# Internet Threats Trend Report
# April 2013

commtouch®

# Overview

The first quarter of 2013 saw a significant growth in unwanted and dangerous emails with a significant spike in levels occurring in March. The spike affected spam and phishing as well as malware emails. Pump and dump spam made a massive comeback. Spammers and particularly malware senders increasingly exploited current news events in their campaigns. In Web security, the first quarter of 2013 saw extensive use made of the Blackhole exploit kit.

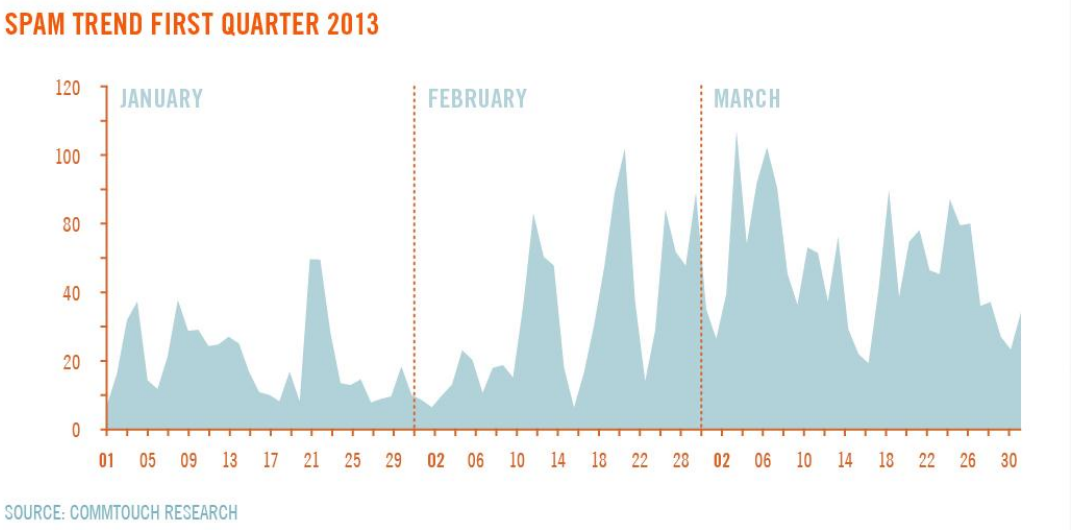
# Email security

## Spam and malware-email volumes

The first quarter of 2013 saw a significant growth in unwanted and dangerous emails with a significant spike in levels occurring in March. Spam, malware and phishing volumes all climbed compared to the previous quarters with the lowest growth rate being 74 percent.

During the first quarter of 2013, an average 97.4 billion spam emails and 973 million malware emails were sent worldwide each day. In March, the number of daily spam emails even significantly exceeded the 100 billion mark (117.8 billion).

Spam volumes almost doubled, increasing by 98.0 percent compared to the end of the previous quarter. The increase was 36.5 percent in March alone, compared to March of 2012 spam levels were 47.7 percent higher. This also lead to a higher share of spam among the entire email volume. In March 2013 78.1 percent of all email were spam. This is a significant increase from January when the spam share was as low as 60 percent.




Similar increases were registered with respect to email-borne malware. In March 2013, the volume of known malware rose by 75.1 percent compared to February, 157.1 percent compared to December and 255.5 percent in comparison to March 2012. Virus outbreaks increased by 124.0 percent in relation to February volumes, by 290.5 percent since December and by 251.5 percent compared to the same month the year before. The increase in phishing

