Internet Threats Trend Report
January 2012

commtouch®

commtouch®
Real Security. In Real Time.

In This Report

Q4 2011 Highlights

▲ **101 billion**

Average daily spam/phishing emails sent

Page 11

▼ **209,000 Zombies**

Daily turnover

Page 16

▼ **Streaming media/ Downloads**

Most popular blog topic on user-generated content sites

Page 17

▲ **Pharmacy ads**

Most popular spam topic (31.2% of spam)

Page 13

▲ **India**

Country with the most zombies (23.5%)

Page 16

▲ **Parked Domains**

Website category most likely to be contain malware

Page 14

Overview

The last months of 2011 saw an increase in free-merchandise scams on Facebook. This trend report includes a study of Facebook attacks in 2011 revealing that many rely solely on social engineering while most ultimately lead victims to fraudulent affiliate marketing/survey sites.

In the fourth quarter of 2011 email attached malware levels dropped significantly from the billions of messages observed in Q3. These were replaced with numerous outbreaks of emails with malicious links. Most of these links led to compromised websites that were used to host malware scripts. Spam levels increased marginally in December but remained at a three year low.

Facebook security – a 2011 retrospective

Facebook continued to grow in 2011, adding over 200 million more users to reach over 800 million. The growth and enormous user base continues to make Facebook an attractive target for attacks from malware distributors, scammers and plain old jokers looking to spread chain messages. Facebook attacks can generally be broken into three parts:

1) **The social engineering** – this is the false information provided in the post or invite that inspires action by a Facebook user. It could be a free gift card offer or the promise of a girls-in-bikinis video.
2) **Further spread** – once the initial user has been hooked, the attack needs to spread. This is usually accomplished with wall posts which are seen by the victim's friends. These friends then follow the links, further perpetuating the attack. An important part of the Facebook ecosystem (and often used to spread attacks) is the "Like" button. When a user likes a link or a post, all of their friends see the like on their own news feeds. Liking a page (company, singer, cybercriminal) gives that page the right to post updates to the user's wall.
3) **The attack goal** – Whoever initiated the attack had some ultimate purpose – it might simply be to deface as many user profiles as possible with pornography and violent images. More often the aim is to lead users to affiliate marketing pages which earn the attackers revenue.

From the attacks reported in 2011, 70 have been analyzed to determine the distribution within the three parts described above.

Social engineering

What interests Facebook users most? What will get them to take the next step (click like, follow a link, add an app) that suits the cybercriminals. The topics of interest can basically be divided into four categories:

Post with free gift card scam

Source: Commtouch

1) Free stuff – in 2011 scammers offered loads of free items ranging from headphones to gift cards to unreleased Facebook phones.

Event publicizing free Facebook phone scam

Source: Commtouch

2) Celebrity or current news scoops – These usually include sensational headlines and promise some unreleased video clip or photo. An example is the death of Osama Bin Laden which was quickly followed by numerous posts inviting users to view an actual death video. The death of Steve Jobs also triggered a wave a "free iPad/iPhone" scams.

Event following the death of Steve Jobs with free iPhone scam

Source: Commtouch

3) Something "you have to see" – These could be any tragic or astonishing event that is not celebrity related. "Girls in bikinis", "a funny photo of you", "a tragic story of a boy who was beaten by his father" – all presented with a call to action. Users must follow a link, or click on Like to see a shocking/amazing video or photo, or forward a chain message to let other users know. The Spanish in the example below translates to "Look what happens".

