

Internet Threats Trend Report July 2011



pallas

com *m* touch[®]



In This Report

Spammer tactics change – Compromised accounts now favored	Page 2
Analysis of compromised accounts – Is all spam from Gmail and Hotmail sent by zombies?	Page 5
e-cigarettes – The new Viagra?	Page 6
IRS payment rejected – Angry users download malware	Page 7
“Osama Bin Laden dead – Actual video” – Facebook users tricked into running malware	Page 10
iPhone 5 virus hosted on compromised site – Exploiting the hype	Page 13
Double the Zombies – Large malware outbreaks recruit new hordes	Page 18
World IPv6 day – New technology, new threats	Page 18

Q2 2011 Highlights

▼ 113 billion

Average daily spam/phishing emails sent
Page 2

▲ 377,000 Zombies

Daily turnover
Page 18

🇮🇳 Streaming media/ Downloads

Most popular blog topic on user-generated content sites
Page 20

▼ Pharmacy ads

Most popular spam topic (24% of spam)
Page 6

🇮🇳 India

Country with the most zombies (17%)
Page 18

▲ Pornography/ Sexually Explicit

Website category most likely to be contain malware
Page 13

Overview

Spammer tactics are changing as spam levels flat-lined this quarter to the lowest levels in around three years, primarily due to the highly-publicized Rustock botnet takedown. In contrast, there have been unusually large email-borne malware attacks during the quarter, more than doubling the daily turnover of zombies tracked by Commtouch Labs.

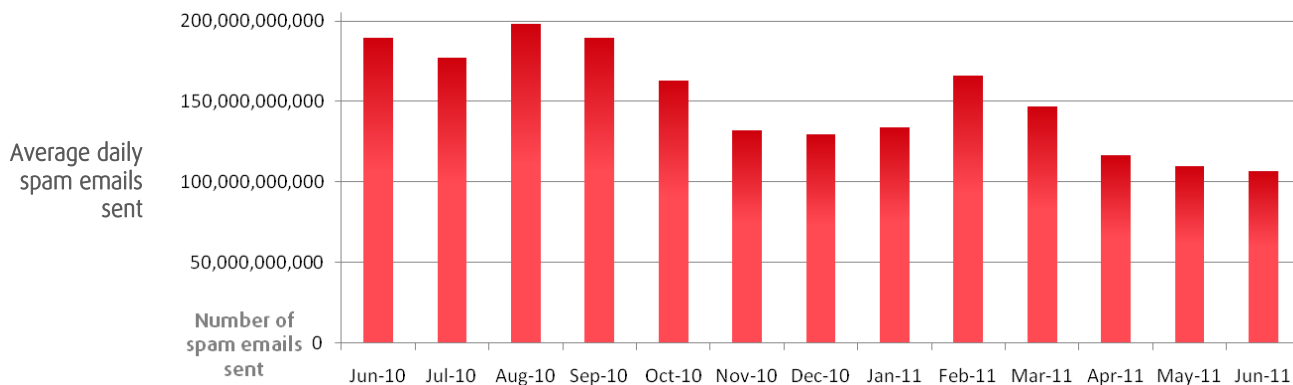
Facebook's large user-base once again made it a favorite target for attacks, most notably following the death of Osama Bin Laden when Facebook malware promised videos of the event to Facebook users. Facebook malware also spread extensively by promising users that it would reveal "who had been viewing their profile."

The second quarter included numerous other malware outbreaks based on SEO poisoning, fake IRS "rejected payment" emails, and malicious scripts embedded in Adobe PDF files. World IPv6 day on June 8th raised the profile of the replacement for IPv4 but also highlighted the potential threats that will accompany its introduction.

Spam Trends

Spammer tactics are changing

In mid-March, Microsoft led a takedown of the Rustock botnet. The immediate effect on spam levels was a drop of nearly 30% to an average of 119 billion messages per day during the last two weeks of March. In the past, botnet takedowns have resulted in temporary drops in spam levels followed by sustained increases, as spammers created new botnets and resumed mass mailings. The spam levels of this quarter however, suggest that the expected "recovery" of spam might not occur in the near term, and that spammers are changing their tactics. Average daily spam levels for the past year are shown below:



Source: Commtouch

June's spam level (106 billion) is the lowest in over 3 years. At its lowest point in June, spam accounted for 75% of all emails.

In addition to the reduced spam levels the following statistics support the idea of changing spammer tactics:

- The Rustock botnet takedown was followed by large increases in email-borne malware (as noted on page 7 of this report).

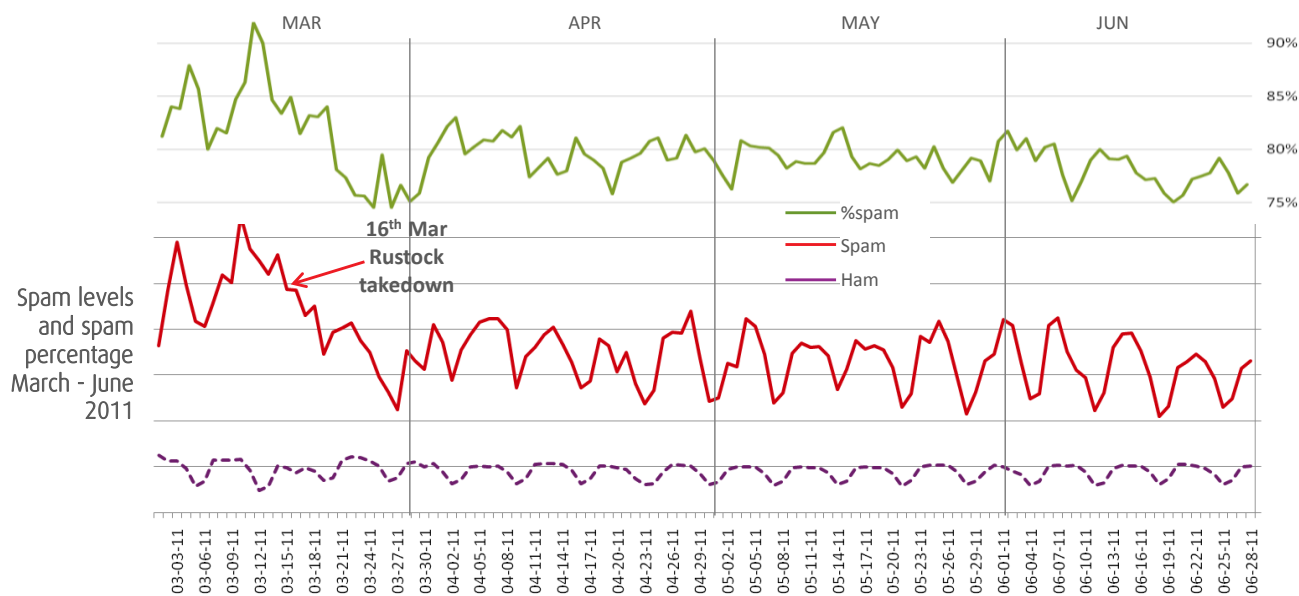
July 2011 Internet Threats Trend Report

- The number of zombies activated daily more than doubled in the weeks following the malware outbreaks (see page 18).
- The increased zombie horde was not used for vast spam mailings (hence the declining spam numbers) but instead for smaller malware distribution attacks.
- Spam coming from compromised or spammer accounts as well as compromised mail servers has increased – this is illustrated by the analysis on page 5 below.

