

# Internet Threats Trend Report October 2011





## In This Report

<b>Email malware returns</b> – huge outbreaks in Q3	<b>Page 2</b>
<b>Exe spelled backwards = malware</b> – right-to-left override used to trick users	<b>Page 4</b>
<b>Gap Athleta</b> – Phony orders include convincing shopping list	<b>Page 4</b>
<b>Spam still low</b> – Massive malware outbreaks don't add new spam-zombies	<b>Page 6</b>
<b>Compromised accounts</b> – Commtouch initiates industry's first research	<b>Page 7</b>
<b>Facebook friend requests lead to malware</b> – Exploiting the hype	<b>Page 10</b>
<b>PHPThumb exploit</b> – legitimate websites used as spam-sending machines	<b>Page 11</b>
<b>Zombie hot spots</b> – Brazil continues to drop, US goes back up	<b>Page 14</b>

## Q3 2011 Highlights

### ▼ 93 billion

Average daily spam/phishing emails sent  
Page 6

### ▼ 336,000 Zombies

Daily turnover  
Page 14

### ▲ Streaming media/ Downloads

Most popular blog topic on user-generated content sites  
Page 15

### ▲ Pharmacy ads

Most popular spam topic (29% of spam)  
Page 8

### ▲ India

Country with the most zombies (18%)  
Page 14

### ▲ Parked Domains

Website category most likely to be contain malware  
Page 12

## Overview

The third quarter saw an explosion of email-borne malware to the highest levels observed in over two years. The ultimate purpose of the huge volumes of malware has remained unclear. Typically, a short while after such a large outbreak, spam levels would increase, however in this case, spam levels continued to decrease. The spread of malware to the Android platform prompted the inclusion of Android virus samples in the Extended Wildlist released during Q3.

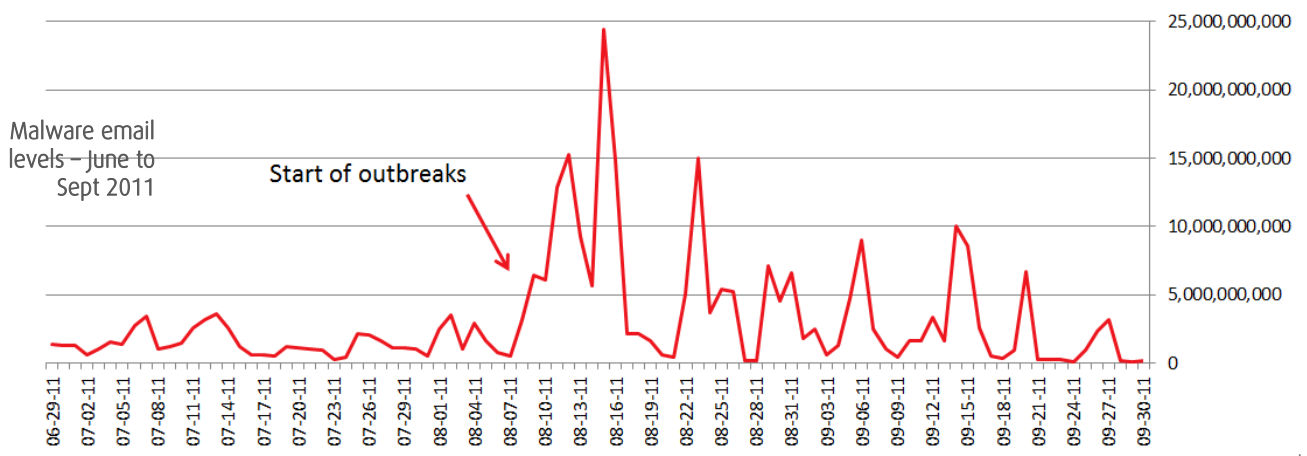
Commtouch Labs observed continued use of compromised accounts to send spam and scams, and undertook a survey to gauge trends related to the theft, usage and recovery of these accounts. A selection of the survey results are presented below. The full report is available here: <http://www.commtouch.com/state-of-hacked-accounts>

## Malware trends

### Email-malware returns

2010 saw steadily decreasing levels of email-attached malware to less than 1% of malicious emails (spam, phishing, malware). In March 2011, this trend abruptly ended with large outbreaks of courier-themed emails with zipped malware attachments. In the following months though, email with malware attached took a brief hiatus, returning to the minimal levels seen prior to March.

In August 2011, however, email-malware returned in several enormous waves with attacks continuing throughout September. The increase is clearly illustrated in the graph below. Pre-outbreak levels varied between a few hundred million emails to around 2 billion malware-emails per day. The peak outbreak included distribution of nearly 25 billion emails with attached malware in a single day.



A review of several end-user forums reveals that the malware campaigns have been successful – with many users having opened the malware attachments. The infection rate is generally linear – the more malware that is emailed, the greater the final number of infections.

A range of malware families have been detected in the outbreaks including variants of Sasfis, SpyEye, Zeus, Fake antivirus, and others. In almost all case the malware contacts external

