Internet Threats Trend Report

October 2013

commtouch®

Overview

The third quarter of 2013 saw further use of real-time malware campaigns that used topical news items to draw in victims. The time between the news event and the attack has been steadily decreasing throughout the year and now averages only 22 hours. Campaigns in Q3 used news of royal baby Prince George, NSA whistleblower Edward Snowden, and the Syria crisis.

The number of phishing sites increased dramatically during Q3 by almost 35%. PayPal phishing sites alone accounted for approximately 750 new phishing sites each day.

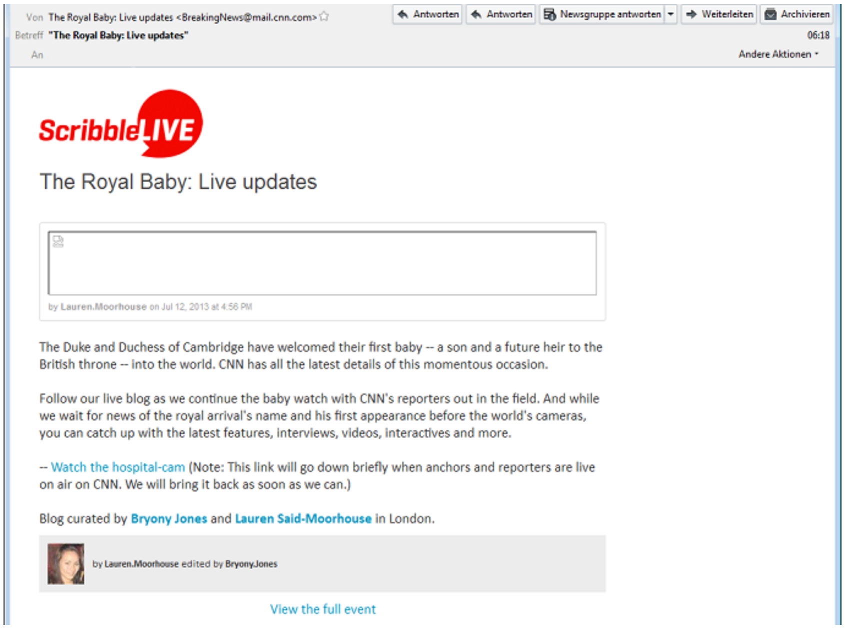
Further report highlights: Spam levels continued to drop (69 billion messages vs. 83 billion messages in Q2); Diet spam was still the leading spam topic; India remains the world's top zombie hoster.

Malware Trends

Real-Time Malware Campaigns

The third quarter of 2013 continued a trend which could already be seen in the first half of the year: the use of current news events to distribute malware, as well as the fast, probably at least semi-automatic adaptation to the latest breaking news which Commtouch has named "real-time malware-campaigns."

A campaign at the end of July focused on the arrival of royal baby Prince George. Within hours of the news, malware campaigns were initiated to exploit the huge interest. Between Tuesday, July 23, and Wednesday, July 24, Commtouch Security Labs observed eight drive-by malware waves with "The Royal Baby: Live updates" as the topic. Almost one third of the emails came from zombies in the United States, followed by Peru and Chile.



Von The Royal Baby: Live updates <BreakingNews@mail.cnn.com>
Betreff "The Royal Baby: Live updates"
An
06:18

The Royal Baby: Live updates

by Lauren.Moorhouse on Jul 12, 2013 at 4:56 PM

The Duke and Duchess of Cambridge have welcomed their first baby -- a son and a future heir to the British throne -- into the world. CNN has all the latest details of this momentous occasion.

Follow our live blog as we continue the baby watch with CNN's reporters out in the field. And while we wait for news of the royal arrival's name and his first appearance before the world's cameras, you can catch up with the latest features, interviews, videos, interactives and more.

-- Watch the hospital-cam (Note: This link will go down briefly when anchors and reporters are live on air on CNN. We will bring it back as soon as we can.)

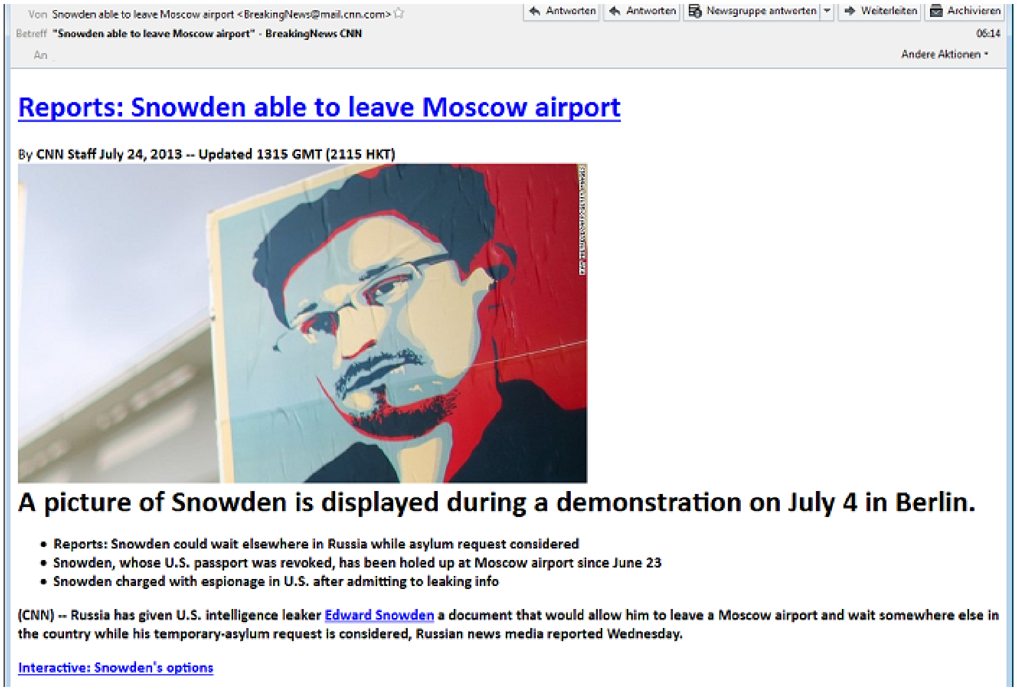
Blog curated by Bryony Jones and Lauren Said-Moorhouse in London.