The new tactic therefore calls for the use of compromised accounts to send spam as opposed to using botnets. The move away from botnet spam can be attributed to the use of IP reputation mechanisms that have been increasingly successful in blacklisting zombie IP addresses and therefore blocking botnet spam. The blocking of spam from compromised accounts based on IP address is more difficult for many anti-spam technologies, since these accounts exist within whitelisted IP address ranges (such as Hotmail or Gmail).

One of the primary aims of the larger malware outbreaks and phishing attacks of this quarter is therefore to acquire enough compromised accounts to make spamming viable. The catch for spammers: While spam from compromised accounts is less likely to get blocked by IP reputation systems, the volumes that can be sent are lower due to the thresholds imposed on these accounts. This at least partially accounts for the lower spam volumes seen this quarter.

It is also likely that cybercriminal groups are diversifying, with money to be made from stolen banking credentials as well as the use of botnets for funded denial of service attacks.



Source: Commtouch

July 2011 Internet Threats Trend Report

Although reduced, spam has certainly not gone away. During this quarter fake Twitter notifications again flooded inboxes worldwide with links leading to pharmacy pages. The example below is from an outbreak that took place in April.

Fake Twitter notification



Destination pharmacy site (with Easter branding)

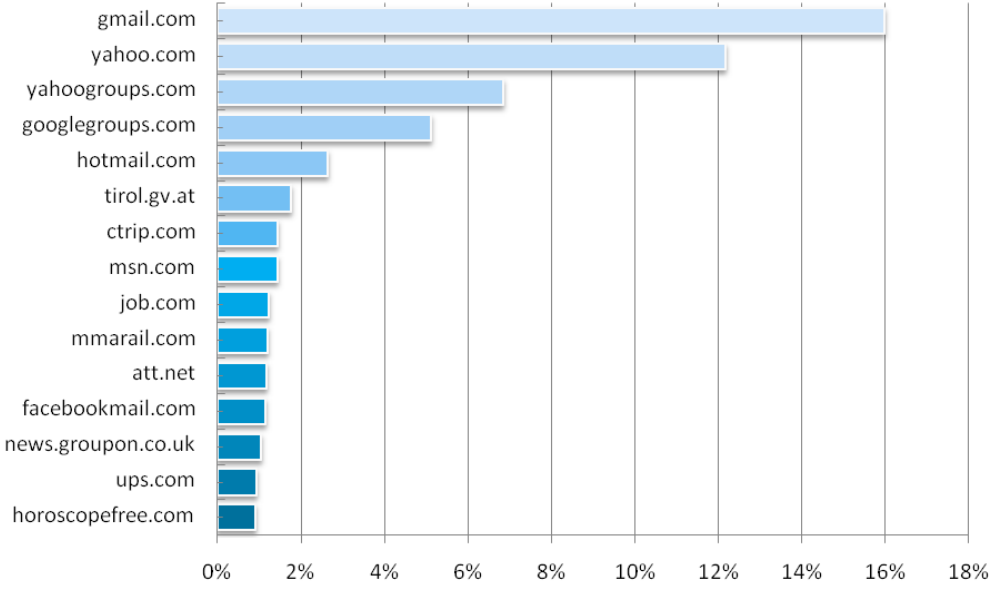


Source: Commtouch

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 faked spam sending domains



Source: Commtouch

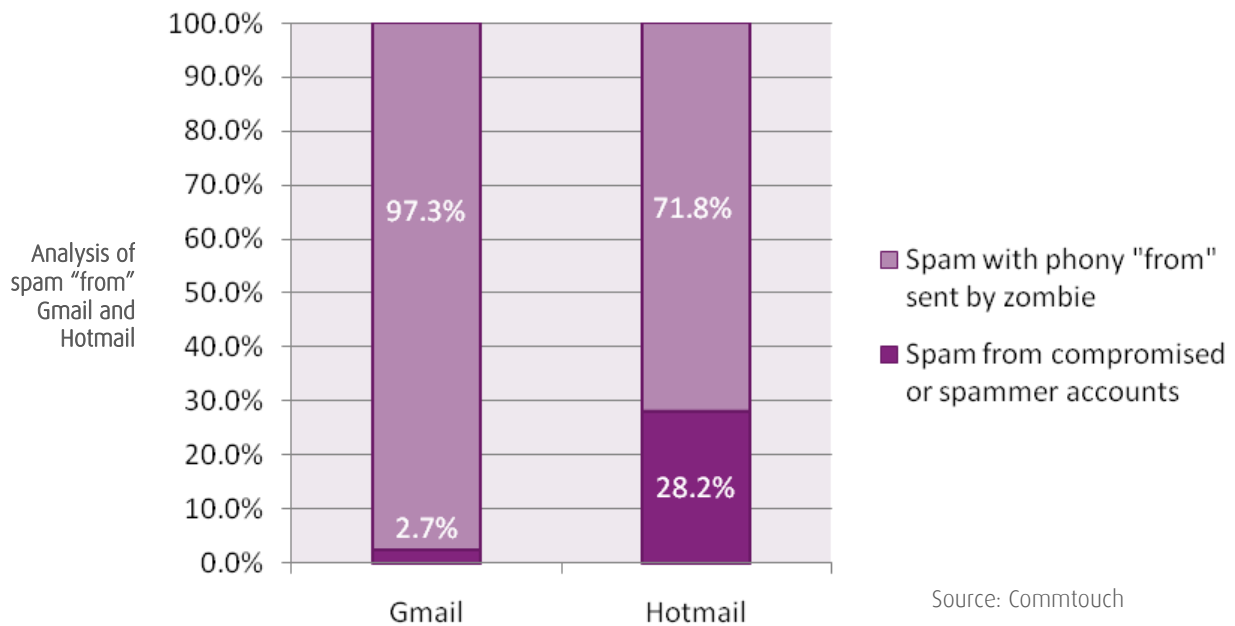
This quarter, gmail.com is once again the most spoofed domain. 14th place is held by ups.com due to the very large numbers of fake UPS notification emails sent as part of the outbreaks of the quarter (see page 7).