Post tempts users with "look what happens next" and link to video

Source: Commtouch

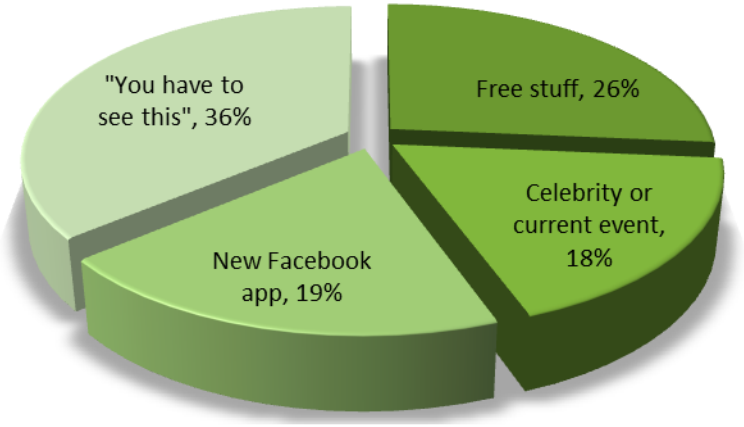
4) Must-have Facebook functionality – the most popular of these (repeated in many attacks) is the mythical app that allows users to see who has been viewing their profile. The post shown below invites users to install an app that tells them the breakdown of boy and girl views of their profile.

Post promising app that reveals who has been viewing a user profile

Source: Commtouch

In 2011 the social engineering themes were spread fairly evenly between the four types described above. Of the attacks analyzed, 36% belonged in the "you have to see this" category. "Free stuff" themed scams (26%) were more common in the second half of 2011.

Facebook attacks: Social engineering used to convince users to take action



Source: Commtouch

Spreading the attack

One of the benefits of Facebook is the inherent trust of a network of friends. This trust also benefits cybercriminals who can use one Facebook user as a starting point to reach out to multiple friends in order to ensure the spread of an attack. Here to, there are several common methods used:

1) Tricking users into sharing – this is pure social engineering – users are aware that they are liking or sharing a page, but are probably doing so under false pretenses. Users fall for scams promising free gift cards in exchange for a like or share. Alternatively they may post a hoax that they believe to be true warning other users about a (nonexistent) virus or telling them the sad tale of a (nonexistent) abused child. In the Costco scam shown below users must first click on "share" and then on "like" to get their "free gift card".

Free gift card scam requires that users willingly click on "like" and "share"

Source: Commtouch

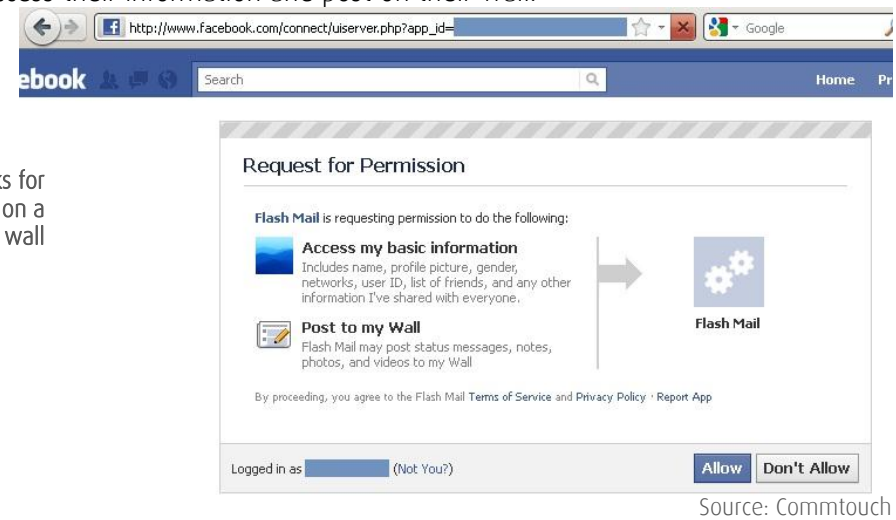
2) Likejacking – in most likejacking attacks, Facebook users will be shown a video player after following some sensationalist link. The player may be functional but the page will include scripts that use any mouse click to generate a like that will lead more friends to the video page. Users are therefore unaware that they have liked a page. Users clicking on a post about girls in Bikinis would arrive at the video player shown below. Clicking on the play button starts a video but also results in a like being generated to their friends that will drive more users to the site.

Site with clickjacking script. Clicking on the play button of the video player generates unwanted likes and shares. Advertising around player generates revenues.

Source: Commtouch

3) Rogue applications – these apps are added by users who believe they will be providing worthwhile functionality – most often, the ability to know who has viewed a user's content. As part of the process of adding an app, users will give that app permission to access parts of their profile and of course post on their wall. This ability to post allows the rogue app to spread itself further within Facebook. The rogue app below is supposed to reveal who has been viewing your profile – as shown users who click on "allow' will be giving the app permission to access their information and post on their wall.