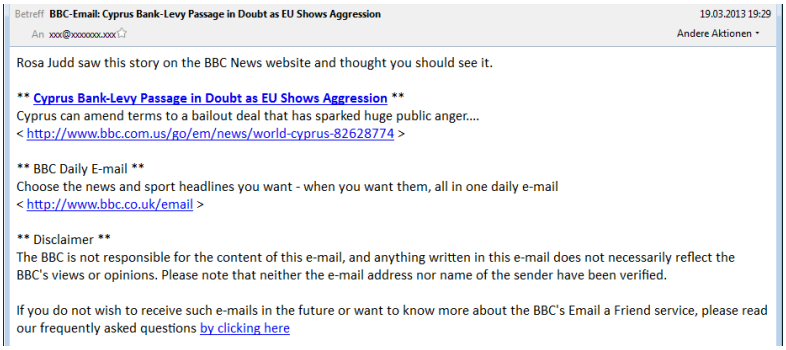
levels somewhat slowed in March (8.1 percent since March), but overall the quarter saw a 73.8 percent increase.

Overall, email-borne malware had a share of 4.5 percent of all emails sent in March 2013, while phishing emails were just below 0.1 percent. In March 2013, clean e-mails had a share of 11.5 percent, legitimate bulk e-mails (e.g. newsletters) were at 3.9 percent.

## Spam trends

Event spam is on the rise again but with a twist: Increasingly, spammers use the current news topics of the day to lure recipients into opening messages or clicking on links. The election of Pope Francis was a major such event in March. Spam message pretended to come from trustworthy news organizations such as CNN or BBC News and promised exclusive news relating to the new pope. The links contained in the messages often led to drive-by malware sites. A day later, the same messages appeared this time containing headlines relating to the financial crisis in Cyprus. It appears that the spammers have found an alt least semi-automatic way of inserting current news into prepared messages in order to make them more appealing.


Event spam examples: New Pope election, Cyprus financial crisis

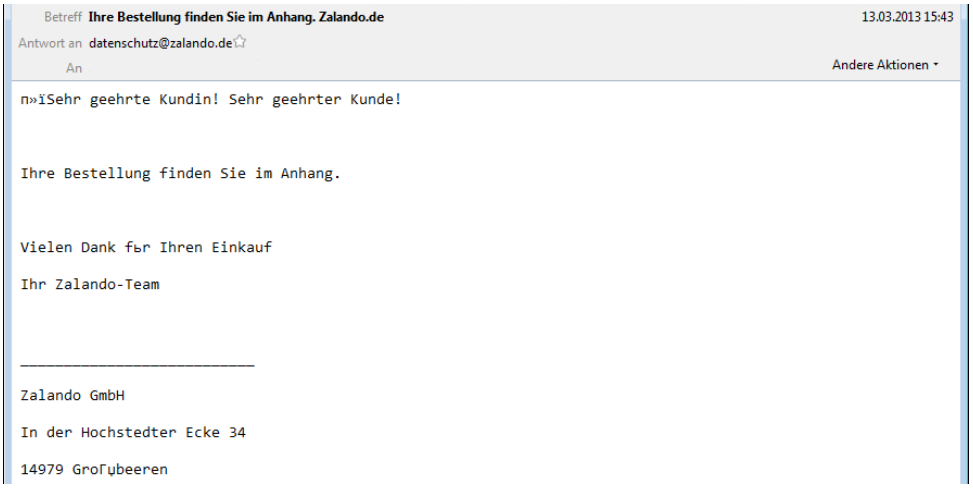



Another trend observed in the first quarter is the use of new and at times extremely strange topics in spam emails. A particularly interesting example was a large German-language spam wave, distributed over several days in late January and early February and which seemingly advertised an information Web page dedicated to strawberry farming. The emails contained no links, attachments or any particular offers. Their purpose might have been to test spam filters in order to get information valuable for future "real" spam campaigns.

## Email-malware trends

Localized email-malware campaigns are becoming the cybercriminals' favourite tools. For example, Commtouch's German-based Eleven Research Labs again discovered various malware campaigns using emails written in German as well as German brand names and alleged senders. Two of the three largest malware email campaigns targeted at German users in March were localized campaigns pretending to come from the German online flight booking site flugladen.de and from a German air cargo company, respectively. Other large waves pretended to be coming from the hugely popular online clothes and shoe shop Zalando or from the hotel booking site hotel.de. These emails contained attachments which carried malware, usually a Trojan.