by Lauren.Moorhouse edited by Bryony.Jones

View the full event

Fake Royal Baby News Alert

Another campaign focused on whistleblower Edward Snowden. Shortly after the "Royal Baby waves," very similar emails were discovered containing subject lines such as "Snowden able to leave Moscow airport – BreakingNews CNN." The emails promised exclusive news about the NSA whistleblower's asylum status. They also contained a short teaser paragraph – apparently taken from CNN – and a link for further details and interactive material.



Von Snowden able to leave Moscow airport <BreakingNews@mail.cnn.com>
Betreff "Snowden able to leave Moscow airport" - BreakingNews CNN 06:14
An

Reports: Snowden able to leave Moscow airport

By CNN Staff July 24, 2013 -- Updated 1315 GMT (2115 HKT)

A picture of Snowden is displayed during a demonstration on July 4 in Berlin.

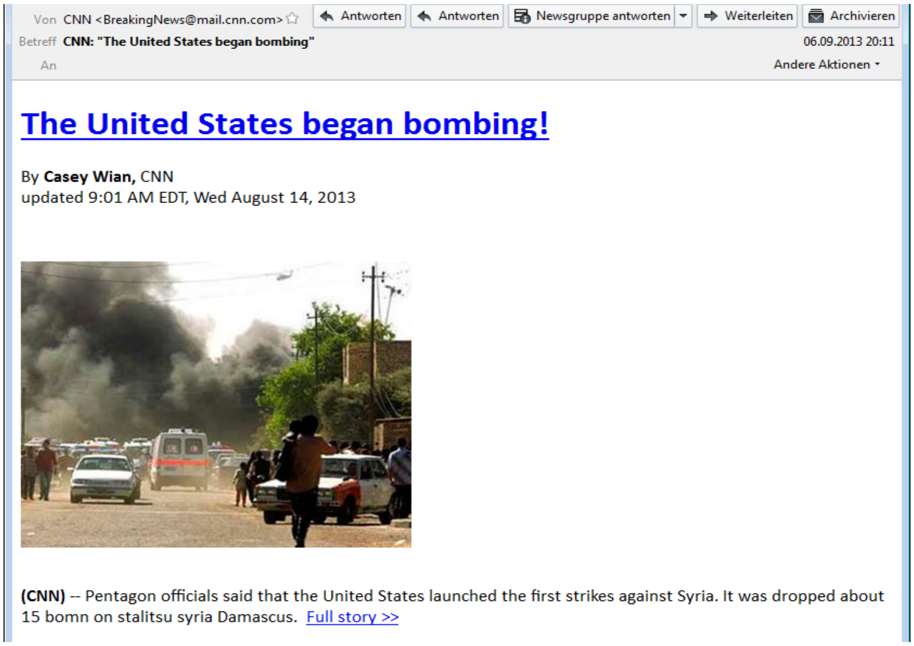
- Reports: Snowden could wait elsewhere in Russia while asylum request considered
- Snowden, whose U.S. passport was revoked, has been holed up at Moscow airport since June 23
- Snowden charged with espionage in U.S. after admitting to leaking info

(CNN) -- Russia has given U.S. intelligence leaker Edward Snowden a document that would allow him to leave a Moscow airport and wait somewhere else in the country while his temporary-asylum request is considered, Russian news media reported Wednesday.

Interactive: Snowden's options

Real-Time Campaign on Edward Snowden.

On Friday, September 6, malware distributors actually invented fake news designed to take advantage of public interest in the possibility of a U.S. airstrike against Syria. The emails used the subject line, "The United States Began Bombing," and were crafted to appear as a legitimate CNN news alert.



Von CNN <BreakingNews@mail.cnn.com>
Betreff CNN: "The United States began bombing" 06.09.2013 20:11
An

The United States began bombing!

By **Casey Wian**, CNN
updated 9:01 AM EDT, Wed August 14, 2013

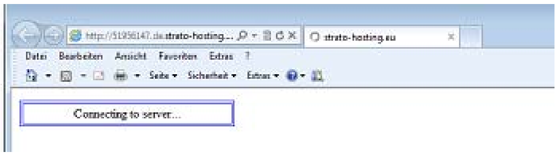
(CNN) -- Pentagon officials said that the United States launched the first strikes against Syria. It was dropped about 15 bomn on stalitsu syria Damascus. Full story >>

Fake News Alert in the Name of CNN on Syria Conflict

As for the trend on these real-time campaigns: They're getting faster. Prior to the Syria-related example, the average start time for a virus attack was already decreasing. In March 2013, when the new Pope was elected, the first malware attacks began after 55 hours. In April 2013, after the Boston Marathon bombing, it took 27 hours to see the first related attacks exploiting interest in the event. Further examples include the above mentioned newborn royal baby and news about NSA whistleblower Edward Snowden. But examples such as the recent Syria-related campaign in September show that spammers are not waiting around – they are becoming even faster than the events themselves.