Analysis of compromised accounts

In addition to the spoofed emails (shown above), a percentage of the emails from Gmail and Hotmail actually come from genuine accounts. These can be compromised accounts or accounts specifically created by spammers for this purpose. The graph below illustrates the percentage of spam received over a trial period this quarter where the "from" field includes Gmail and Hotmail. Based on the IP address, received spam could either be:

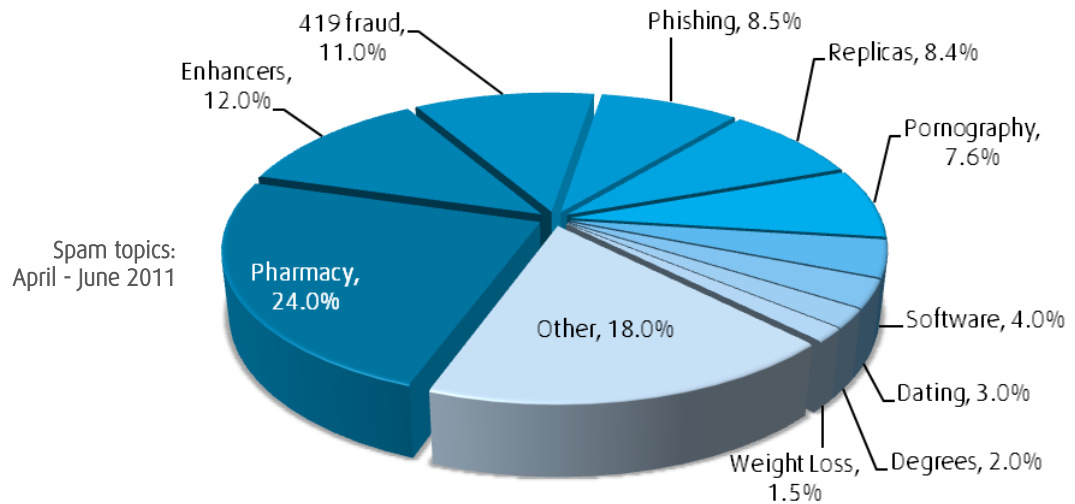
- Sent from a zombie with a phony Gmail or Hotmail address in the from field
- Or, sent from a compromised or spammer account at Gmail or Hotmail

As shown, almost 30% of the spam from Hotmail actually comes from compromised or spammer Hotmail accounts. Gmail spam, on the other hand, is mostly from zombies that simply forge their Gmail addresses.



Spam topics

Pharmacy spam remained in the top spot but continued to drop this quarter to only 24% (down from 28% in Q1 2011). 419 fraud, phishing, and pornography all increased.



Source: Commtouch

In addition to the traditional products covered by spam emails, the second quarter saw the emergence of e-cigarette spam. There is still no consensus about the health risks or benefits of these new devices – resulting in widely varying and sometimes confusing legislation among different countries. Some countries have banned e-cigarettes, some have allowed controlled sales, some are relying on local governments to decide, and others are permitting open sales to anyone. Naturally, spammers are stepping into this confusion to offer e-cigarettes to anyone with an email address. Some examples received in Russian (with translation):

- Оптовые поставки электронных сигарет (Wholesale of electronic cigarettes)
- Е-сигареты опт (E-cigarette wholesale)
- е-сигареты из Китая (опт) (E- cigarette Chinese (wholesale))
- е-сигареты – из Азии (опт) (E- cigarette – from Asia (wholesale))

A French email shown below promotes the health benefits due to the absence of the 4000 unwanted substances found in a normal cigarette.

e-cigarette spam

E-fumer : la curiosité a du bon
Add contact

Si vous ne parvenez pas à lire ce message correctement, consultez la version en ligne
Ou collez cette adresse dans votre navigateur internet : <http://www.commtouch.com/fusion/display.php?M=4241217&C=80d5c7b3abc4e1ccf8ddeb2153394bd2&S=68>

La cigarette électronique jetable

Ne contient aucune des 4000 substances toxiques ou cancérigènes contenues dans une vraie cigarette

[Voir la Vidéo](#)

Source: Commtouch

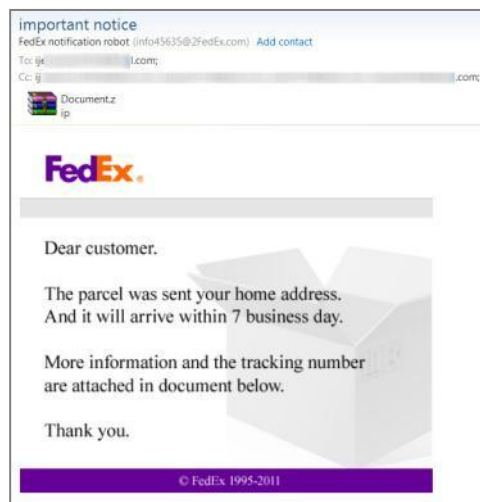
Malware trends

The first quarter ended with enormous outbreaks of email-borne malware – in some cases accounting for 30% of global email traffic. Initially the attachments were “UPS package notifications”. Then the subjects changed focus to “DHL package notifications”. At the start of the second quarter these attacks continued on a smaller scale and switched once again, this time to “FedEx notifications”.

The second quarter included malware distributed using a variety of methods - several of these are shown below. The iPhone 5 virus is described on page 13.

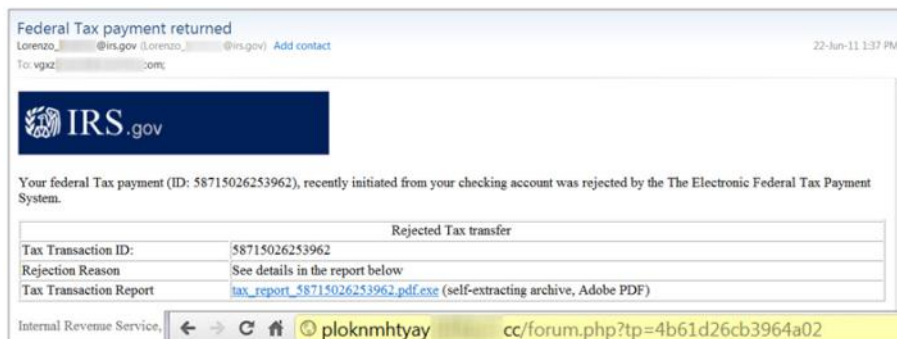
IRS payment rejected

Emails from fake .irs.gov addresses were distributed in late June informing recipients that their tax payments made via the IRS’s electronic payment system had been rejected. A link to a “tax transaction report” assured recipients that it was a “self extracting archive” – apparently to allay the fears of those who noticed the .exe file extension.