Phony Zalando order email with attached malware



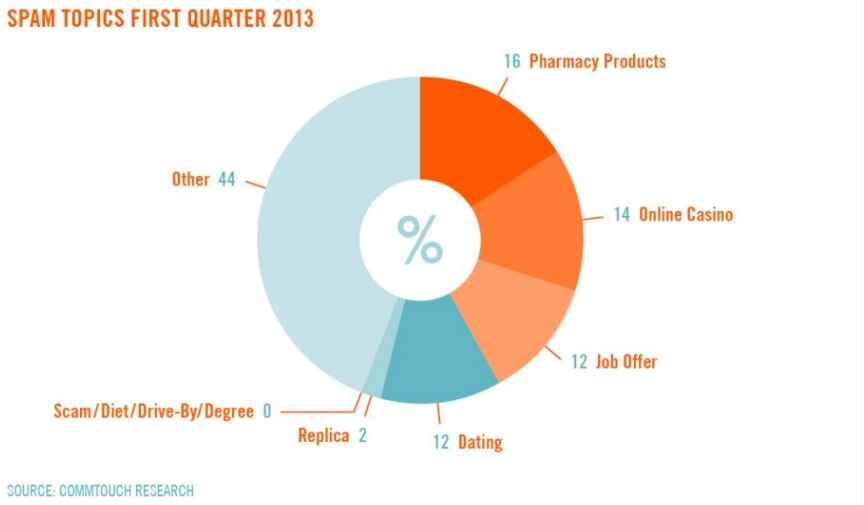

These campaigns are representative of a general trend: Cybercriminals increasingly target specific markets, hoping to significantly increase opening and infection rates by giving the emails a legitimate and, to the recipient, seemingly relevant appearance. This is achieved by exploiting popular brands and sites and using language-specific email texts. Currently this is largely confined to larger markets, such as Germany, but it is likely to spread to smaller ones if the success of such campaigns matches their originators' expectations.

The favorite method of luring recipients into opening mail attachment remains fake orders, confirmations, invoices, etc. The emails pretend that the recipient has placed an order, is sent an invoice, etc. which is attached and it is urgent that he look at it. If these emails are allegedly sent from popular companies or service providers, the better known or more critical (e.g. mobile phone companies) the apparent sender, the more plausible the story the better.

## Spam Topics

The biggest change in the first quarter of 2013 was the re-emergence of pump and dump or penny stock spam. This was a favourite spam topic until about five years ago before it all but disappeared. These emails advertise cheap shares with very small trading volumes, indicating there was significant earning potential in them. The trick: If only a few recipients can be fooled into buying the stock, the value will rise significantly and the spammers cash in. This kind of spam has become a significant part of overall spam volumes. In March 2013, 18 percent of the top 25 spam mailings (with a combined volume of 46 percent of all spam) were pump and dump mailings, among them the two biggest spam waves in March. This is not the first time in recent years old tricks have been recycled by spammers hoping current-generation spam filters would not catch them. Because of its absence in recent years, stock spam is not a separate topic category recognized by the Commtouch Labs but it was a major factor in the "other" category gaining a 53.0 share in March 2013 and 43.4 percent in all of Q1.

The first quarter of 2013 witnessed a further decline in "classic" spam topics. In Q1, pharmacy spam topped the list with a share of just 16.3 percent of the entire spam volume – a meager number compared to the 50, 60 percent it used to have regularly in the past. Online casinos dropped to 14.1 percent, dating spam to 11.7 percent and replica watches fell to just above 1 percent (1.4 percent), 419 scams hat a share of 0.4 percent. One of the "winners" were illegal job offers ("money mule spam") which reached a share of 12.1 percent.