Rogue app asks for permission to post on a user wall

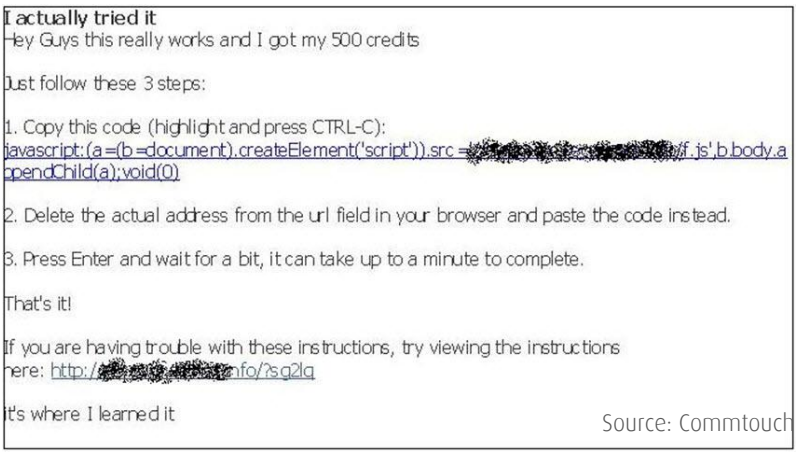


Source: Commtouch

4) Malware and "self-XSS" – In these cases the user has unwittingly installed malware on their PC. This malware can then hijack their Facebook session for posts or any other activity. Traditional cross-site scripting (XSS) attacks rely on some hidden script within a webpage that hijacks a Facebook session. Self-XSS means that a malicious script was activated by a user (the "self") giving another site access to the Facebook session. In

these attacks, users are asked to enter a line of text directly into their browser address bars in order to see some "exciting" content. When users paste the text provided into their browser they are effectively telling their browser to act on their behalf and do whatever the script says – in most cases it will visit an external site (the "cross-site" of "cross-site scripting") and then be told to post a wall post or an event invite. This perpetuates the attack as friends see the posts and follow them.

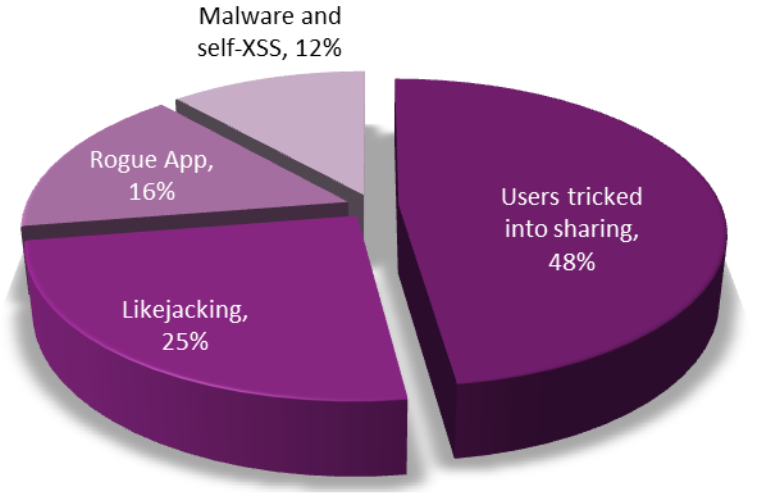
"self-XSS" attack: users are instructed to paste JavaScript into the browser address bar. The script activates code from another site within the user session



Source: Commtouch

In 2011, most attacks were spread by users without the need for any hidden scripts or malware. In almost 48% of the attacks, users willingly clicked on Like or share in order to get some bogus free item or in order to view some scandalous content. Although likejacking accounted for nearly 25% of the spreader mechanisms, the second half of 2011 saw reduced reports of this technique.

Facebook attacks – how attacks are spread between friends



Source: Commtouch

The attack goal

The user has been tricked with social engineering, the attack has been further spread using one of the techniques listed above, and now the cybercriminal must reap whatever reward they set out for. These may be divided into the following categories:

1) Fraudulent marketing affiliate/survey sites – users are led to believe that completion of a questionnaire or a form will result in a free gift (iPhone, gift card, cap, etc.).