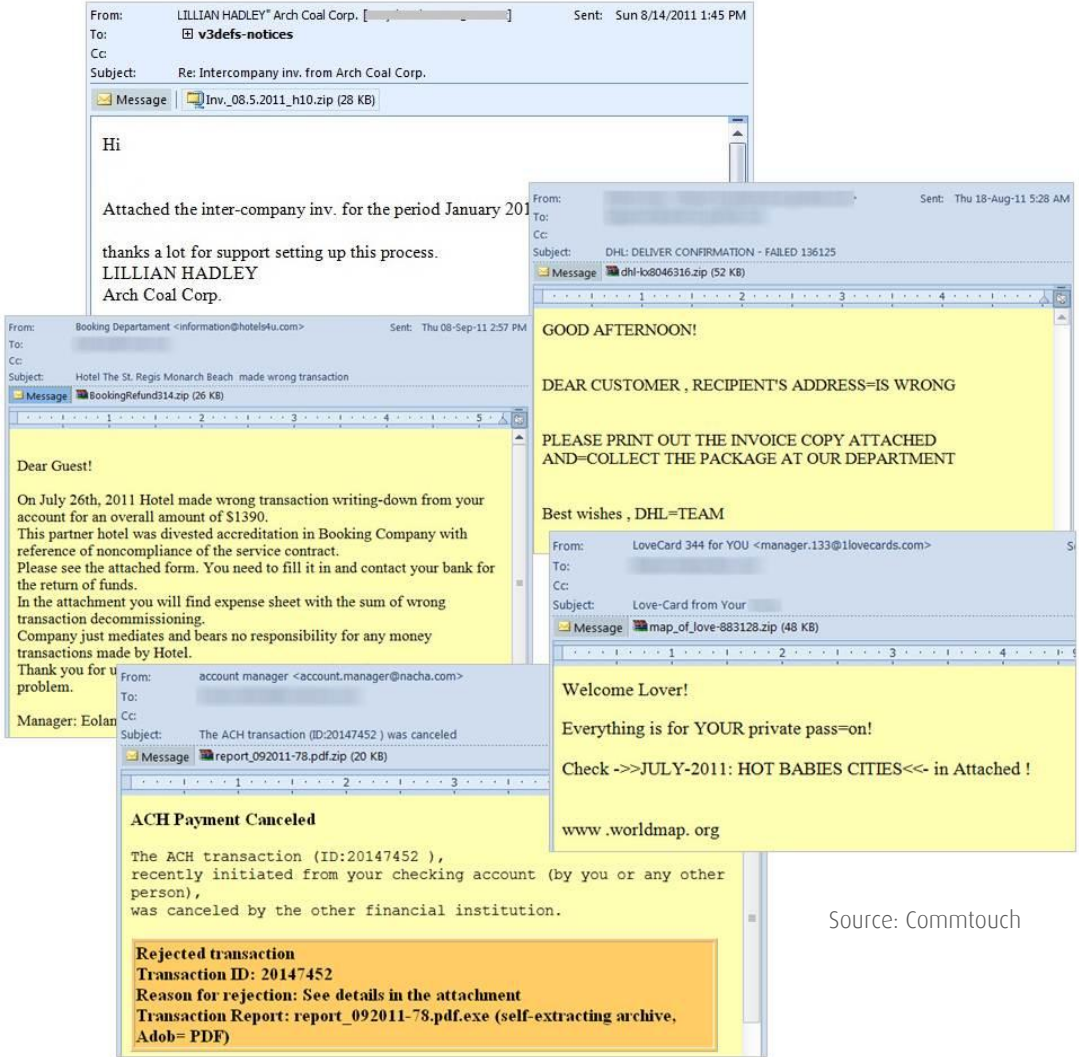
# October 2011 Internet Threats Trend Report

servers and downloads several other malware files which are then run on the infected machine.

Each of the malware types mentioned above have generally been associated with a certain type of malicious activity, for example, Zeus with banking fraud. The vast scale of the attacks though, combined with the methodical use of recurrent themes suggests a more general purpose for the millions of newly recruited bots.

In the past, large botnets have been used to send high volumes of spam. Malware distribution therefore aimed to increase spam distribution, but this does not seem to be the case now. The spam levels of the past few months are shown on page 6 below, with the flat, generally decreasing trend clearly visible. The malware outbreaks of the last month do not appear to have had any effect on the levels of spam being sent.

Malware emails with varied themes used in attacks



Source: Commtouch

There are several other potential alternatives for the use of a huge botnet such as: large scale banking fraud, Facebook/Gmail/Yahoo account theft, distributed denial of service (DDOS), or some other criminal activity. At this time, the specific purpose of the vast malware outbreaks

is still unclear, since there have been no reports of significant increases in banking fraud, account theft, DDoS or other activities.

The various peaks of the malware outbreaks each represented different “themes” used to trick users into opening the attachments. These included:

- Courier (UPS, Fedex, DHL) package notifications - a notification of a package that is due to arrive or has been held up, with more details promised in the attached notice.
- Hotel charge error – an erroneous hotel bill needs to be corrected by opening the attached form.
- The “map of love” - promising juicy information about global sites of “interest” in the attached map.
- Credit card errors – an incorrect credit transaction needs to be reversed with more details in the attached.
- HP scanner doc – a document scanned on the office scanner has been delivered
- Inter-company invoice – includes a confusing message about an attached invoice.
- NACHA errors – an inter-banking transaction has been rejected. The reasons for the rejection are in the attached document.

## Unicode Right-to-Left override trick used extensively

In many of the emails with attached malware, the attachments display an Adobe PDF icon even though they are executable files. This is designed to fool users who do not display or look closely at file extensions in Windows.

Many of the attachments also used a Unicode control character with a right to left override (RLO) function, so even if the user saw the file extension, he would perceive it as harmless. This Unicode control character (U+202E) reverses the character reading order from the traditional left-to-right, to right-to-left. This is mainly used for right-to-left languages (such as Arabic or Hebrew). Malware uses RLO to reverse the direction of text in a filename as shown in the example below (this example is extracted from one of the “Inter-company invoice” themed emails described above).



Source: Commtouch

The RLO control character is not displayed. It is placed just before the part of the filename “exe.doc”. The actual filename is:

“CORP\_INVOICE\_08.14.2011\_Pr.phylcod.exe”

As shown in the screen above, the effect is very convincing and users believe they are opening a harmless .doc file. The same trick was also used to display “fdp.exe” as “exe.pdf”.