Source: Commtouch

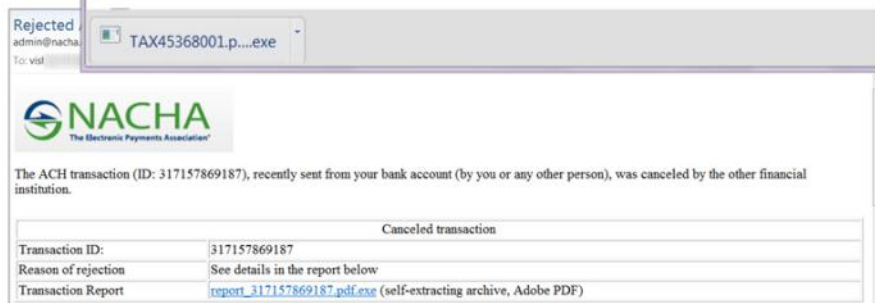
Phony “IRS payment rejected” emails lead to malware



Destination site with “404 not found” message – malware downloaded in background



Phony “NACHA payment rejected” emails lead to malware



Source: Commtouch

The links lead to any of 2,500 domains that were registered in the 48 hours before the attack. The destination pages (confusingly) show a “404 not found” messages which actually hides the script that starts the “PDF” file download. The downloaded filename for this site was: TAX45368001.pdf.exe. Analysis indicated that the malware’s purpose was most likely password theft.

One week after the outbreak, an almost identical template was used – this time referring to rejected payments by NACHA (an interbank electronic payments organization).

SEO poisoning leads to fake antivirus

YeheyTV is an Internet site offering Filipino television shows online. The site has been around since 2009 and is frequented by Filipinos around the world. In June fake-antivirus distributors exploited this popularity by using a Search Engine Optimization (SEO) poisoning attack directed at Internet users looking for the YeheyTV site. Searching for the keywords “yeheytv pinoy” via the Yahoo, Google or Bing search engines gave the following results:

Searches on different engines for Filipino “Yehey TV” lead to poisoned results



Source: Commtouch

Clicking the links circled in red on the search results above leads to fake scanning pages – a common trick used by Fake-AV to fool users into downloading and executing various malicious files.

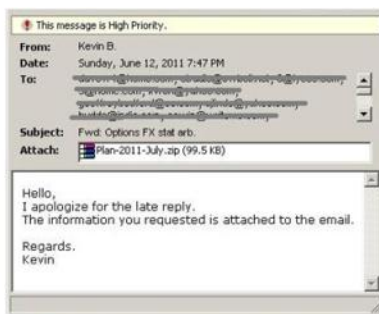
PDF malware

PDF files as well as executables disguised as PDF files were used in numerous attacks during Q2 2011. Two examples are shown below. The first example is clearly targeted at a financially savvy victim since the subject mentions “stat arb.” This actually refers to statistical arbitrage – a term used in foreign exchange trading.

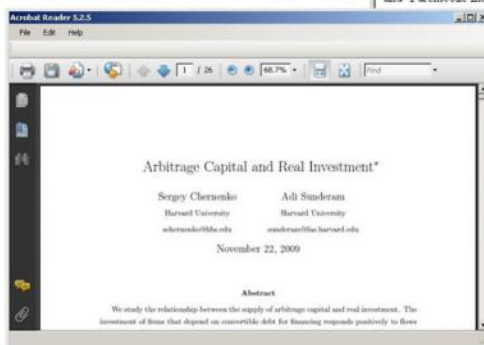
The zip file extracts to an executable file, but the icon shown is of an Adobe Acrobat PDF file. Users with file extension view disabled on their computers, will see a PDF icon and think the file is simply a PDF. When the file is executed, it will show a non-malicious PDF file in a fake PDF reader window.

July 2011 Internet Threats Trend Report

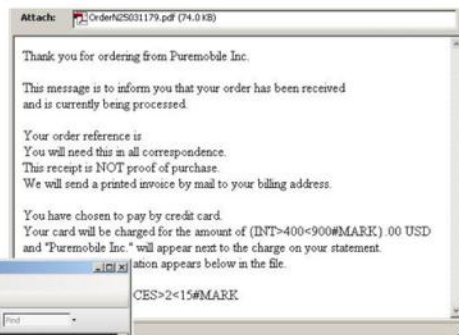
Email promising "stat arb" information



Phony PDF reader application shows text while malware executes in background



Email with PDF attachment containing hidden malware script



Source: Commtouch

The malware then does the following:

- Captures all keystrokes and activities as users browse the internet.
- Saves the stolen keylogging information in the file on the user's hard drive – "updates2.txt".
- Sends the keylogger file to the malware owner via e-mail.

The second example of PDF malware uses complex coding to hide a malicious JavaScript within the PDF file. The "order confirmation" PDF includes what appears to be a PNG image. PNG is usually used for image encoding, but not in this case. The PNG data actually hides an electronic form. This electronic form (which uses the XFA format) includes the malicious JavaScript.

Top 10 Malware

The table below presents the top 10 most detected malware as compiled by Commtouch's Command Antivirus Lab.

Top 10 Detected Malware			
Rank	Malware name	Rank	Malware name
1	IFrame.gen	6	W32/Worm.MWD
2	W32/Ramnit.E	7	W32/VBTrojan.17E!Maximus
3	W32/Worm.BAOX	8	W32/Ramnit.D
4	W32/RAHack.A.gen!Eldorado	9	W32/Mydoom.0@mm
5	W32/Sality.gen2	10	W32/Vobfus.L.gen!Eldorado

Source: Commtouch

Web Security

Facebook security

Facebook's vast and ever-increasing user base continues to attract cybercriminals. The trusted friend environment is proving to be both a benefit and a difficulty for those seeking to abuse the social network. The benefit is the unquestioned trust of any message, wall post or invitation received from a friend – most Facebook users will never suspect that the message comes from a compromised account. Spammers or malware distributors wishing to exploit the Facebook platform will encounter certain difficulties, such as:

- 1) The need for compromised accounts – since messages, wall posts, invites etc. can only be sent to friends.
- 2) The limited scale of attacks since friend networks rarely exceed a few hundred people, and Facebook have put mechanisms in place to detect multiple simultaneous messages postings. Spam and malware sent using traditional email can still reach much wider audiences.

This quarter saw several techniques used to compromise user accounts combined with social engineering elements to increase the scale of attacks.