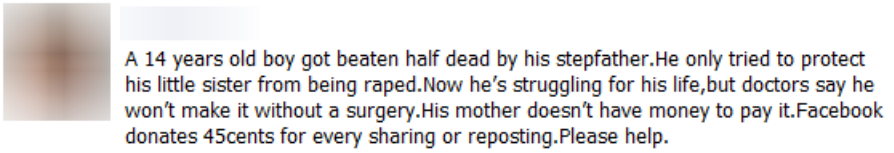
Cybercriminals receive affiliate payments for driving these users to the sites with these offers. Users may be tricked into signing up for unwanted products or may simply be providing personal information that will later be used for identity theft. . Legitimate businesses are often defrauded of their affiliate marketing budget by having them included in these pages.

Fraudulent marketing affiliate/survey site

Source: Commtouch

2) Chain posts and hoaxes – fake stories that have done the email rounds many years ago are receiving a second life in the world of Facebook. Users like or share stories of abused children or devastating computer viruses without bothering to verify whether there is a shred of truth in the story. The aim here is the same as it was 10 years ago – pranksters having a laugh at the expense of unaware Internet users.

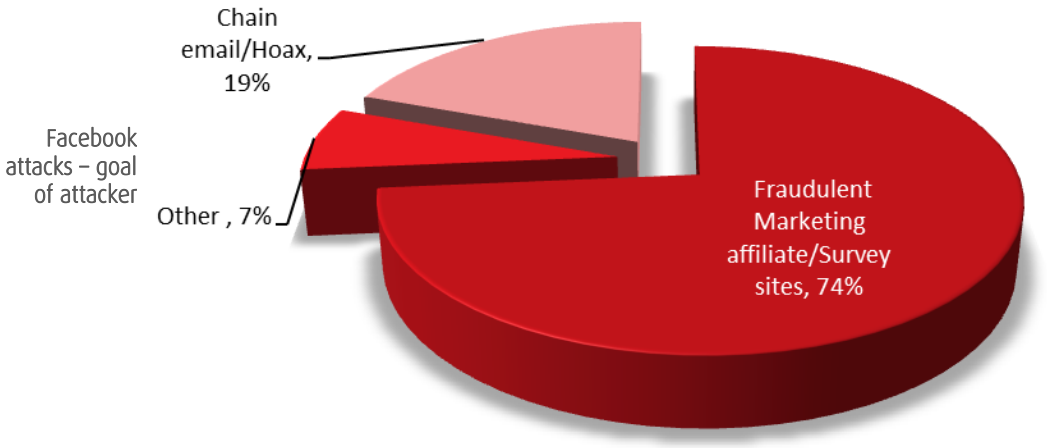
Hoax chain post convinces users they are helping by sharing and reposting



Source: Commtouch

3) Other – A small percentage of attacks with very different goals including
   a. Defacement – particularly the November attack that spread pornographic and violent images on many user walls. The aim of the attack seems to have been embarrassing Facebook.
   b. Spreading malware – where the aim of the malware may not be exclusively limited to Facebook posts i.e.: malware that steal passwords or sends spam.
   c. Collecting Likes – attacks that resulted in enormous likes of a page (several hundred thousand in some cases) but with no clear further malicious purpose.

The vast majority (nearly 74%) of Facebook attacks in 2011 were designed to lead users to fraudulent marketing affiliate/survey sites. Surprisingly chain posts and hoaxes accounted for nearly 20%.