Web Malware

The campaigns described above use email to reach targets, but embed the malware in drive-by downloads that are usually redirected from compromised websites. The royal-baby emails led to sites with three hidden links leading to malware-infected sites. The script "<turncoat.js>" activated the Blackhole Exploit Kit in the background – without the user noticing. The only visible item on the page was a message saying "Connecting to server…" The Blackhole Exploit Kit, one of the cybercriminals' favorite tools these days, scans the target system and then downloads the malware most appropriate to it depending on the OS, browser type, Flash version, PDF reader version, etc.



Connecting to server...

"Connecting to server…"

The number of malicious websites listed in Commtouch's GlobalView URL database saw a small decrease of 5% in Q3. The categories of websites that were most likely to be compromised with malware are summarized in the table below.

Website categories infected with malware

Rank	Category		Rank	Category
1	Travel		6	Education
2	Transportation		7	Search Engines & Portals
3	Business		8	Arts
4	Sports		9	Restaurants & Dining
5	Leisure & Recreation		10	Real Estate

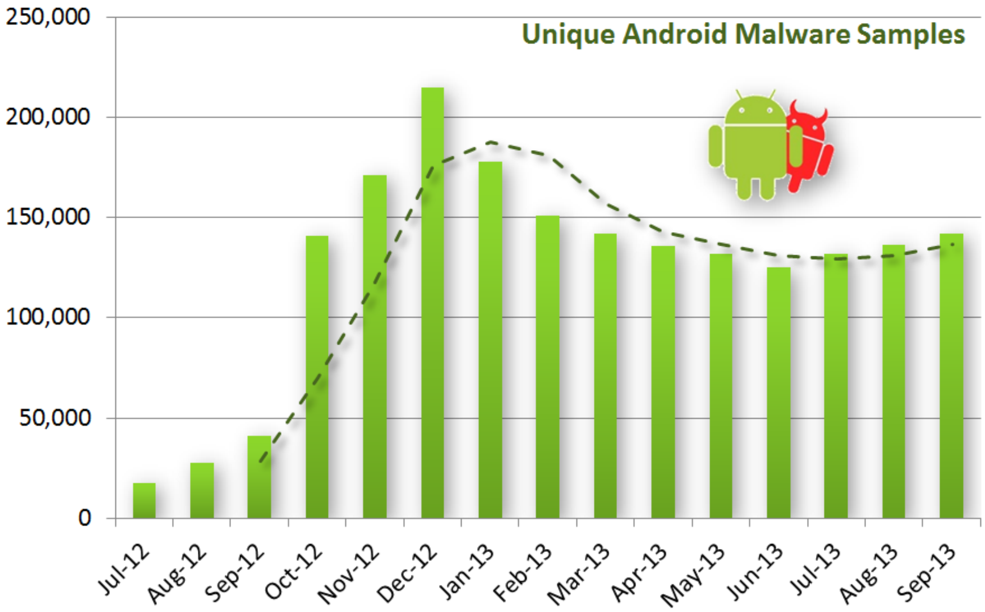
Mobile Malware

After dropping at the start of the year, the amount of unique Android malware tracked by Commtouch's Security Labs continued to gradually increase during Q3. The top 5 most commonly seen Android threats as detected by Commtouch's Mobile Security for Android included:

- AndroidOS/AirPush.A.gen!Eldorado
- AndroidOS/Plankton.A.gen!Eldorado
- AndroidOS/Leadbolt.B
- AndroidOS/Wooboo.A.gen!Eldorado
- AndroidOS/FakeDoc.H

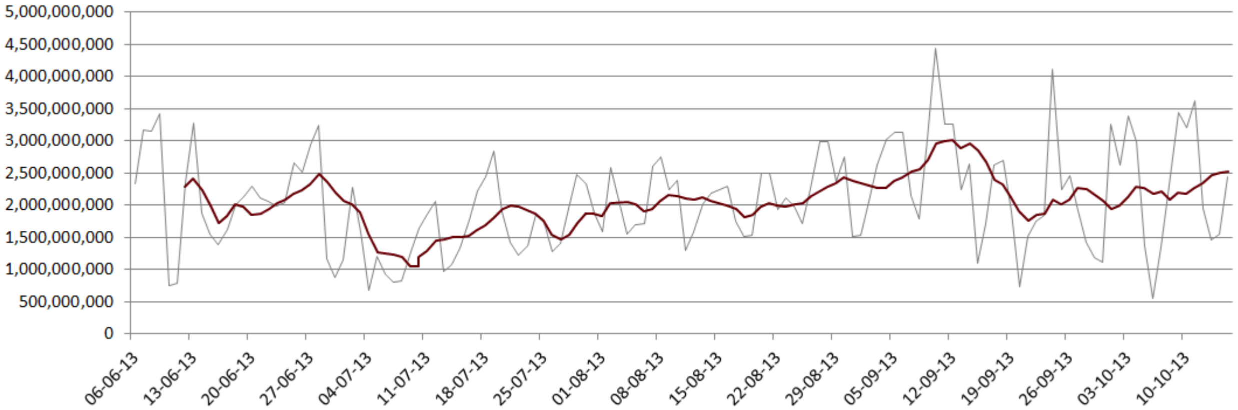
Three of the top 5 (AirPush, Leadbolt, and Wooboo) are adware, capable of collecting information about the phone and user as well as displaying ads in the notification area without user consent.

Plankton and FakeDoc are potentially more damaging Trojans. Both connect to remote servers and can download and install further malware. Plankton can set the browser homepage and bookmarks and also create application shortcuts that will download apps costing the user money. Additionally, the device information that is collected can be used to clone the user device.