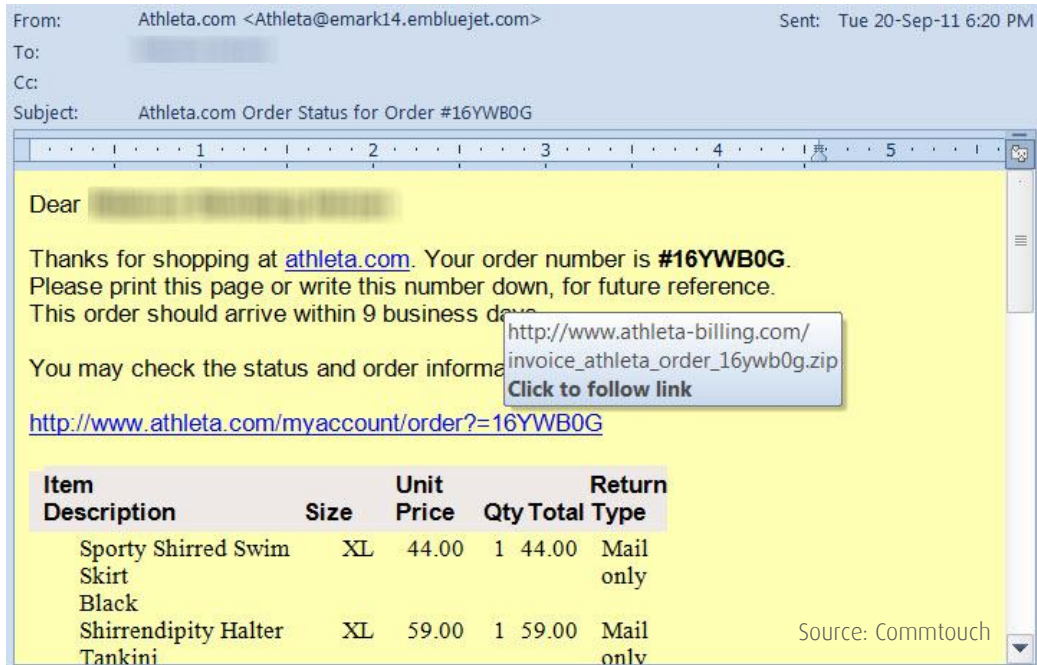
## Gap.Athleta shopping malware

A September outbreak of password-stealing malware lured victims with a phony order status email from Athleta (part of the Gap clothing chain). The widely distributed emails contained

# October 2011 Internet Threats Trend Report

very limited variations of a list of “chosen” items. The attack is notable for the successful social engineering, with many recipients reporting that they were intrigued by the clothes that had been selected.

Phony order status email from Athleta – link leads to malware download



Clicking on the “order status” or “return policy” URLs in the email message downloaded a zip file which included the executable “invoice\_athleta\_order—.exe.” If opened, the malware determined the geographical location of the recipient and sends the results to a control server. The malware then copies or downloads several other pieces of malware: “google.exe”, “googles.exe”, “googletools.exe” and “SOD.exe.”

“googletools.exe” downloads a configuration file with a list of sites and URLs. Browsing to these sites will trigger another bit of malware, most likely logging keystrokes or taking screenshots in order to steal login usernames and passwords. Among the sites that trigger this behavior are: Amazon, AT&T, Bank of America, Best Buy, CHASE Home, Citibank, Craigslist, Facebook, Fifth Third Bank, Go Daddy, Google Checkout, IMVU, LastPass, Moneybookers, Myspace, Netflix, Newegg, PayPal, PlayStation, RapidShare, RoboForm, Target, T-Mobile, U.S. Cellular, Verizon, Walmart.com, WebMoney, Western Union, and World of Warcraft.

# October 2011 Internet Threats Trend Report

## Top 10 Malware

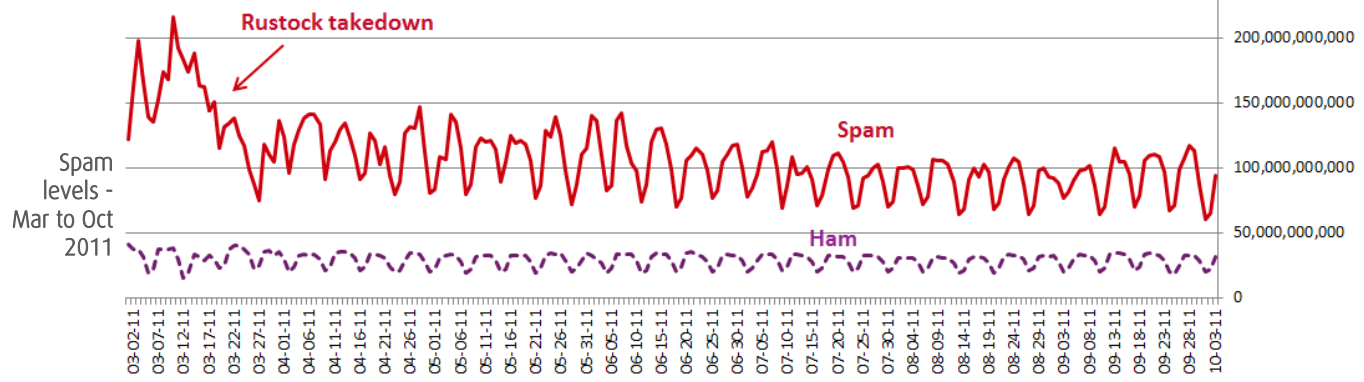
The table below presents the top 10 most detected malware during the third quarter of 2011 as compiled by Commtouch's Command Antivirus Lab.

Top 10 Detected Malware			
Rank	Malware name	Rank	Malware name
1	W32/Oficla.FO	6	W32/Patched.G
2	W32/RAHack.A.gen!Eldorado	7	W32/Damaged_File.B.gen!Eldorado
3	W32/Adware.PAP	8	W32/Bredolab.AP.gen!Eldorado
4	W32/Sality.gen2	9	W32/MalwareF.AFPRH
5	JS/Pdfka.BG	10	W32/Heuristic-210!Eldorado