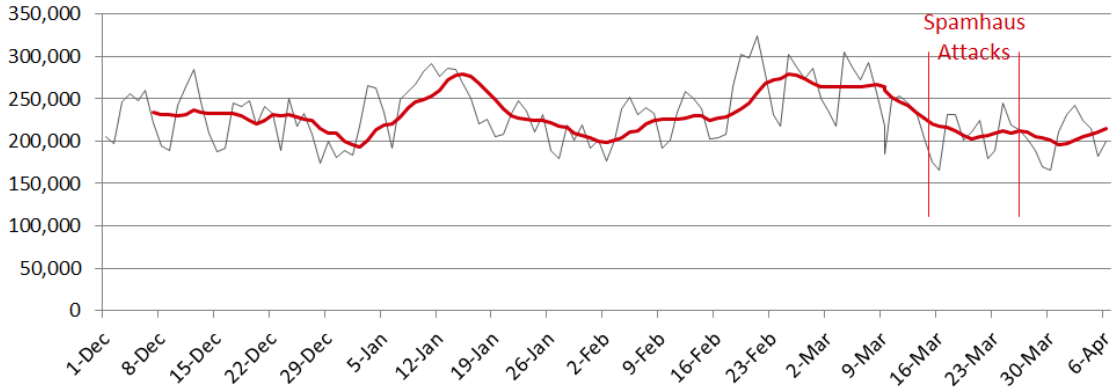



# Zombie trends

## Spamhaus DDOS Attacks

Spamhaus – who maintain several popular IP and URL blacklists, were targeted in a large distributed denial of service attack in late March. Spamhaus took steps to minimize the effect of the attacks and it seems that service was minimally affected. Reports suggested that the attack was the work of one or more organizations who resented their inclusion in one or more of the Spamhaus blocklists. This theory is supported by Commtouch's zombie levels monitored during the attack. As shown in the graph below the number of zombies activated daily did not change significantly during the 3rd week of March. It therefore seems unlikely that a spam-sending group was trying to disrupt Spamhaus operations while simultaneously building their bot infrastructure.

Dec 2012 to Apr 2013: Spam Zombies activated each day

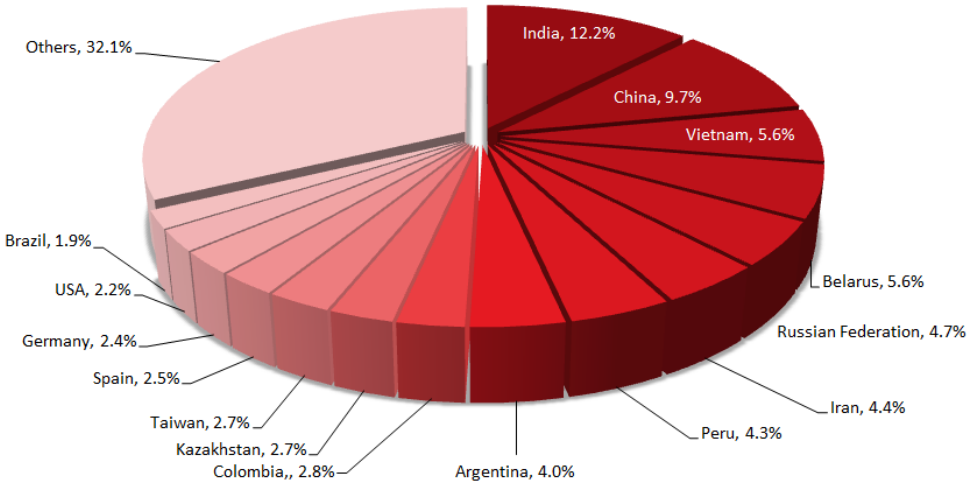



## Zombie countries

During the first quarter of 2013, India took the zombie crown once again. 12.2 percent of all spam sending bots used Indian IP addresses, followed by China (9.7 percent), Vietnam, Belarus (5.6 percent each) and the Russian Federation (4.7). Again, zombie distribution was dominated by Asia (the top three and five out of the top ten), South America (three) and Eastern Europe (two). Remarkable was the absence of Western industrialized nations from the top ten with