Source: Commtouch

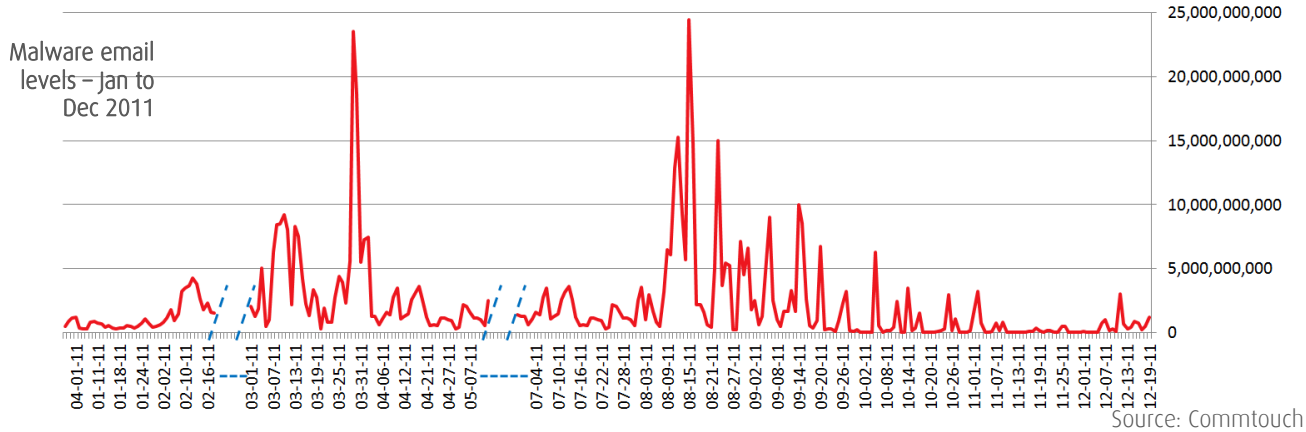
Looking ahead

A review of 2011 shows some progress, with various attacks being more quickly detected and removed by Facebook. In addition there are almost no recent reports of rogue applications compared to the numerous examples from the first half of the year. Some attack methods were almost completely eliminated – such as the self-XSS method. In this case the major browser vendors provided updates which do not allow users to paste scripts directly into the address bar. On the other hand, "Free merchandise" scams are still common. 2012 will no doubt reveal new cybercriminal tactics – Facebook is too large a target to ignore.

Malware trends

Email-malware subsides, blended threats increase

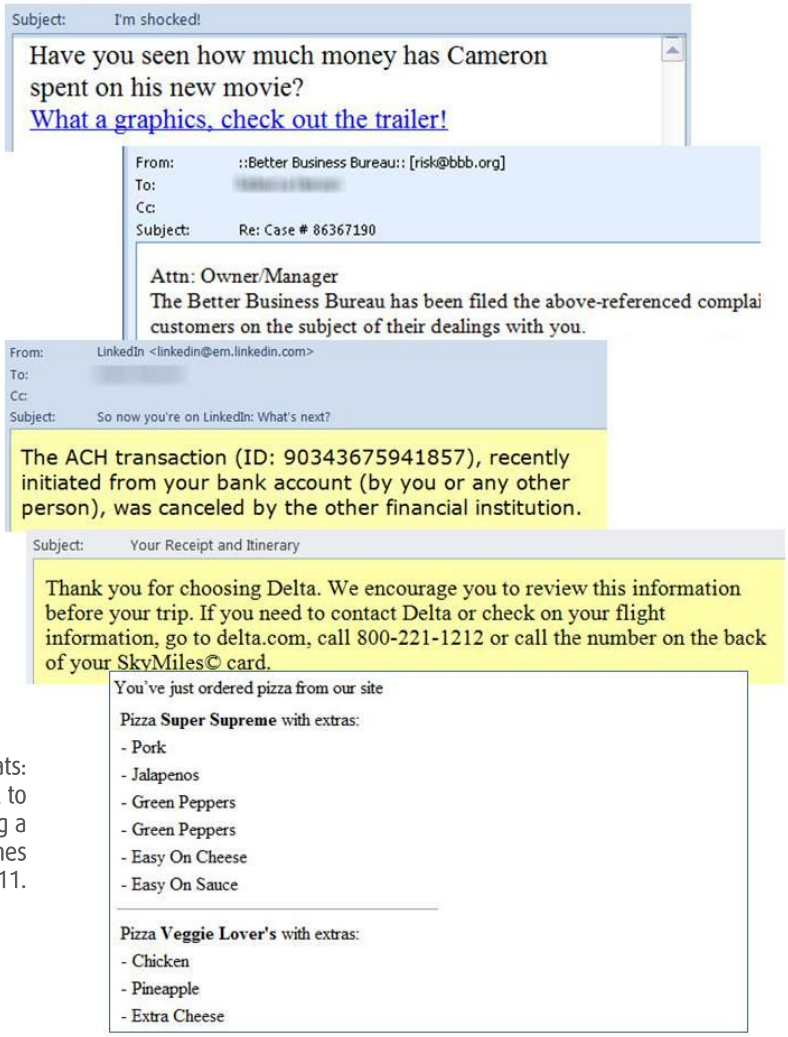
The enormous email with attached malware outbreaks of August and September, that produced peaks of several billion messages per day, subsided in October, even dropping to a mere trickle of several million messages on some days. The year-long graph below also clearly shows the large outbreaks that occurred in March. The large amounts of email-malware in 2011 were a surprise to many analysts who had predicted the continued demise of this threat vector following a quiet 2010.