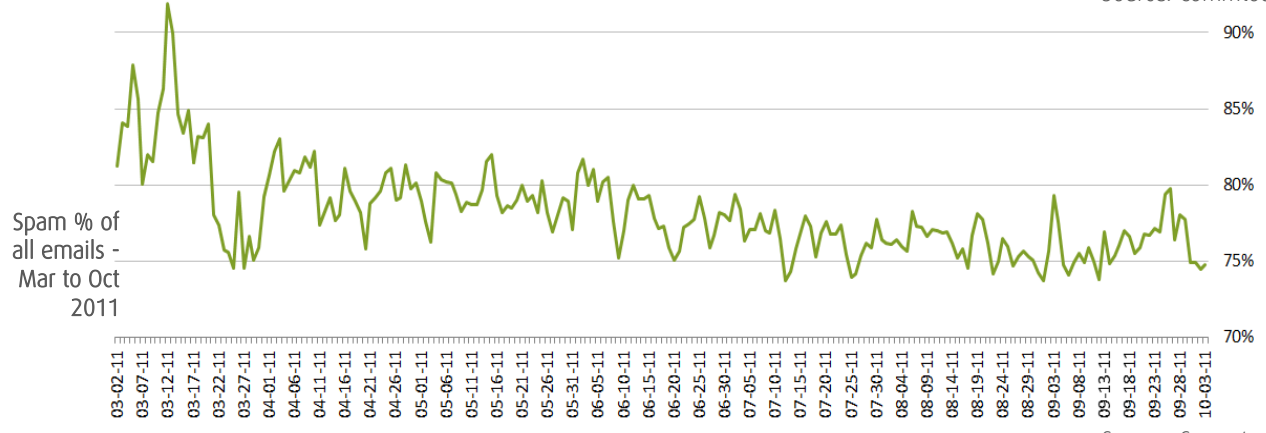
Source: Commtouch

## Spam trends

Spam levels have remained at their lowest in years following the Rustock botnet takedown in March. As described above, the large malware outbreaks of August and September have had no effect on spam levels which averaged near 93 billion messages per day. Spam averaged 76% of all emails sent during the third quarter (excluding emails with malware attachments).



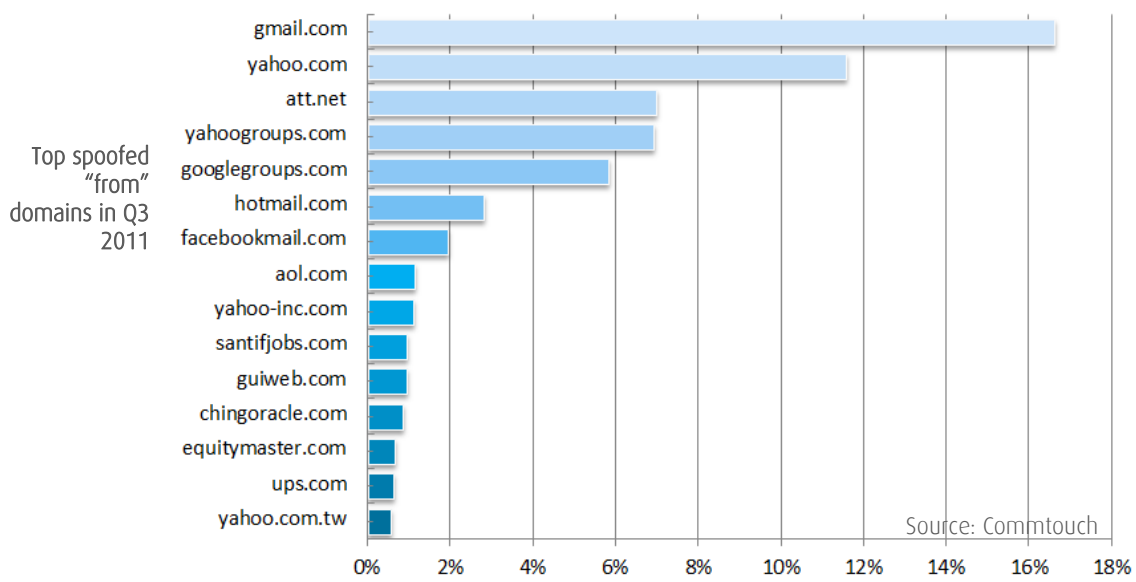
Source: Commtouch



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.



This quarter, gmail.com is once again the most spoofed domain. 14<sup>th</sup> place is again held by ups.com due to the very large numbers of fake UPS notification emails sent as part of the outbreaks of the quarter.

## Compromised accounts survey

In addition to the spoofed emails (shown above), a percentage of the emails from Gmail, Hotmail and Yahoo actually come from genuine accounts. Often these are compromised accounts (though they can be accounts specifically created by spammers for this purpose).

The Trend Report of the last quarter described the current spammer tactic to make more use of compromised accounts to send spam (as opposed to botnets). The blocking of spam from compromised accounts based on IP address is more difficult for anti-spam technologies that rely solely on IP-address-based rules. The reason is that these stolen accounts exist within whitelisted IP address ranges (such as Hotmail or Gmail). Spam sent from a stolen account is therefore much more likely to get through.

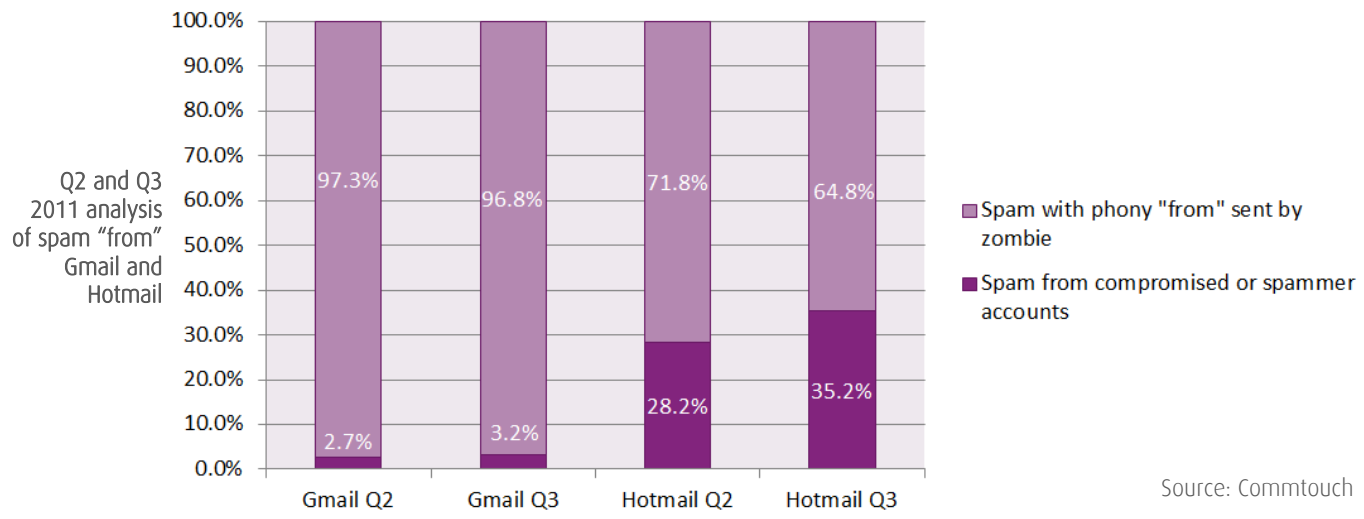
The graph below compares the percentage of spam received over sample periods in Q2 and Q3 2011, where the "from" field includes "Gmail" or "Hotmail". Based on the IP address, received spam could either be:

- 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, between 28-35% of the spam from Hotmail actually comes from compromised or spammer Hotmail accounts. Gmail spam, on the other hand, is mostly (96-97%) from zombies that simply forge Gmail addresses.