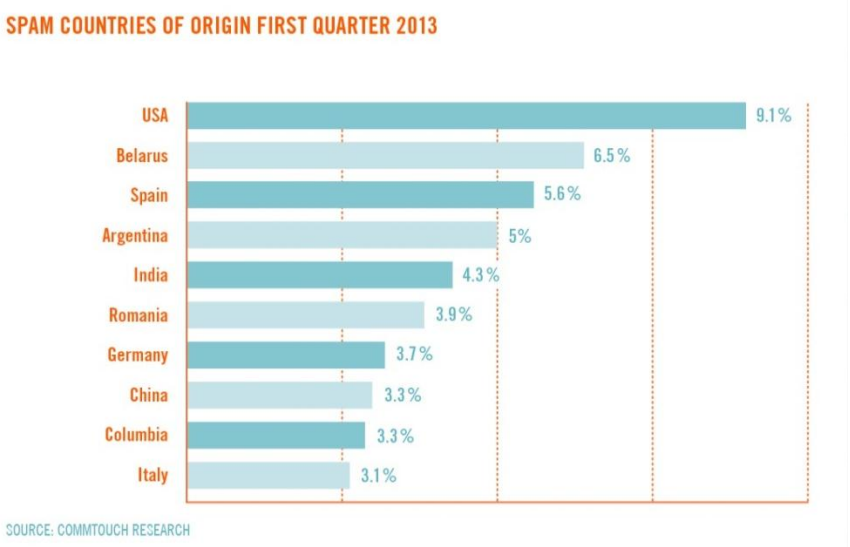
Germany coming in at number 13 and the United States dropping to number 14. Despite the strong concentration of spam sending bots in South America in recent years, Brazil, has now dropped to 1.9 (place 15).

Most spam zombies per country – Q1 2013




## Spam countries of origin

The top countries in zombie distributions are also the top sources of spam emails, although the actual order of the ranking varies. Particularly interesting is the significantly greater role the United States plays: they topped the list of Spam-sending IPs in the first quarter with a 9.1 percent share of the overall spam volume. Unusual were also the high spam levels emanating from Spain who were number three in Q1 (5.6 percent). One of the rising spam sources was Belarus who placed second at 6.5 percent. The top five were completed by Argentina (5.0 percent) and India (4.3 percent). Brazil's disappearance from the zombie top ten was mirrored in the spam top ten list: The geographical distribution was similar to the zombie list: In Q1, the top ten consisted of two countries from Eastern Europe, two from Asia and two from South America. Different was the presence of Western, Central and Southern Europe (three) as well as North America (one).



# Phishing

The popular online payment service PayPal has emerged as the most popular target in phishing scams. More than half of all phishing emails detected in March 2013 targeted PayPal users. Just as in the cases of spam and malware, the trend to localize campaigns is on the increase when it comes to phishing. While PayPal is popular with phishers all over the world, phishing attacks are increasingly targeted to users in specific countries. Again, there were significant German-language phishing emails abusing the PayPal brand name. When it comes to content and goals, there is little new: Credit card and banking data is still the number one target, the favorite method remains the pretense of limiting or denying access to the user's account which can only be restored after entering his data into a Web form.

# Scams

419 scams (also known as "Nigerian scams") are alive and well. Long gone are the days when obscure Nigerian princes needed help with their money. The new generation of scam emails exploits current news stories, preferably those related to events in the Middle East. At the height of the upheavals in Egypt and Libya, there were plenty of emails allegedly seeking help with rescuing large amount of money from the countries. Among the "senders" were close relatives of former leader Mubarak and Gaddafi. In the first quarter of 2013, new campaigns appeared relating to the anniversary of the Libyan uprising.

