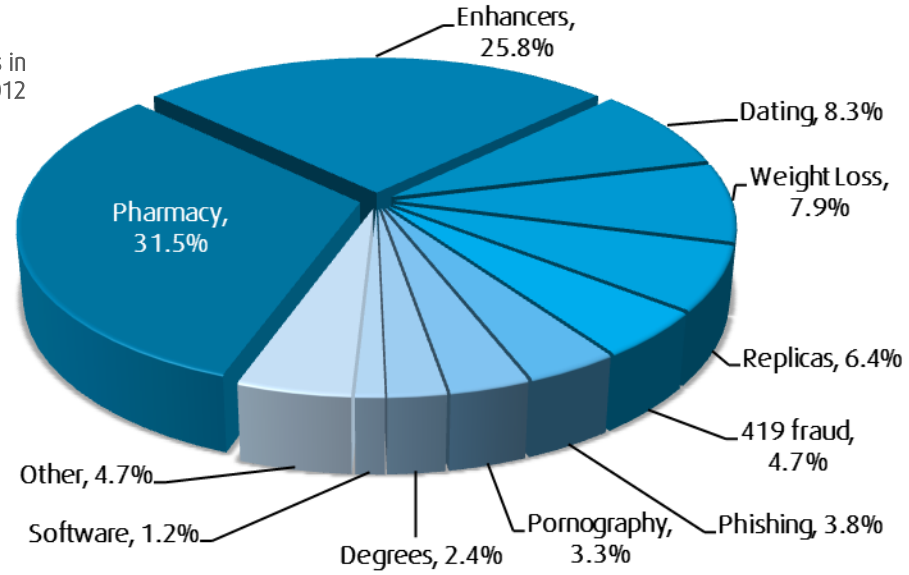
Commtouch's spam topics cloud tool samples thousands of spam messages at definable intervals and plots frequently occurring terms in proportionally larger text. Spam subjects that have been sent in massive quantities therefore become instantly distinguishable. The spam cloud for the entire third quarter is shown below. Traditional spam topics such as pharmaceuticals, replicas and "enhancers" are clearly visible.

Spam topics cloud for Q3 2012

Source: Commtouch

Pharmacy spam dropped nearly 10% this quarter but remained the most common spam subject. Enhancer spam gained almost 10% and replica themed spam dropped almost 5% to be only the 5th most popular topic.

Spam topics in Q3 2012

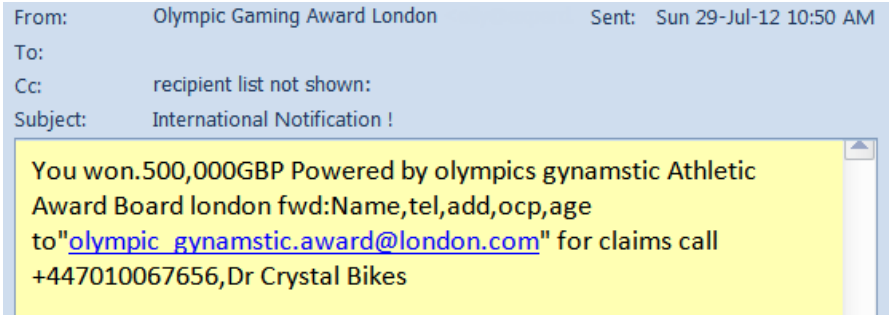


Source: Commtouch

Olympic 419s

419 (advance fee fraud) emails make up nearly 5% of emails sent. The Olympic Games (July and August) proved to be a very popular theme for 419 scams during the quarter. Most scams promised money from Olympics-related lotteries (see example below). Other emails offered Games-related merchandise for large fees or offered recipients interesting Olympic job-opportunities (in exchange for "processing" fees).