# October 2011 Internet Threats Trend Report

The collected data shows compromised accounts growing in Q3 for both Hotmail and Gmail.



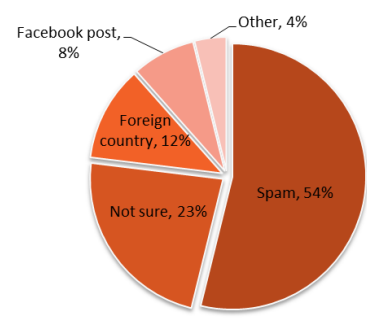
Having observed greater use of compromised accounts, Commtouch undertook primary research into the use of compromised accounts for spam by surveying people whose accounts had been compromised.

The results confirm what Commtouch has observed with regard to compromised account use. Over half of the compromised accounts were used to send spam or scams according to the respondents in the survey. 23% of respondents were not sure what their accounts were used for – having simply been informed that they had been victimized. It is safe to assume that most of these were used to send spam or scams as well. Compromised Facebook accounts were generally used to further the spread of malware or post links to marketing scam websites.

In addition to analyzing how compromised accounts were used, these aspects were also researched:

- Which accounts were affected
- How the account was compromised
- How the account owner found out
- What action they took to regain control of the stolen account

The full results of the survey are available for download at:  
<http://www.commtouch.com/state-of-hacked-accounts>



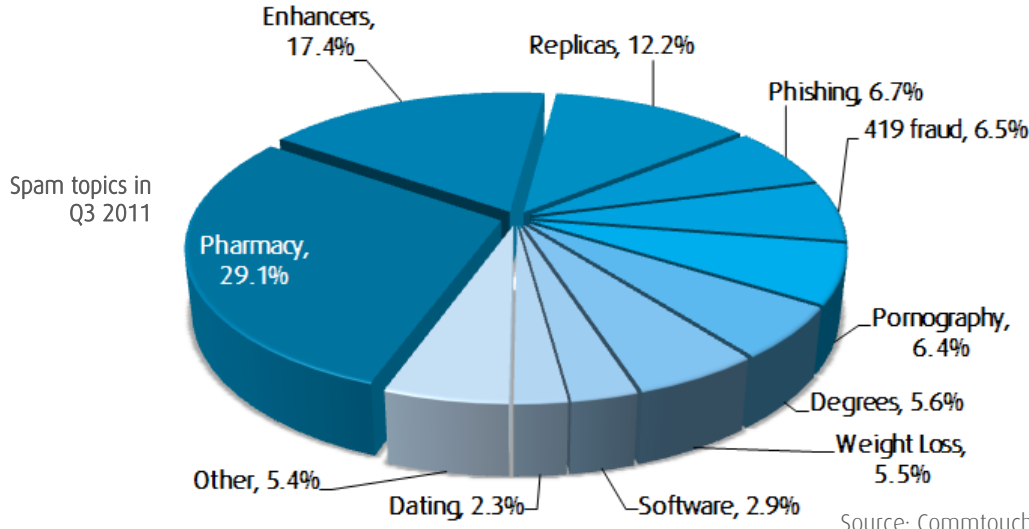
### What was done with the stolen account?

- Used to send spam promoting a product
- Used to ask my friends to send me money since I was "stuck in a foreign country"
- Used to send a phony message/wall post on my Facebook account
- Not sure - I was just told it was compromised
- Other

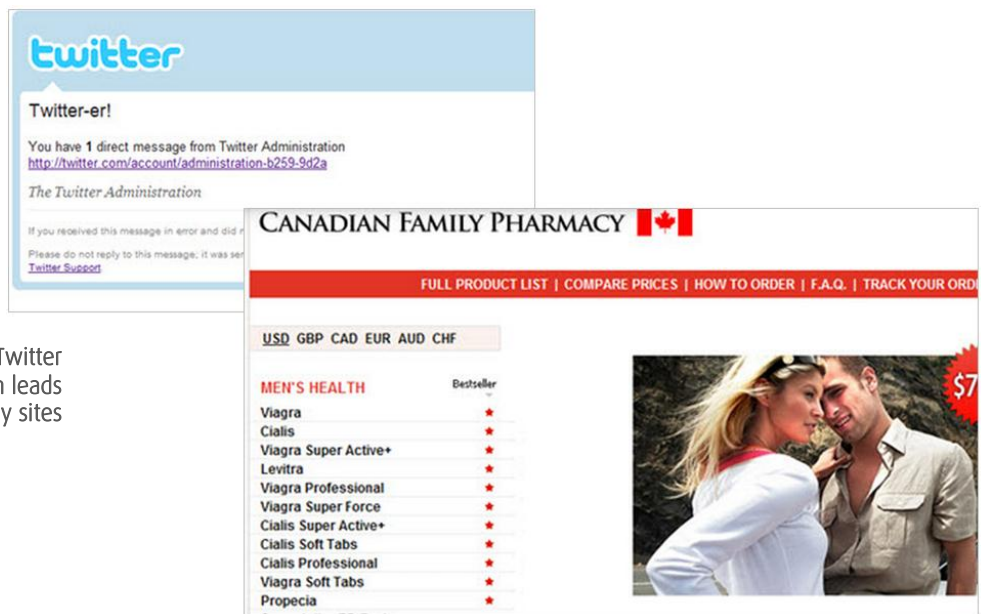
Source: Commtouch

## Spam topics

Pharmacy spam finally stopped its downward slide of the past six quarters and increased to reach 29% of all spam (5% more than the previous quarter). Enhancers also added 5 points and accounted for more than 17% of spam.