Source: Commtouch

As the malware-attachment outbreaks died down, Commtouch Labs tracked multiple email outbreaks with links to malware hosted on compromised websites, also known as "blended threats" since they blend email messages with malicious websites. The numerous outbreaks in Q4 used well-crafted emails with social engineering tricks to entice recipients to follow the links. The themes used included:

- Pizza delivery notifications – including very detailed orders of toppings and drinks that were altered per email. The emails included a link to "correct" the $100+ orders.
- James Cameron movie trailer – an invitation to see the graphics of James Cameron's forthcoming epic.
- Airline itineraries – including links to online check-in and flight information.
- Rejected bank transactions – claiming to originate from the Electronic Payments Association, ACH (Automated Clearing House), or NACHA (National Automated Clearing House Association).
- Traffic tickets – include links to "plead" if there is an error in the ticket issued by the NYC – Department of Motor Vehicles.
- Better Business Bureau complaints – with links to respond to the complaints



Blended threats: Emails link to malware using a range of themes in Q4 2011.

Source: Commtouch

Top 10 Malware

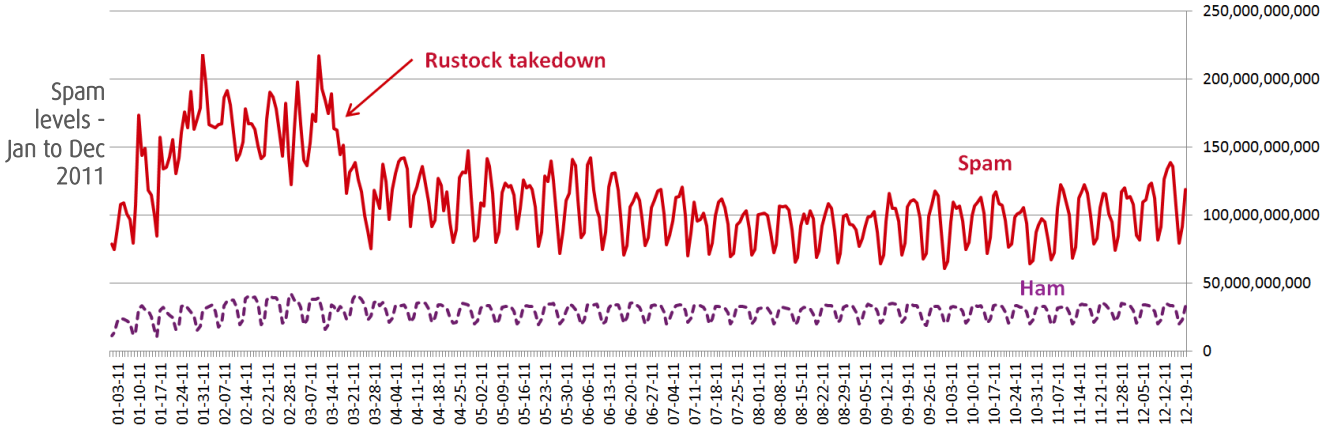
The table below presents the top 10 most detected malware during the fourth quarter of 2011 as compiled by Commtouch's Command Antivirus Lab.