Libyan 419 scam email

My name is Linda; I am the daughter of Richard J. Williams an American but based in UK and Libya. My father is a crude Oil business man and he has his oil block and oil services company in Libya.

He died last year in Libya during the Gadhaffi crises because he was there when the crises erupted but due to the UN no fly zone order, he was not able to fly out of Libya again and unfortunately, he was shot by the Gadhaffi forces because he is an American and he died a day after I spoke with him in the hospital.[tears!!!!]

I am 16 years of age and an undergraduate, raised by my father as a single parent so my father's untimely death has devastated me and I have suffered a lot of problems because I am not able to locate any one that relates him. Please bear with me that I don't hear clearly but I seriously need help from you as the environment I am is not friendly again. My father's friends are now seeing me as a pest and are not welcoming again; some ask for sex before they could help me.

Please I am seeking your consent to assist me especially in the area of moving me out of this place to a new environment where I will forget about this pains and continue my education because my father wanted me to be a medical doctor and I love it and before his death, he told me

Not surprisingly, current events in Syria are currently exploited by scammers. This time, the money to be saved, does not come from the rulers but from a U.S. (!) soldier claiming to have found it – a trick already used in relation to Libya. How successful these scams still are, is difficult to evaluate, however, the fact that they still exist and are constantly adapted and re-invented suggests that there still is money to be made.

# Mobile security

Android malware continues to be generated in high numbers. March saw continued use of an attack method first seen in mid-2012. The main elements of the attack are:

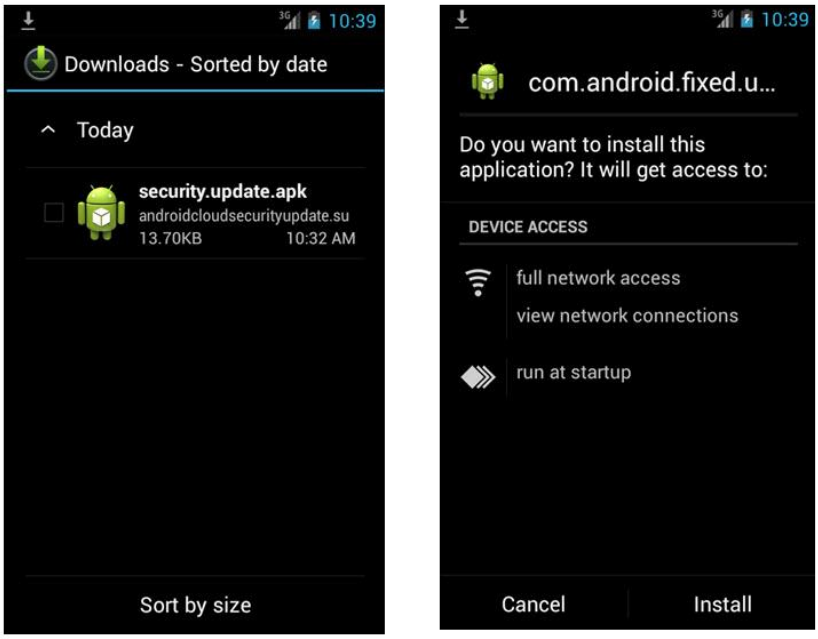
- Single link emails sent from the compromised Yahoo accounts
- Links lead to compromised websites which redirect to "distribution sites"
- Distribution sites direct the visitor based on the browser type
- PC visitors sent to diet scam pages
- Android visitors sent to malware download page

The emails, received from a legitimate Yahoo user, look like this:

Compromised Yahoo account sends link


In this case the site "thedivschool.com" is a legitimate website (teaching life insurance classes) that has been hacked. The hacked website redirects to a distribution website. The distribution website has a hidden iframe that detects what kind of device is accessing the webpage. If the device accessing the webpage uses an android browser the user is redirected to a site and the code is injected through the device browser. The Android device then automatically downloads the malware (security.update.apk). The .apk extension describes a packaged Android app.