Email Malware

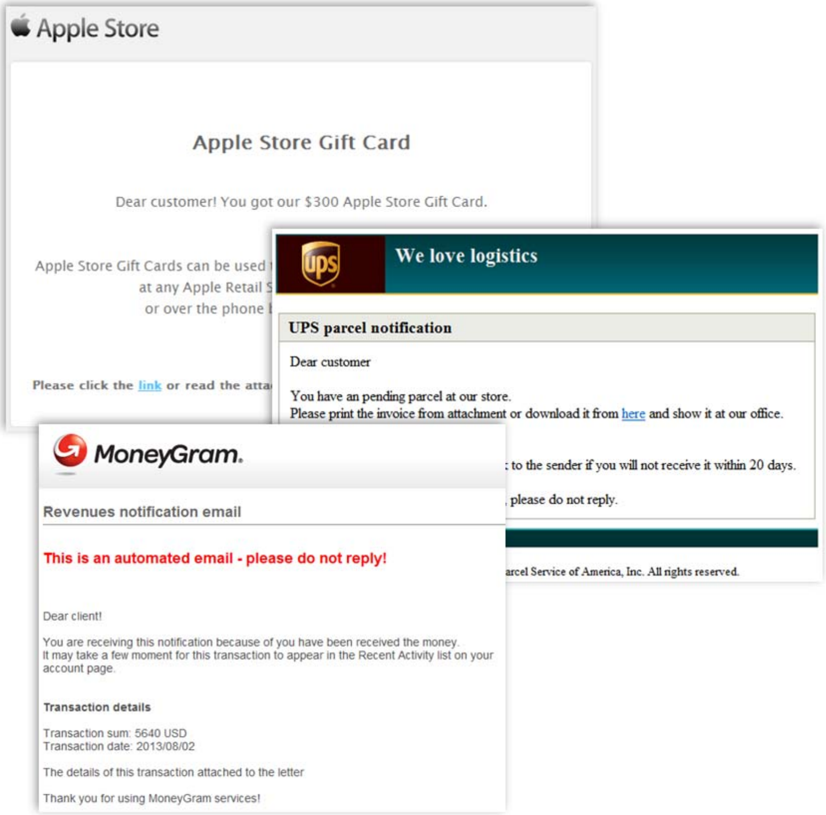
The average daily amount of email malware remained almost unchanged compared to last quarter at nearly 2 billion emails per day. This average hides the steady increase from July to September which included outbreaks of double the daily average.



Email-malware levels June – September 2013

Commtouch Security Labs saw numerous repeating email-malware campaigns in Q3. As usual, the emails and notifications were sent in the name of big companies and brands, but included a malicious email attachment and in some cases, also a link to an infected website. The brands used in the attacks included:

- Apple – an "Apple Store Gift Card" from August had a virus attachment as well as a malicious link in the message body. The gift card amount varied per email.
- Burger King – with a coupon titled: "THE KING CELEBRATES SPRING!"
- KFC – with a "KFC for Lunch" coupon
- Walmart
- UPS – parcel notifications – attached malware identified by Commtouch as: W32/Trojan.HATG-6756
- DPD – a big logistics company in Germany, with emails written in German and targeting German users
- MoneyGram – the transaction sum varied a bit per email



Apple Store

Apple Store Gift Card

Dear customer! You got our $300 Apple Store Gift Card.

Apple Store Gift Cards can be used
at any Apple Retail S
or over the phone

Please click the link or read the atta

We love logistics

UPS parcel notification

Dear customer

You have an pending parcel at our store.
Please print the invoice from attachment or download it from here and show it at our office.

: to the sender if you will not receive it within 20 days.

, please do not reply.

arcel Service of America, Inc. All rights reserved.

MoneyGram.

Revenues notification email

This is an automated email - please do not reply!

Dear client!

You are receiving this notification because of you have been received the money.
It may take a few moment for this transaction to appear in the Recent Activity list on your account page.

Transaction details

Transaction sum: 5640 USD
Transaction date: 2013/08/02

The details of this transaction attached to the letter

Thank you for using MoneyGram services!

Samples of emails with attached malware

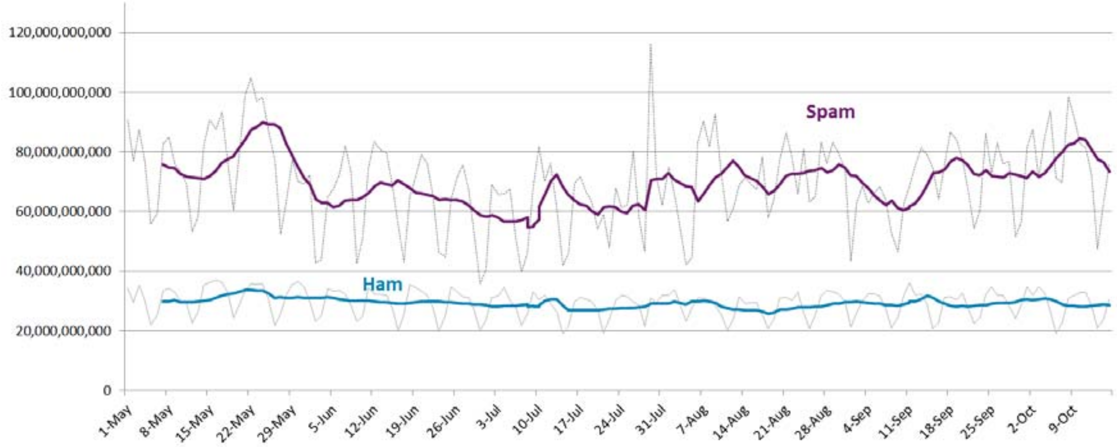
There were 2 noticeable trends:

1. Malware authors love to recycle – in all cases the URL links and malicious attachments lead to the same type of Trojan – only the subjects and brands are changed.