“Osama Bin Laden dead – Actual video”

In May, the news of Osama Bin Laden's death was quickly exploited by affiliate marketing groups. Affiliates make money by driving victims to a range of sites that pay bonuses to the affiliates based on clicks or successful sign-ups. The initial Osama-themed messages were spread from several compromised accounts and then used the following steps to increase the spread and draw users to the affiliated sites:

Invitation to view
Osama Bin Laden
video



Source: Commtouch

- Facebook friends received messages or event invitations promising actual videos of the death of Bin Laden.
- These messages trick users into running a malicious JavaScript. Since the script is run while the user has Facebook open, the malware has access to all of the user's friends and privileges (such as being able to send messages).
- The now-infected user is lead to a website with a YouTube clip of President Obama's announcement of the operation (which was cut down to a few seconds). The site then quickly redirects to an affiliate marketing page.

July 2011 Internet Threats Trend Report

- In parallel the malicious script sent out more “Bin Laden Death Video” messages and the cycle restarted.

And below is a screenshot of one of the many destination pages which feature the instructions to start the malware cycle. Note that the instructions are very specific about copying and pasting the link into the open Facebook page. This effectively runs the script “within” a Facebook session allowing the script to hijack the legitimate Facebook session and perform any account related activity.

“Instructions” to download Osama Bin Laden video



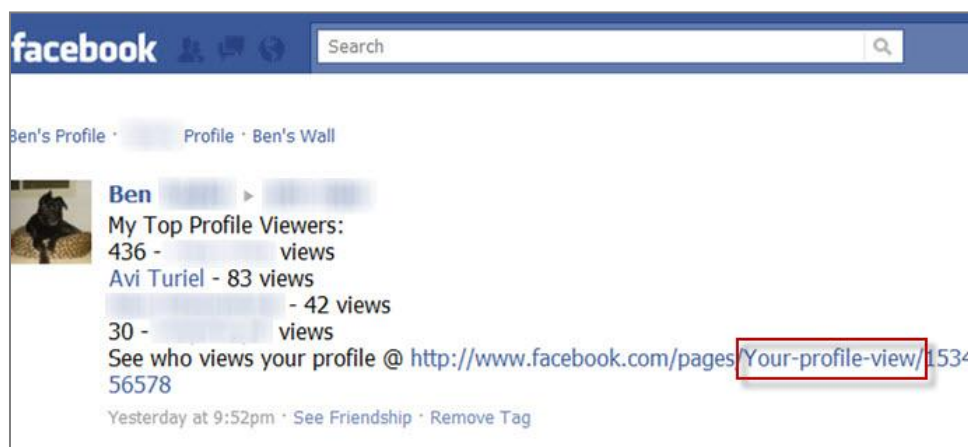
Source: Commtouch

See who's been viewing your profile

A few days prior to the Bin Laden incident, there were other occurrences of the techniques described above, requiring users to paste scripts into their browser address bars. The subjects used were also designed to attract as much user interest as possible including:

- “See who views your profile”
- “Free Facebook credits”

Invitation to “see who views your Facebook profile”



Source: Commtouch

Once the application is authorized, the name changes to “Top Stalkers”. The Top Stalkers application then appears to load but is blocked seconds later by a “Security Check” screen.

Following the link “Are you and your partner compatible” leads to an affiliate marketing site requesting the user’s mobile number and attempting to sign them up for premium SMS services. In parallel, the rogue application posts on the new victim’s wall. This post is slightly changed from the original post followed by the user.

These subtle text changes (circled) are apparently an attempt to outwit spam filters used within Facebook.

Compromised sites

Cybercriminals often hack websites to hide phishing pages or malware. This provides them with two main advantages:

- 1) The legitimate domain probably has a good reputation from the point of view of most URL filtering engines and is therefore not likely to be blocked.
- 2) The compromised site provides free hosting for the malware or phishing page.

iPhone 5 virus hosted on compromised site

In May, a malicious email was distributed that exploited the hype surrounding the release of the iPhone 5. The email describes the “iPhone 5G S” with text and forged images that group together several of the popular rumors circulating about the new device, i.e. slimmer, faster, bigger display, better cloud integration. All the images and links in the email point to the file “iphone5.gif” – which is actually the malware “iphone5.gif.exe”.

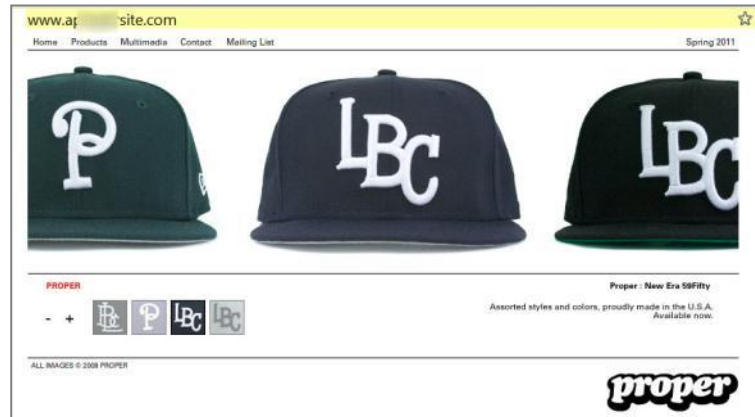
iPhone 5 virus -
email with links to
malware
“iphone5.gif.exe”



Source: Commtouch

Clicking anywhere in the email will lead to the download of the malware file. Closer examination of the link provided in the email reveals that the malware has been hidden inside a compromised legitimate site. The screen below shows one of the genuine pages:

Legitimate site
hiding iPhone 5
Virus download



Source: Commtouch

Categories of compromised sites with malware

During the second quarter of 2011, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware. Pornographic and sexually explicit sites were once again at the top of the list – pushing parked domains into second place. As noted in previous reports though, the hosting of malware may well be the intention of the site owners. The portals category includes sites offering free homepages which are often abused to host phishing and malware content or redirects to other sites with this content.

Website categories infected with malware			
Rank	Category	Rank	Category
1	Pornography/Sexually Explicit	6	Business
2	Parked Domains	7	Health & Medicine
3	Portals	8	Travel
4	Education	9	Computers & Technology
5	Entertainment	10	Fashion & Beauty

Source: Commtouch

Phishing Trends

Phishing attacks continued to target local and global banks, Web email users, Facebook accounts, and even online gaming sites. A phishing page targeting users of the game RuneScape is shown below.