Android device – download of "security.update.apk" malware




The downloaded Android file "security.update.apk" 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 – detected by Commtouch's Antivirus as AndroidOS/NotCom.A – acts as a proxy so it's able to transmit and receive network data through the infected android device. This means it can steal all kinds of sensitive data sent or received through the device network connection. Alternatively, the network access could allow communication with botnet command and control servers.

If the browser accessing the distribution site is from a PC then the browser is redirected to a diet scam site.

# Web security

During the first quarter of 2013, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware – such as the examples in the discussion of the Blackhole exploit below. The top 10 is summarized in the table below.

| Website categories infected with malware | | | | |
|---|---|---|---|---|
| Rank | Category | | Rank | Category |
| 1 | Education | | 6 | Health & Medicine |
| 2 | Business | | 7 | Transportation |
| 3 | Travel | | 8 | Leisure & Recreation |
| 4 | Sports | | 9 | Pornography/Sexually explicit |
| 5 | Entertainment | | 10 | Free Web Pages |

Similarly, the table below summarizes the categories of legitimate Web sites that were most likely to be hiding phishing pages.

| Website categories infected with phishing | | | | |
|---|---|---|---|---|
| Rank | Category | | Rank | Category |
| 1 | Free Web Pages Portals | | 6 | Shopping |
| 2 | Education | | 7 | Travel |
| 3 | Computers & Technology | | 8 | Real Estate |
| 4 | Business | | 9 | Streaming Media |
| 5 | Sports | | 10 | Health & Medicine |

The first quarter of 2013 saw extensive use made of the Blackhole exploit kit. The kit is installed on target websites allowing the installation of drive-by malware. The kit works as follows:

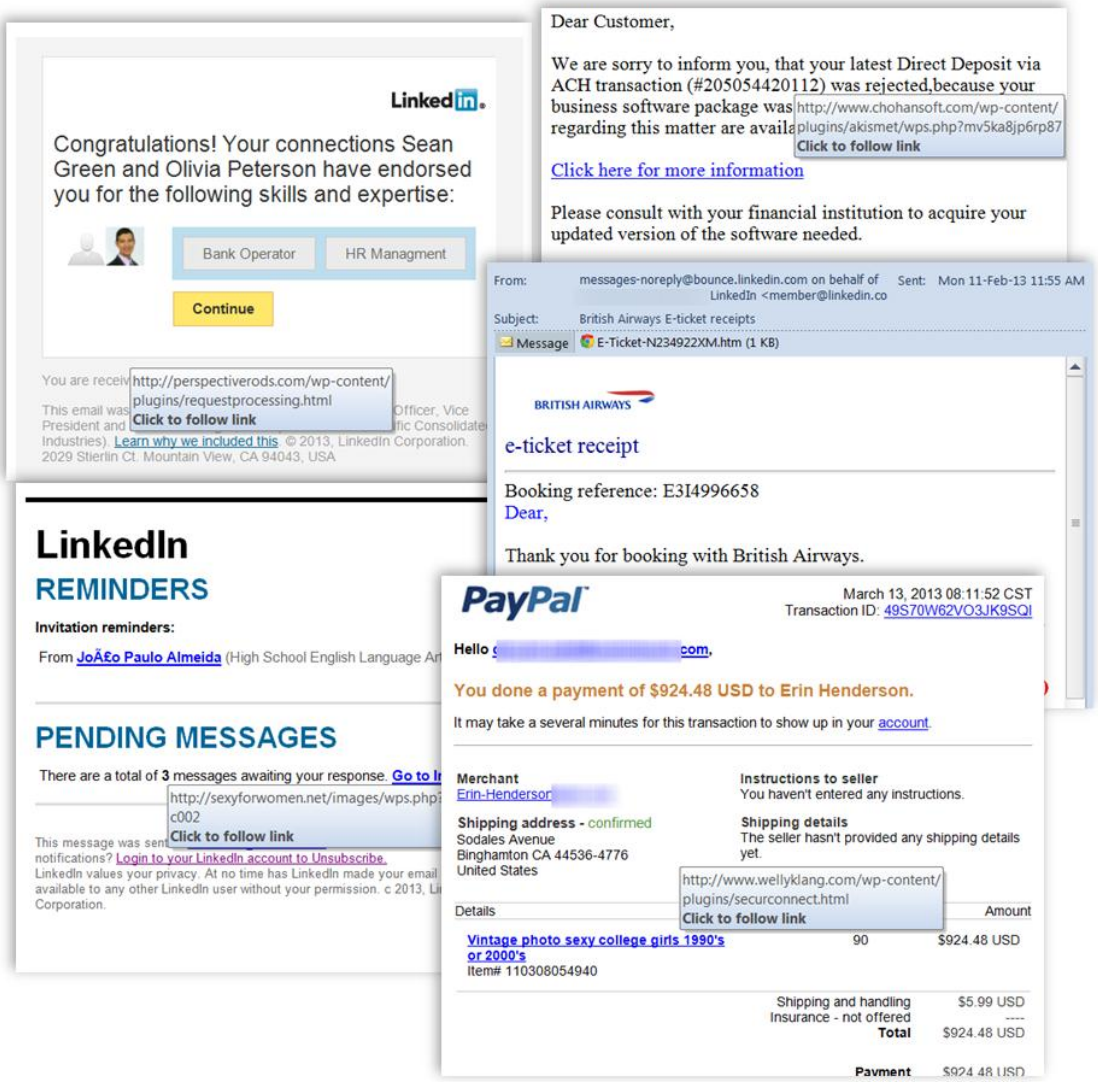
- The JavaScript on the page scans the visiting system to determine the versions of popular and operating system software such as Adobe Flash, Adobe Reader, Java, Windows, and browsers.
- Once the kit has determined that there is vulnerability – for example, in an older version of Adobe Flash found on the visiting system – the relevant exploit is loaded allowing the controller to gain a foothold on the infected system.