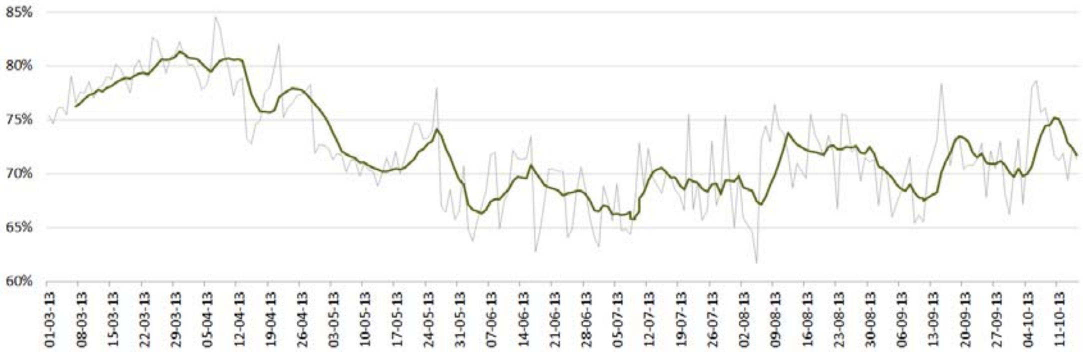
2. Cybercriminals are local experts. The fact that comparable malware campaigns target different countries and regions at the same time supports the result of the Q2 trend report: the strong increase in regionalized malware distribution. These campaigns are increasingly targeted at specific countries or areas, written in the language of the target audience, and use brands, services, products and events that are popular in the region in order to make the emails appear genuine and lure users to open attachments containing malware.

Spam Trends

In the third quarter of 2013, spam levels continued to drop. The average daily spam for the quarter was 69 billion messages, compared to the second quarter's 83 billion – a drop of around 17%. Although the quarterly level is the lowest in more than four years, the average per month has been steadily increasing since June's historic low of 63 billion messages per day. Over the period of Q3, spam represented 70% of all emails sent globally, dropping as low as 62% at the start of August.



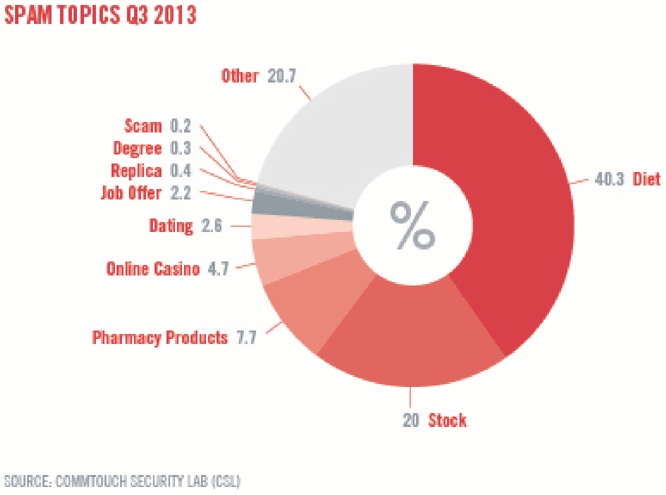
May to October 2013: Spam Levels



May to October 2013: Spam % of all email

Spam Topics

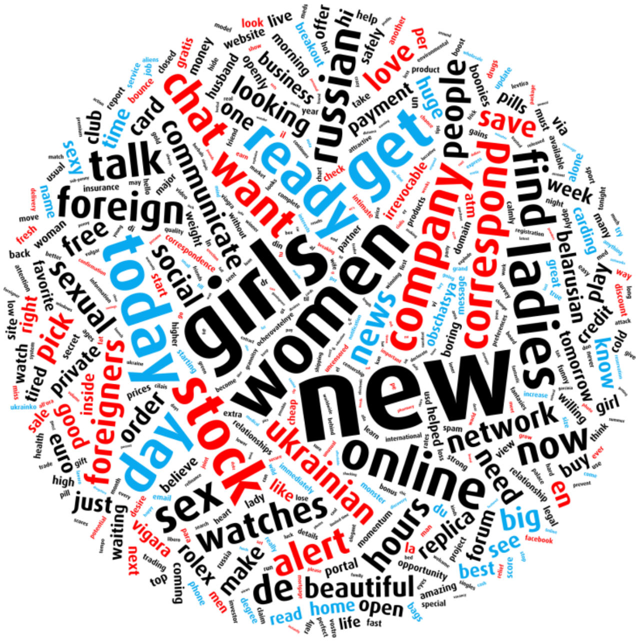
During the last three months spammers focused on diet products (such as Green Coffee Beans) – and so this category took position number one of the top 10 spam topics with a share of 40.2% (in Q2 it took position three, with 10.8%). Stock Spam moved from position number seven (4.7%) in Q2 to spam topic number two (20%) – so called Penny Stock Spam could be seen on a regular basis in the last quarter.



Spam Topics in Q3, 2013

After Stock Spam, the “other” category made position number three, followed by “Pharmacy Products” – which fell to position number four compared to number two in Q2.