Pharmacy spammers continue to use direct emails where the subject explicitly states that the email is offering medicines or alternatives. Since much spam ends up in quarantine or junk email folders, there is apparently a percentage of people who will be interested in the offered product and who will open the email even from those folders. Indirect emails were also used extensively – such as the Twitter and Facebook examples below. The spammers lure recipients with phony notification emails.



Phony Twitter notification leads to pharmacy sites

Source: Commtouch

## Web security

### Facebook friend malware and "like" scams

Facebook continues to draw the attention of malware authors. An August attack used a range of "friend request" emails to draw recipients to a download of a banking Trojan.

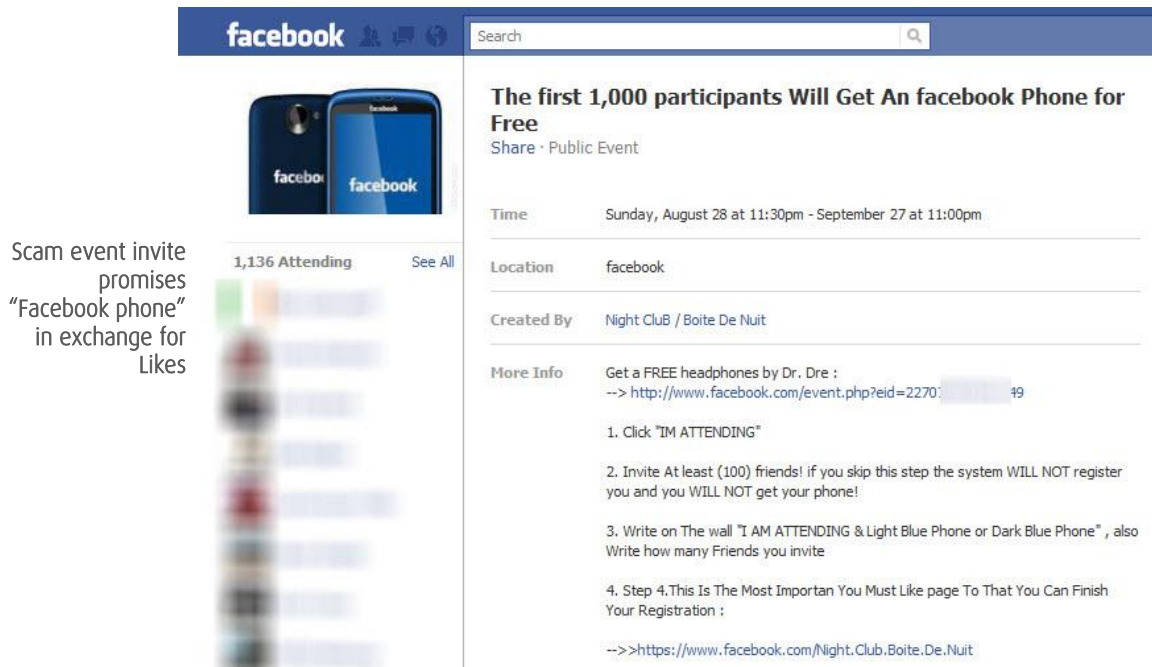


Phony Facebook friends request leads to malware

Source: Commtouch

Scammers also went after Facebook "likes" in a series of September campaigns. The scams were spread as events with titles such as:

- "The First 50.000 participants Get an iPhone 4 for free"
- "The first 25,000 that signup get a free pair of Beats by Dre headphones"
- "The first 1,000 participants Will Get An Facebook Phone for Free"
- "The First 25,000 Participants Will Get A Free Facebook Hoodie"



Scam event invite promises "Facebook phone" in exchange for Likes

Source: Commtouch

# October 2011 Internet Threats Trend Report

Those wanting to receive the “free” merchandise were asked to like several pages, provide their shipping addresses and forward the invite on to 100 or so friends – thus ensuring the spread of the scam. The pages were liked by hundreds of thousands of Facebook users.

The benefits of being “liked” for the scammer include:

- The like appears on the Liker’s Wall and may also appear in News Feed, generating free publicity for the scam, to bring in other potential victims.
- The Liker will be displayed on the Page that was liked, in advertisements about that Page, lending credibility to the scam
- The liked Facebook Pages may post updates to the Liker’s News Feed or send them messages, promoting additional scams.

In addition to these advantages, the scammers also obtained people’s shipping addresses which could be combined with other information available on their profiles for identity theft. One of the offers (The Facebook Hoodie) links to an external site with further links to marketing scams that bring the scammer per-click revenues.

## PHP Thumbs exploit

Thousands of websites use a script called “PHPTThumb” to manage the images on their webpages. The script allows page designers to fix image sizes, add watermarks and perform other image-related actions as pages are generated.