- Finally the Blackhole controller, having gained control of the visitor, can now deliver further malicious content. This could include a wide range of badware such as fake AV, ransomware, or logging software to steal banking and Web credentials.

A range of emails were used to drive recipients to Blackhole hosting sites:

- Pope-related as described above
- ACH or NACHA payment details
- PayPal notifications
- LinkedIn invitations and notifications
- British Airways e-tickets – the attached html files simply redirect users to the Blackhole site.

Emails with links to Blackhole exploit kit



# About Commtouch

Commtouch® (NASDAQ: CTCH) is a leading provider of Internet security technology and cloud-based services for vendors and service providers, increasing the value and profitability of customers' solutions by protecting billions of Internet transactions on a daily basis. With six global data centers and renowned technology, Commtouch's email, Web, and antivirus capabilities easily integrate into customers' products and solutions, keeping more than 350 million end users safe. To learn more, visit http://www.commtouch.com/.

# 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.
- https://blog.commtouch.com/cafe/malware/compromised-yahoo-accounts-spread-android-malware/
- https://blog.commtouch.com/cafe/email-security-news/election-of-new-pope-used-as-lure-in-malware-attacks/
- http://www.eleven-securityblog.de/2013/03/die-neuen-spam-wellen-tagesaktuell-zur-malware/
- http://www.eleven-securityblog.de/2013/03/falsche-zalando-bestellung-und-flugladen-de-buchungen-enthaltenen-trojaner/
- http://www.eleven-securityblog.de/2013/02/die-zahl-des-monats-februar-2013/

Visit us: www.commtouch.com and blog.commtouch.com
Email us: sales@commtouch.com
Call us: Americas: +1-650-864-2000, EMEA: +49-30-5200-560
APAC: +972-9-863-6888



commtouch®
Real Security. In Real Time.