Although Dating in Q3 just made position number five, there have been several campaigns on that topic. The content of such campaigns, and the mix of words used, can be seen in the following word cloud:

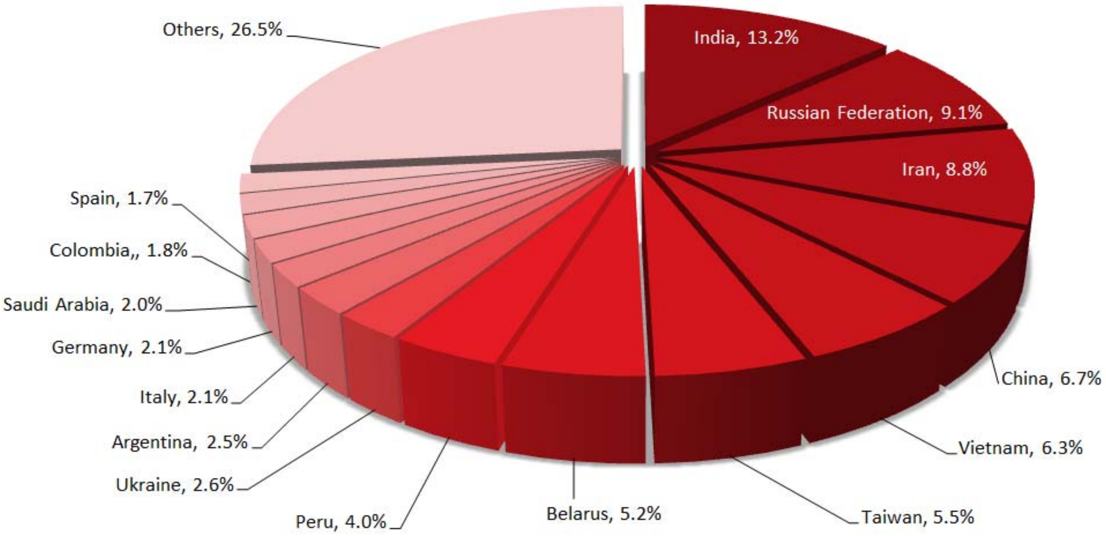


Word cloud on dating campaigns in Q3

Email zombies

During the third quarter of 2013, India stayed in first place with the most spam-sending bots – although their share dropped by 6% to 13.2%. Russia appeared to absorb most of this percentage and moved from 8th place into 2nd. New entries include Ukraine, Saudi Arabia, and Spain, while the United States, Serbia, and Mexico dropped out of the top 15.

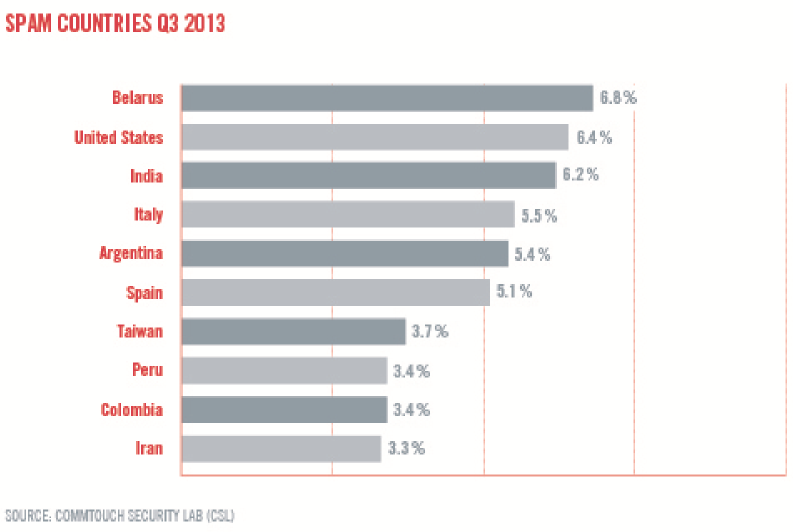
Although these zombies send unwanted email (including links to malware, spam and phishing pages), they have also been seen as part of denial of service attacks. As many as 20% of the approximately five million zombies tracked by Commtouch Security Labs also participate in other non-email attacks.



Countries with the most spam-sending zombies Q3 2013

Spam countries of origin

Belarus is again the number one spamming country (6.7%) – but in comparison to Q2 (14.7%) only with half as many spam emails. After topping the spam list in the first quarter of 2013, the United States fell to second place in Q2 (6.3%) – and stay there, even in Q3 (6.4%). The United States is followed by India (6.2%). There is only a small distance between Italy (position four with 5.47%) and Argentina (position five with 5.41%). Positions six to eight are made by Spain (5.1%), Taiwan (3.6%) and Peru (3.4%). Colombia (3.3%) and Iran make position nine and 10.



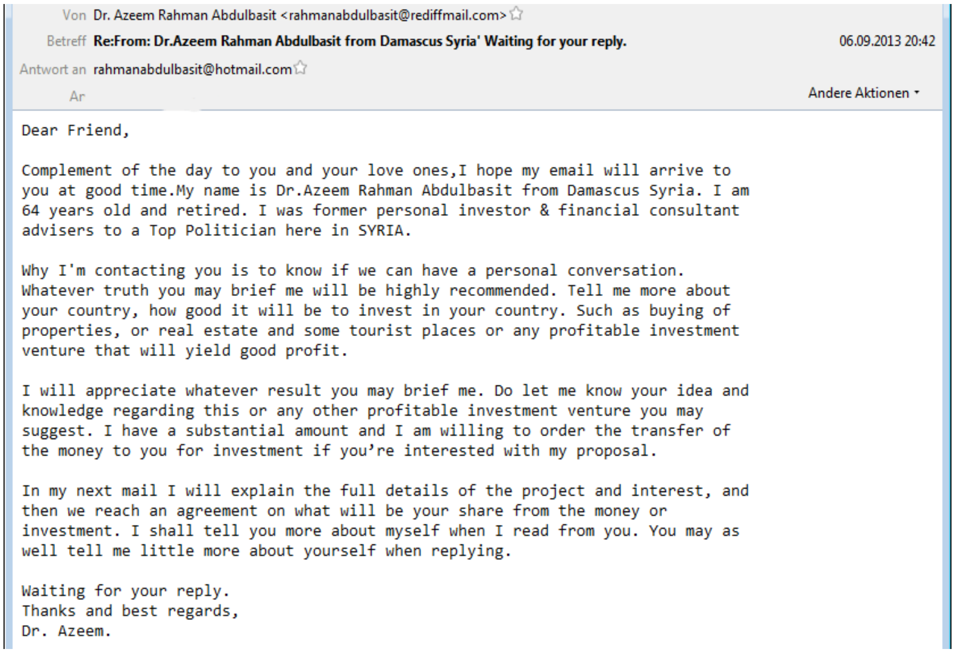
Countries of spam origin Q3, 2013

Geographically, the top 10 were widely distributed and featured three Asian countries, one from Eastern Europe, three from South America, two from southern Europe and one from North America. Noticeable was the absent of long-time top spamming countries such as Brazil and Russia as well as the complete absence of any central and western European countries.