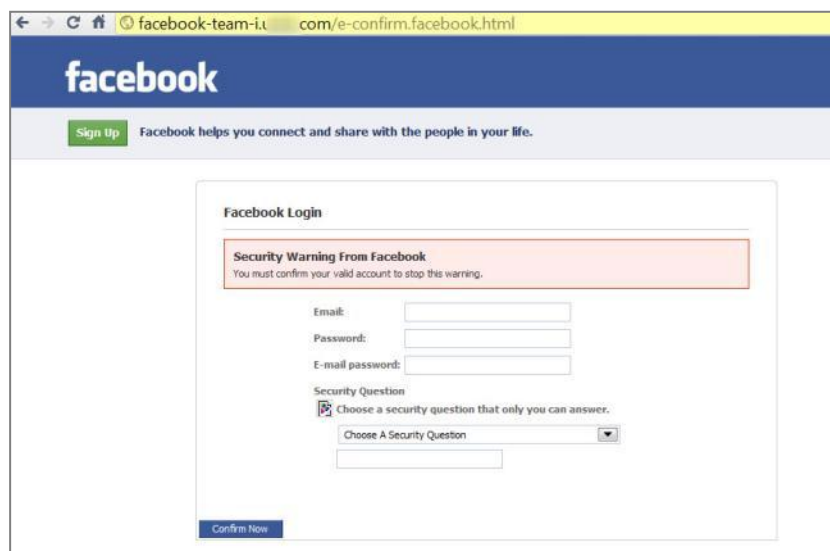
Runescape online game phishing page



Source: Commtouch

As described in the “Facebook Security” section above, compromised Facebook accounts are highly valued as they provide access to a trusting network of friends. An example of a Facebook phishing page using a domain set up to target Facebook users is shown below. The page purports to be a Facebook login page, designed to overcome a security warning that appears in red at the top of the page. Users are asked to log in to take care of this security issue. By entering their credentials, they are providing valid Facebook credentials to the phisher, who can then use them himself or sell them to another criminal who needs them.

Facebook phishing page



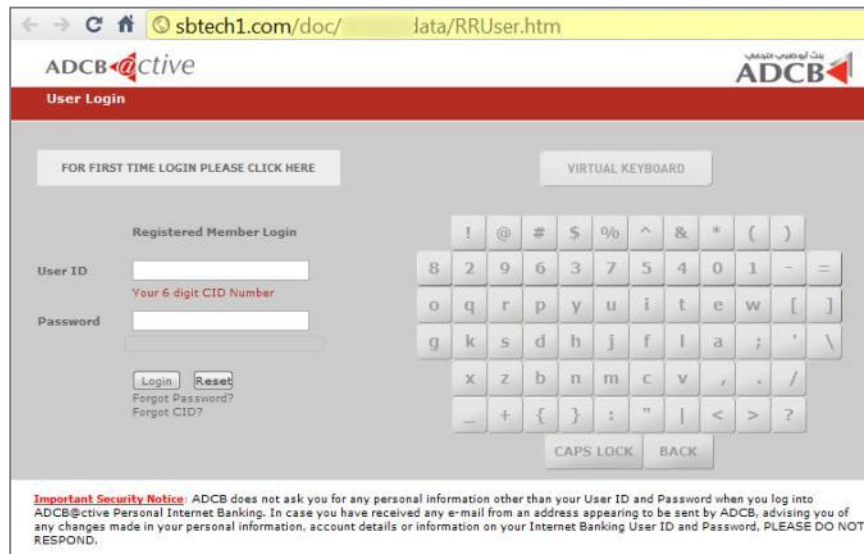
Source: Commtouch

Improved phishing sites

In order to provide protection from keyloggers, some financial institutions have added more complex login pages including virtual keyboards. Phishers have kept up with this

trend - this phishing page for ADCB (Abu Dhabi Commercial Bank) successfully mimics the virtual keyboard found on the real site – where the password may only be entered using the onscreen version.

ADCB phishing site with functional password entry virtual keyboard



Source: Commtouch

Categories of compromised sites with phishing

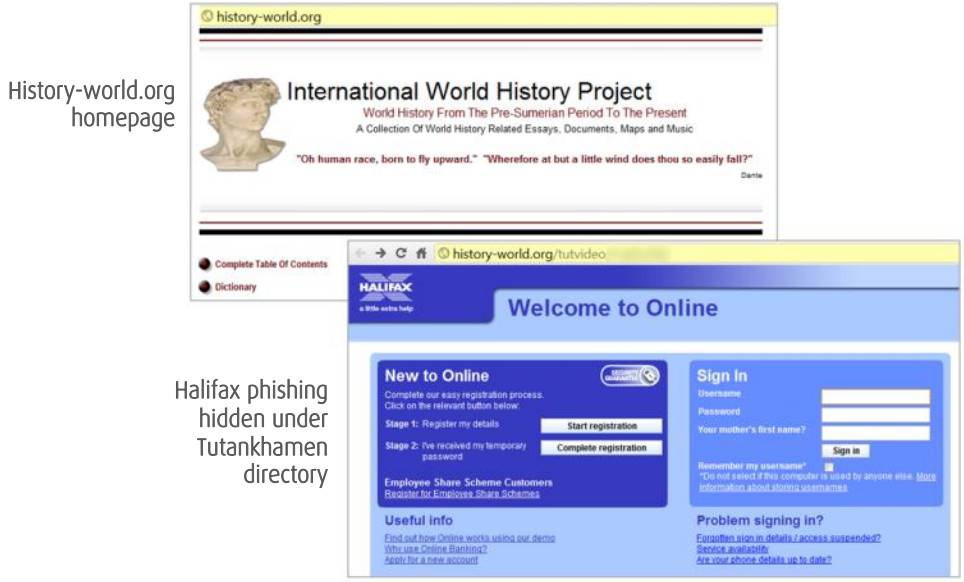
During the second quarter of 2011, Commtouch analyzed which categories of legitimate Web sites were most likely to be hiding phishing pages. Sites related to games ranked highest, similar to last quarter.

Website categories infected with phishing				
Rank	Category		Rank	Category
1	Games		6	Fashion & Beauty
2	Portals		7	Leisure & Recreation
3	Shopping		8	Sports
4	Forums/Newsgroups		9	Education
5	Non-profits & NGO		10	Business

Source: Commtouch

An example of a site that was compromised in June is shown below. The site "history-world.org" provides essays about numerous periods of history. Buried in the Egypt department (Tutankhamen) is a thoroughly modern phishing page targeting customers of UK bank Halifax.