PHPTThumb script used to manage images on a site

1 Image as it appears on blogsite

2 PHPTThumb script used to resize image

Source: Commtouch

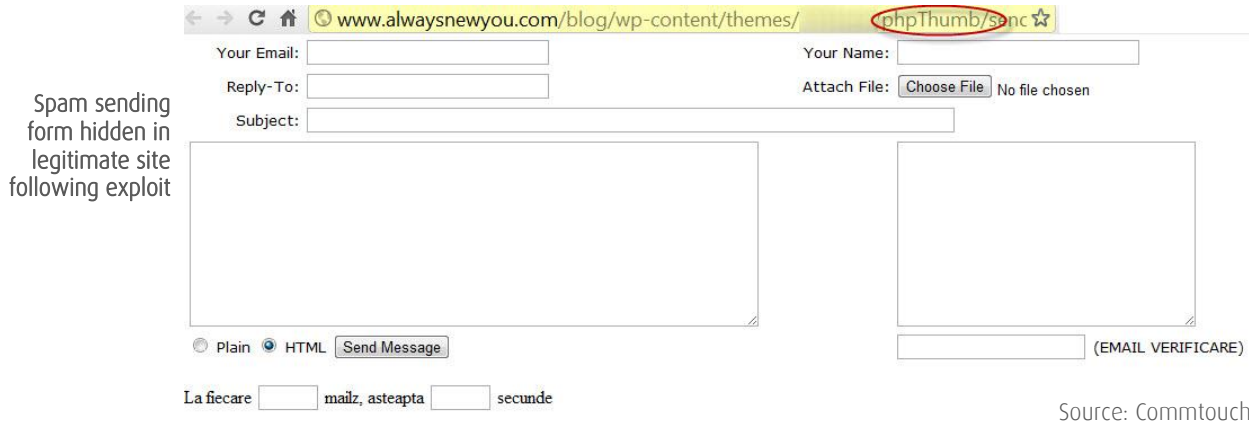
PHPTumbs also includes a vulnerability (already documented over 5 years ago) that allows an attacker to run any code they wish on the target website. In August, masses of spam and phishing emails were sent from sites that were hacked using the PHPTumbs exploit. The vulnerability allowed hackers to install email-sending code on the Web server – usually in the PHPTumbs directory. The inserted code (sendme.php) presents a neat and easy-to-use spam/phishing sending form that looks like this:

The form allows a spammer to control all aspects of the sent message:

- The sender fields such as “from”, “reply-to”, and sender name

# October 2011 Internet Threats Trend Report

- Target addresses (of multiple recipient at once)
- Attachments, HTML formatted content, etc.



The advantage of this technique for spammers is the source of the emails – since these are sent using a reputable IP address (from the compromised websites). These emails can therefore more easily evade anti-spam systems that rely on IP reputation. The spammer can send an almost unlimited number of emails from the compromised web server.

## Categories of compromised sites with malware

During the third quarter of 2011, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware. Pornographic and sexually explicit sites were pushed down to the 3<sup>rd</sup> spot by parked domains and portals. As noted in previous reports, the hosting of malware may well be the intention of the owners of the parked domains and pornography sites. 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	Parked Domains	6	Business
2	Portals	7	Computers & Technology
3	Pornography/Sexually Explicit	8	Health & Medicine
4	Education	9	Shopping
5	Entertainment	10	Travel

Source: Commtouch

## Categories of compromised sites with phishing

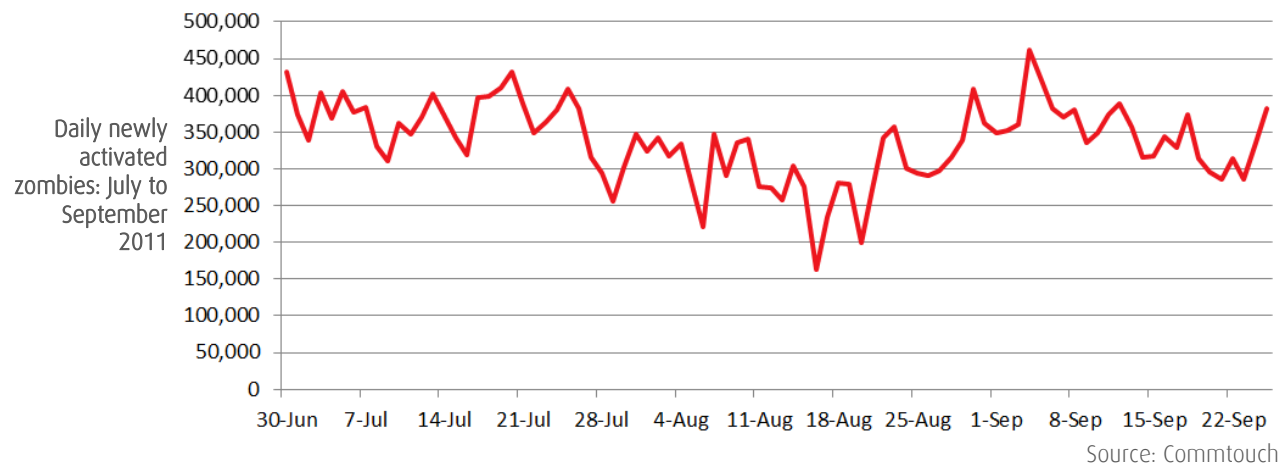
During the second quarter of 2011, Commtouch analyzed which categories of legitimate Web sites were most likely to be hiding phishing pages (usually without the knowledge of the site owner). Sites related to games ranked highest, similar to last quarter.

Website categories infected with phishing				
Rank	Category		Rank	Category
1	Games		6	Sports
2	Portals		7	Leisure & Recreation
3	Shopping		8	Business
4	Fashion & Beauty		9	Health & Medicine
5	Education		10	Entertainment