Overall, the top 10 spam countries were responsible for almost half of all spam (49.1%).

Scams

In Q3 the Commtouch Security Lab also noted several scam campaigns that abused current topics. The following scam appeared at the same time as the Syria mailings described above (September 6, 2013) and had subject lines such as “Dr. Azeem Rahman Abdulbasit from Damasus Syria Waiting for your reply”:



Von Dr. Azeem Rahman Abdulbasit <rahmanabdulbasit@rediffmail.com>

Betreff **Re:From: Dr.Azeem Rahman Abdulbasit from Damascus Syria' Waiting for your reply.** 06.09.2013 20:42

Antwort an rahmanabdulbasit@hotmail.com

Ar

Dear Friend,

Complement of the day to you and your love ones,I hope my email will arrive to you at good time.My name is Dr.Azeem Rahman Abdulbasit from Damascus Syria. I am 64 years old and retired. I was former personal investor & financial consultant advisers to a Top Politician here in SYRIA.

Why I'm contacting you is to know if we can have a personal conversation. Whatever truth you may brief me will be highly recommended. Tell me more about your country, how good it will be to invest in your country. Such as buying of properties, or real estate and some tourist places or any profitable investment venture that will yield good profit.

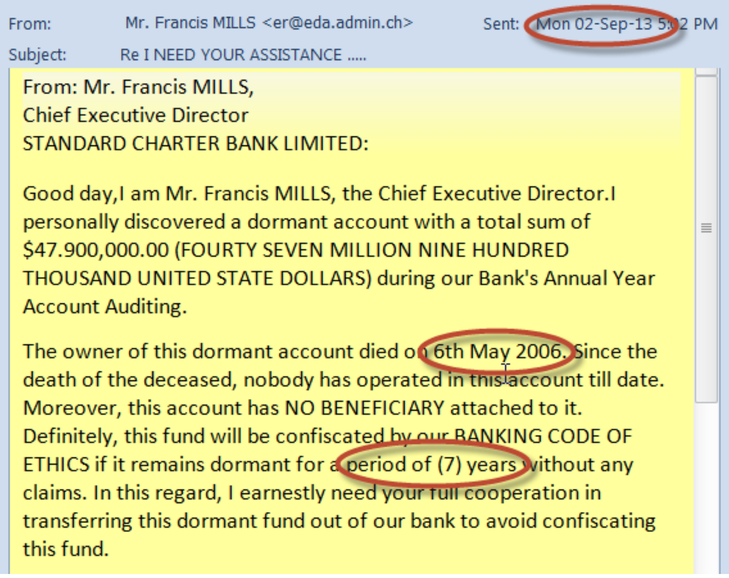
I will appreciate whatever result you may brief me. Do let me know your idea and knowledge regarding this or any other profitable investment venture you may suggest. I have a substantial amount and I am willing to order the transfer of the money to you for investment if you’re interested with my proposal.

In my next mail I will explain the full details of the project and interest, and then we reach an agreement on what will be your share from the money or investment. I shall tell you more about myself when I read from you. You may as well tell me little more about yourself when replying.

Waiting for your reply.
Thanks and best regards,
Dr. Azeem.

Scam Mailing, regarding Syria Conflict

A more amusing scam comes in the form of a standard “dormant bank account” mailing. Someone forgot to do the math which would indicate that according to the “bank” rules, this account would by now have been “confiscated” and would no longer be dormant. Of course those who believe they are going to receive 47 million dollars would probably not notice this discrepancy.



From: Mr. Francis MILLS <er@eda.admin.ch> Sent: Mon 02-Sep-13 5:02 PM

Subject: Re I NEED YOUR ASSISTANCE .....

From: Mr. Francis MILLS,
Chief Executive Director
STANDARD CHARTER BANK LIMITED:

Good day,I am Mr. Francis MILLS, the Chief Executive Director.I personally discovered a dormant account with a total sum of $47.900,000.00 (FOURTY SEVEN MILLION NINE HUNDRED THOUSAND UNITED STATE DOLLARS) during our Bank's Annual Year Account Auditing.

The owner of this dormant account died on 6th May 2006. Since the death of the deceased, nobody has operated in this account till date. Moreover, this account has NO BENEFICIARY attached to it. Definitely, this fund will be confiscated by our BANKING CODE OF ETHICS if it remains dormant for a period of (7) years without any claims. In this regard, I earnestly need your full cooperation in transferring this dormant fund out of our bank to avoid confiscating this fund.