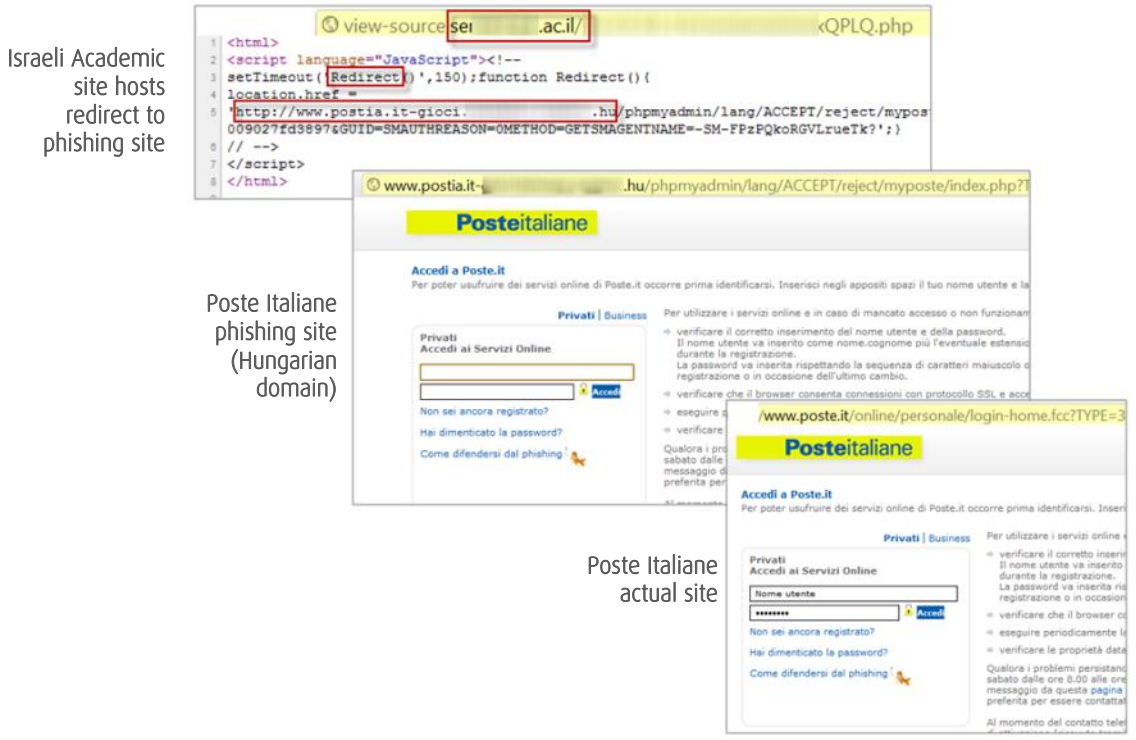
July 2011 Internet Threats Trend Report



Source: Commtouch

The global nature of phishing

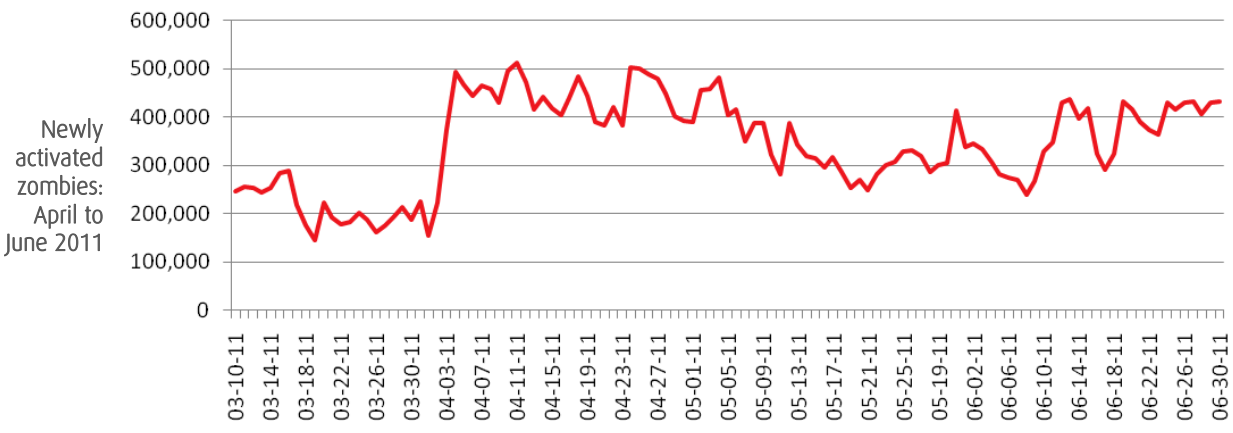
Compromised sites do not always have to host actual phishing pages, yet they can still pose a danger to users. In the example below an **Israeli** academic institution is hosting a simple redirect script to a phishing page hosted on a **Hungarian** domain. The phisher is aiming for login credentials of Poste Italiane customers – the **Italian** site offers online banking facilities. This multi-national phishing scheme demonstrates well the global nature of the phishing industry.



Source: Commtouch

Zombie trends

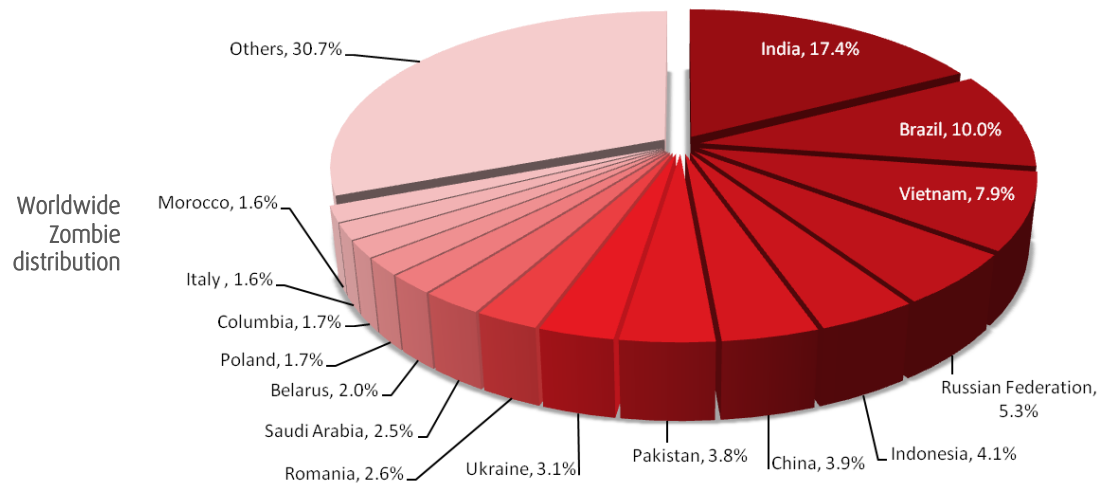
The second quarter saw an average turnover of 377,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. This number shows a substantial increase compared to the 258,000 of the first quarter of 2011. The large malware outbreak that took place at the end of March (see Page 7) resulted in large-scale recruitment of new zombies – more than doubling the daily turnover. Speculation as to the use of these zombies is provided on page 2 of this report.