Olympic Games themed 419 email



Source: Commtouch

Web security

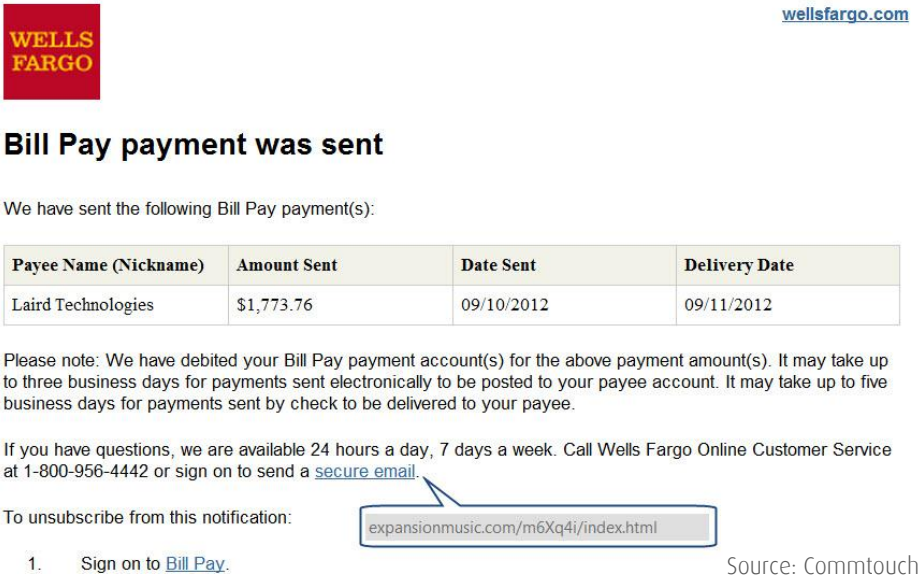
Malware campaigns use recurring Modus Operandi

Malware and spam distributors continue to make extensive use of hacked websites to host spam product pages or drive-by downloads (or redirects to these). The way these sites are abused can actually provide evidence of the activities of a particular malware gang. The repetition of attack patterns also indicates that a particular malware or spam campaign has been successful enough in the past to warrant repeating. One malware sending group is clearly happy with the method they have created which uses different social engineering themes with the same modus operandi. The process repeated several times this year generally includes the following steps:

- Hack legitimate website
- Create new subfolder with random 6 or 8-letter/number name (this is the clearest indication that the same group is at work again and again)
- Insert file "index.html" into new folder with redirect to a domain that hosts the Blackhole Exploit Kit
- Think up new theme to trick users into clicking link – usually something account/money related. Examples: Verizon Wireless, ACH transfer rejected, AT&T Wireless.

Attacks in Q3 came in the form of bill payments from Wells Fargo and payment reminders from ADP Dealer Services. All links (including the Wells Fargo "Fraud information center") follow the proven pattern: *<hacked site/6 character folder/index.html>*

Phony Wells Fargo notification with link to malware download site. Site URL follows common pattern of a particular gang.



wellsfargo.com

WELLS FARGO

Bill Pay payment was sent

We have sent the following Bill Pay payment(s):

Payee Name (Nickname)	Amount Sent	Date Sent	Delivery Date
Laird Technologies	$1,773.76	09/10/2012	09/11/2012

Please note: We have debited your Bill Pay payment account(s) for the above payment amount(s). It may take up to three business days for payments sent electronically to be posted to your payee account. It may take up to five business days for payments sent by check to be delivered to your payee.

If you have questions, we are available 24 hours a day, 7 days a week. Call Wells Fargo Online Customer Service at 1-800-956-4442 or sign on to send a secure email.

To unsubscribe from this notification: expansionmusic.com/m6Xq4i/index.html

1. Sign on to Bill Pay.

Source: Commtouch

The Blackhole Exploit Kit, in the form of obfuscated JavaScript on the final destination page, assesses the exploitable versions of various browsers and add-ons and executes appropriate payloads that start a process of downloading further malware onto the victim's computer.