Scam mailing requiring better quality control

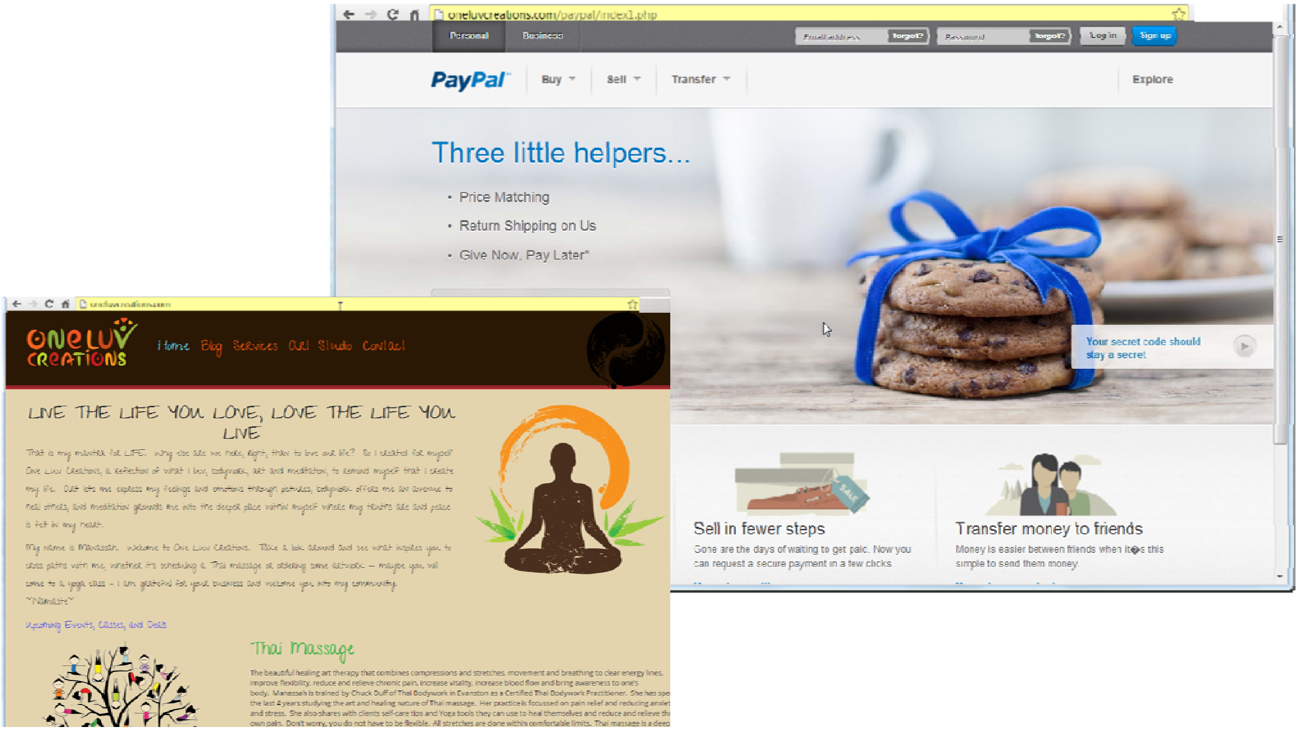
Phishing Trends

The table below summarizes the categories of legitimate websites that were most likely to be hiding phishing pages. The average number of daily phishing sites tracked in Commtouch's GlobalView database increased by nearly 35% in Q3.

Website categories infected with phishing

Rank	Category		Rank	Category
1	Free Web pages		6	Travel
2	Education		7	Shopping
3	Sports		8	Health & Medicine
4	Business		9	Real Estate
5	Computers & Technology		10	Fashion & Beauty

This perfectly rendered PayPal page appeared in August – one of about 750 created every day in August (that's 22,000 for PayPal in August alone). The only giveaway is the URL belonging to a hacked website called "One Luv Creations." According to the owner, "One Luv Creations, a reflection of what I luv, bodywork, art and meditation." For a few days in August One Luv Creations was also a phishing site (very bad karma…).



Three little helpers...

- Price Matching
- Return Shipping on Us
- Give Now, Pay Later*

Your secret code should stay a secret

Sell in fewer steps

Gone are the days of waiting to get paid. Now you can request a secure payment in a few clicks.

Transfer money to friends

Money is easier between friends when it�s this simple to send them money.

LIVE THE LIFE YOU LOVE, LOVE THE LIFE YOU LIVE

That is my mantra for LIFE. Why else are we here, right, than to love our life? So I created for myself One Luv Creations, a reflection of what I luv, bodywork, art and meditation, to remind myself that I create my life. Art lets me express my feelings and emotions through pictures, bodywork offers me an avenue to heal others, and meditation grounds me into the deeper place within myself where my truths are and peace is felt in my heart.

My name is Manessah. Welcome to One Luv Creations. Take a look around and see what inspires you to cross paths with me, whether it's scheduling a Thai massage or ordering some artwork – maybe you will come to a yoga class – I am grateful for your business and welcome you into my community.
~Namaste~

Upcoming Events, Classes, and Deals

Thai Massage

The beautiful healing art therapy that combines compressions and stretches, movement and breathing to clear energy lines, improve flexibility, reduce and relieve chronic pain, increase vitality, increase blood flow and bring awareness to one's body. Manessah is trained by Chuck Duff of Thai Bodywork in Evanston as a Certified Thai Bodywork Practitioner. She has spe the last 4 years studying the art and healing nature of Thai massage. Her practice is focussed on pain relief and reducing anxiet and stress. She also shares with clients self-care tips and Yoga tools they can use to heal themselves and reduce and relieve th own pain. Don't worry, you do not have to be flexible. All stretches are done within comfortable limits. Thai massage is a deep

PayPal phishing site hidden in legitimate site "One Luv Creations"

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 550 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/number-of-the-month-september-2013/
- https://blog.commtouch.com/cafe/phishing/750-new-paypal-phishing-sites-each-day/
- https://blog.commtouch.com/cafe/data-and-research/current-malware-campaigns-in-the-name-of-apple-ups-and-moneygram/
- https://blog.commtouch.com/cafe/data-and-research/real-time-spam-delivers-a-royal-baby/

commtouch®
Real Security. In Real Time.

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