Source: Commtouch

Zombie Hot Spots

India again claimed the top zombie producer title hosting 17% of the global zombie population. Brazil, Vietnam, and the Russian federation all remained in the same places. Peru and Argentina dropped out of the top 15 replaced by Romania and Morocco.



Source: Commtouch

IPv6 – new opportunities for zombies

June the 8th was global IPv6 day, when top websites and Internet service providers around the world, including Google, Facebook, Yahoo!, and Commtouch joined together with more than 1000 other participating websites for a successful global-scale trial of the new Internet Protocol, IPv6. As a result of the impending IPv4 address exhaustion, many

organizations have begun to more seriously consider their roadmaps to IPv6. As the global implementation of IPv6 becomes a reality, the associated security concerns are starting to be considered.

In an IPv4 environment, a zombie can almost certainly be associated with a single IP address due to the limited number of addresses available. A zombie operating in an IPv6 Internet though, may have access to a wide range of IP addresses. Blocking a single address may therefore be ineffective as the zombie can simply move to another address. Blocking a range of addresses is also not effective for the following reasons:

- The range might be used by other users/devices that are not malicious i.e.: false positives.
- There is no standard IP range allocation currently defined – it is therefore difficult to know how wide a range of IPs should be blocked.

CommTouch has begun to monitor spam received from IPv6 sources and future Internet Threat Trend Reports may include relevant data as IPv6 traffic grows. Two on-demand webcasts are available from CommTouch that more fully describe IPv6 and the potential threats:

- [An introduction to IPv6](#)
- [Overview of IPv6 threats](#)

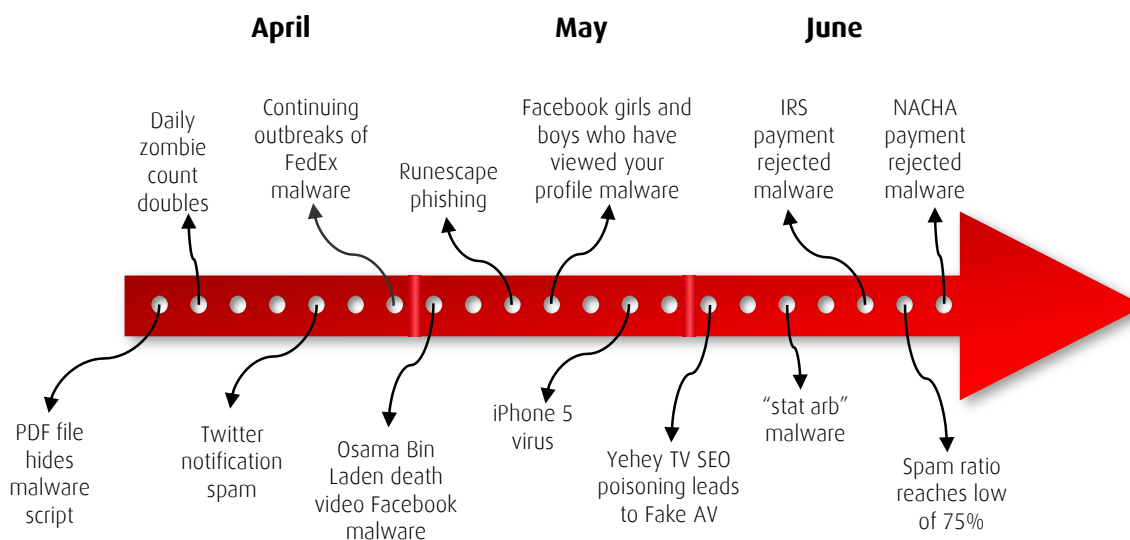
Web 2.0 trends

CommTouch's GlobalView Network tracks billions of Web browsing sessions and URL requests, and its 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, remaining at 21% of user-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.

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

Source: CommTouch

Q2 2011 in Review



About Commtouch

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

About Pallas

Pallas provides Managed Security Services through its own computer centers. The business model combines the advantages from centralization and managed operating. Pallas delivers all services for securing the Internet, e.g. secure messaging, firewalling, URL-filtering, VPN solutions and authentication. Pallas integrates and operates market leading products from security suppliers, both conventional techniques and real-time protection methods from Commtouch against new threats. Other Pallas business areas are Security Consulting and Secure Hosting, e.g. Livelink from Open Text and other Enterprise Content Management Systems, Oracle and Domino servers as well. Pallas was second-best in the international CEAS 2007 Live Spam Challenge. The Pallas Managed Security Services are certified from German TUEV. Pallas was founded in 1991, and is headquartered in Bruehl near Cologne, Germany. For more information see www.pallas.com or write [information \(at\) pallas.com](mailto:information@pallas.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.
- <http://blog.commtouch.com/cafe/malware/complex-pdf-hides-malware-inside-xfa-which-is-inside-png-%e2%80%93-not-an-image/>
- <http://blog.commtouch.com/cafe/phishing/more-fake-twitter-emails/>
- <http://blog.commtouch.com/cafe/malware/fedex-used-for-continued-email-malware-zombies-up-70/>
- <http://blog.commtouch.com/cafe/malware/500-free-credits-from-facebook-%e2%80%93-malware/>
- <http://blog.commtouch.com/cafe/malware/%e2%80%93cosama-bin-laden-dead-%e2%80%93-actual-video-%e2%80%9d-new-facebook-malware/>
- <http://blog.commtouch.com/cafe/anti-spam/e-cigarettes-%e2%80%93-the-new-viagra-for-spammers/>
- <http://blog.commtouch.com/cafe/phishing/avoiding-facebook-phishing/>
- <http://blog.commtouch.com/cafe/phishing/phishing-%e2%80%93-going-the-extra-mile-with-virtual-keyboard/>
- <http://blog.commtouch.com/cafe/email-security-news/the-iphone-5-virus/>
- <http://blog.commtouch.com/cafe/miscellaneous/commtouch-com-ready-for-ipv6-day-%e2%80%93-8th-june-2011/>
- <http://blog.commtouch.com/cafe/web-security/another-fake-%e2%80%93-facebook-profile-views-%e2%80%9d-application-how-many-girls-and-boys-have-viewed-your-wall/>
- <http://blog.commtouch.com/cafe/malware/forex-stat-arb-malware-disguised-as-pdf-steals-user-data/>
- <http://blog.commtouch.com/cafe/malware/yeheytv-searchers-end-up-watching-fake-antivirus-seo-poisoning/>
- <http://blog.commtouch.com/cafe/malware/your-irs-eftps-payment-rejected-malware/>
- <http://blog.commtouch.com/cafe/malware/nacha-payment-rejected-%e2%80%93-malware/>
- <http://www.commtouch.com/threats-ipv6>
- <http://www.commtouch.com/introduction-ipv6>

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.