During the third quarter of 2012, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware. The top 10 is summarized in the table below.

Website categories infected with malware				
Rank	Category		Rank	Category
1	Education		6	Restaurants & Dining
2	Shopping		7	Travel
3	Sports		8	Health & Medicine
4	Business		9	Streaming Media & Downloads
5	Entertainment		10	Leisure & Recreation

Source: Commtouch

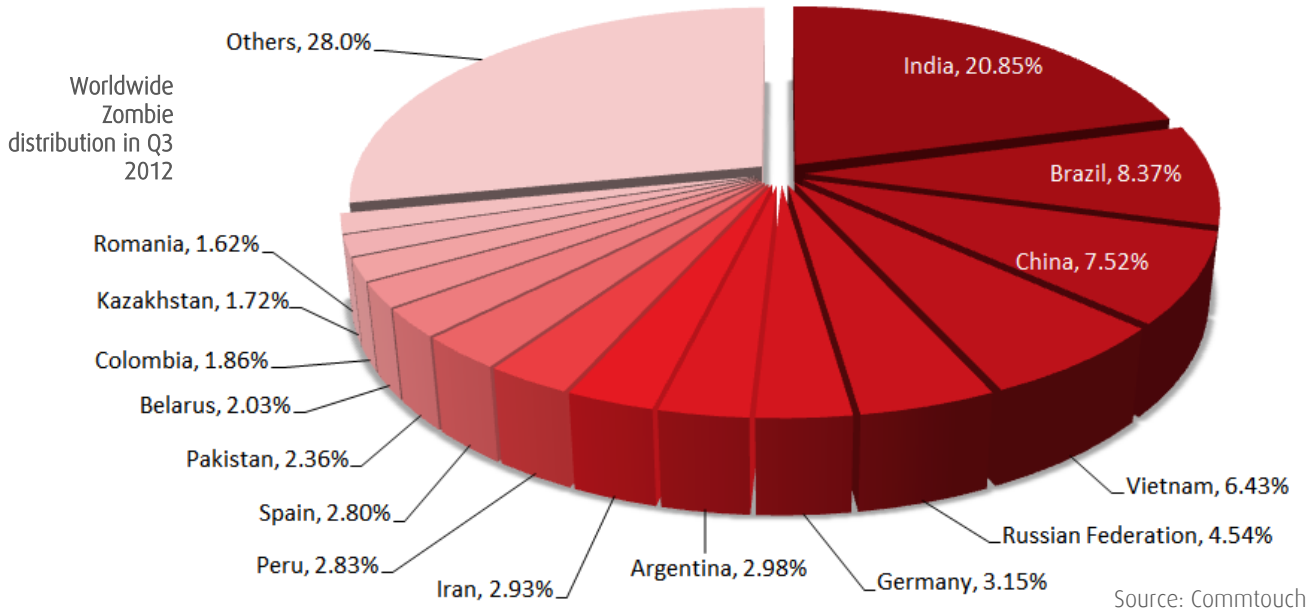
Similarly, the table below summarizes the categories of legitimate Web sites that were most likely to be hiding phishing pages. The "Portals" category represents free webpage services which are easily abused to host phishing pages.

Website categories infected with phishing				
Rank	Category		Rank	Category
1	Portals		6	Real Estate
2	Education		7	Leisure & Recreation
3	Arts Sports		8	Travel
4	Shopping		9	Computers & Technology
5	Business		10	Health & Medicine

Source: Commtouch

Zombie Hot Spots

India still hosts over 20% of the world's spam sending zombies. Germany – which returned to the top 15 last quarter, moved up to 6th place. Morocco and Saudi Arabia dropped out of the top 15, replaced by Spain and Colombia.



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/data-and-research/measuring-the-success-of-a-malware-campaign-2/
- http://blog.commtouch.com/cafe/email-security-news/your-friend-has-shared-a-groupon-malware-coupon-with-you/

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.