Source: Commtouch

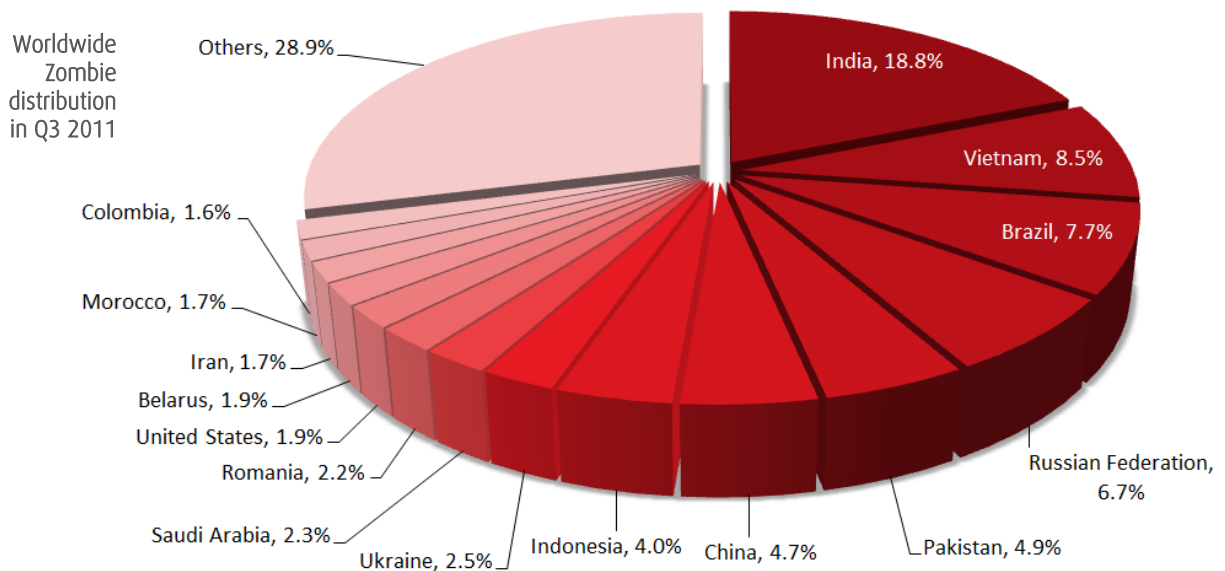
## Zombie trends

The third quarter saw an average turnover of 336,000 zombies each day that were newly activated for sending spam. This number shows a slight decrease compared to the 377,000 of the first quarter of 2011. As described above (page 2), the large malware outbreaks of the quarter have not greatly increased the number of spam-sending zombies.



## Zombie Hot Spots

India again claimed the top zombie producer title, increasing its share to over 18%. Brazil dropped to 3<sup>rd</sup> position by decreasing its share of the global zombie population by nearly 3%. The US, and Iran joined the top 15, displacing Poland and Italy.



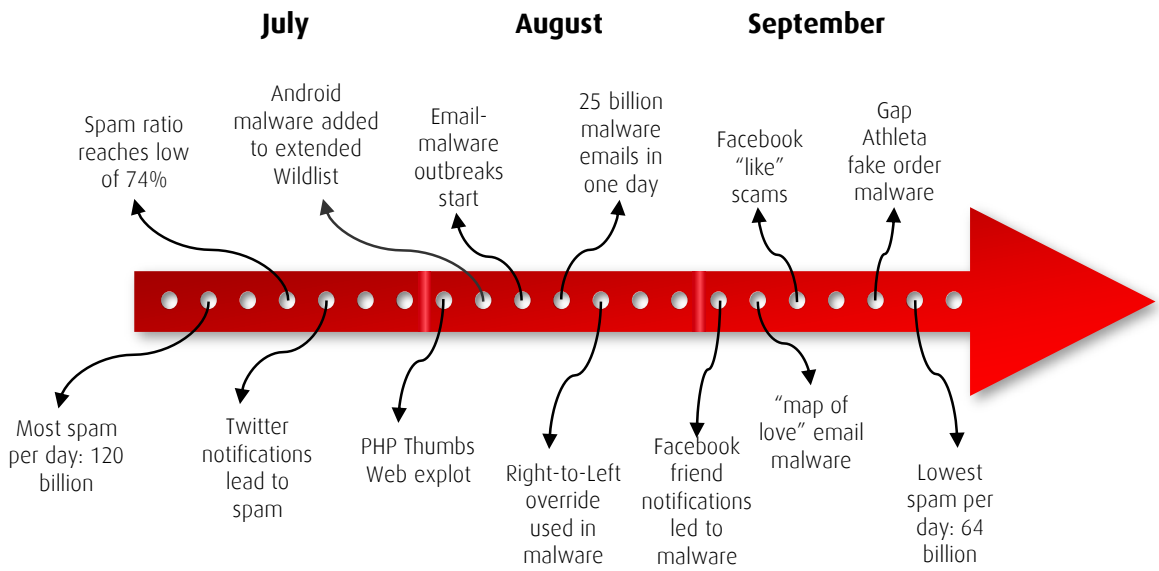
## Web 2.0 trends

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, increasing its share to nearly one quarter of user-generated content. The streaming media & downloads category includes sites with MP3 files or music related sites such as fan pages (these might also be categorized as entertainment).

Most popular categories of user-generated content						
Rank	Category	Percentage	Rank	Category	Percentage	
1	Streaming Media & Downloads	24%	8	Arts	5%	
2	Entertainment	9%	9	Sports	4%	
3	Computers & Technology	8%	10	Education	4%	
4	Pornography/Sexually Explicit	6%	11	Leisure & Recreation	3%	
5	Fashion & Beauty	5%	12	Health & Medicine	3%	
6	Religion	5%	13	Games	3%	
7	Restaurants & Dining	5%	14	Sex Education	2%	

Source: CommTouch

## Q3 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](http://www.pallas.com) or write information (at) 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/spam-favorites/shopping-in-my-sleep/>
- <http://blog.commtouch.com/cafe/data-and-research/has-your-emailfacebook-account-been-compromised-complete-our-2-minute-survey/>
- <http://blog.commtouch.com/cafe/email-security-news/step-1-infect-millions-of-computers/>
- <http://blog.commtouch.com/cafe/malware/incorrect-hotel-charges-%e2%80%93-install-malware-for-refund/>
- <http://blog.commtouch.com/cafe/web-security/facebook-the-first-1000-participants-get-facebook-phone/>
- <http://blog.commtouch.com/cafe/malware/the-map-of-love-leads-to-trouble/>
- <http://blog.commtouch.com/cafe/email-security-news/facebook-friends-that-you-don%e2%80%99t-need/>
- <http://blog.commtouch.com/cafe/malware/welcome-to-android-malware/>
- <http://blog.commtouch.com/cafe/antivirus/email-malware-levels-skyrocket/>
- <http://blog.commtouch.com/cafe/malware/exe-read-backwards-spells-malware/>
- <http://blog.commtouch.com/cafe/malware/a-wild-malware-rollercoaster-%e2%80%93-over-500-increase/>
- <http://blog.commtouch.com/cafe/phishing/compromised-websites-phphthumbs-exploit/>
- <http://blog.commtouch.com/cafe/malware/this-week%e2%80%99s-facebook-and-twitter-abuse/>

Visit us: [www.commtouch.com](http://www.commtouch.com) and [blog.commtouch.com](http://blog.commtouch.com)

Email us: [info@commtouch.com](mailto:info@commtouch.com)

Call us: 650 864 2000 (US) or +972 9 863 6888 (International)

**commtouch®**  
Real Security. In Real Time.