Top 10 Detected Malware			
Rank	Malware name	Rank	Malware name
1	W32/Swizzor-based!Maximus	6	W32/MyWeb.D
2	W32/Brontok.A.gen!Eldorado	7	W32/Tibs.K.gen!Eldorado
3	JS/IFrame.HC.gen	8	W32/Mabezat.A-2
4	W32/Virut.9264	9	W32/Virtumonde.T.gen!Eldorado
5	W32/Heuristic-210!Eldorado	10	W32/Mywebsearch.B.gen!Eldorado

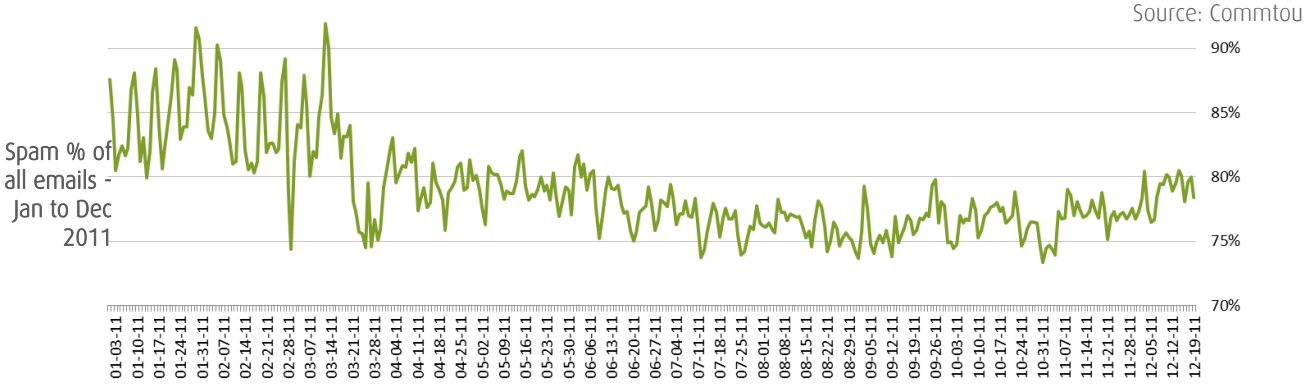
Source: Commtouch

Spam trends

Spam levels increased marginally in November and December but remained at their lowest in years following the Rustock botnet takedown in March. Spam levels averaged near 101 billion messages per day. Spam averaged 77% of all emails sent during the fourth quarter. As with email-malware levels, the sustained drop in spam was not expected by most analysts following years of continued increases in spam levels. The decrease has been attributed to many factors including: botnet takedowns, increased prosecution of spammers and the source industries such as fake pharmaceuticals and replicas, and increased revenues for cybercriminals from other avenues such as banking fraud.



Source: Commtouch



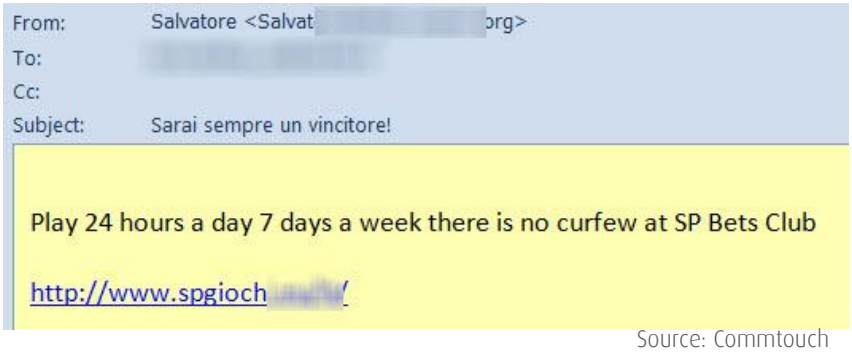
Source: Commtouch

Spammers Use Unregistered Domains to Bypass URL Checks

Spammers continue to work on methods to outwit spam filters and also URL filtering systems that block access to spam sites. These URL reputation systems usually run a few checks before adding the URL to the "spam" category. One of these checks is that the URL is registered. Once this is known the date of registration can be checked – bad sites usually have registrations that are only several hours old and this is then an important indicator of the reputation of a site.

But what if the site is not registered (as in the spam example shown below)? Many URL reputation systems will not blacklist such a site and will not be able to pursue any further reputation checks (such as the date of registration). This loophole allows spammers to send out emails linking to unregistered URLs – and then register them an hour or so after the outbreak in order to prevent the URLs from being blocked.

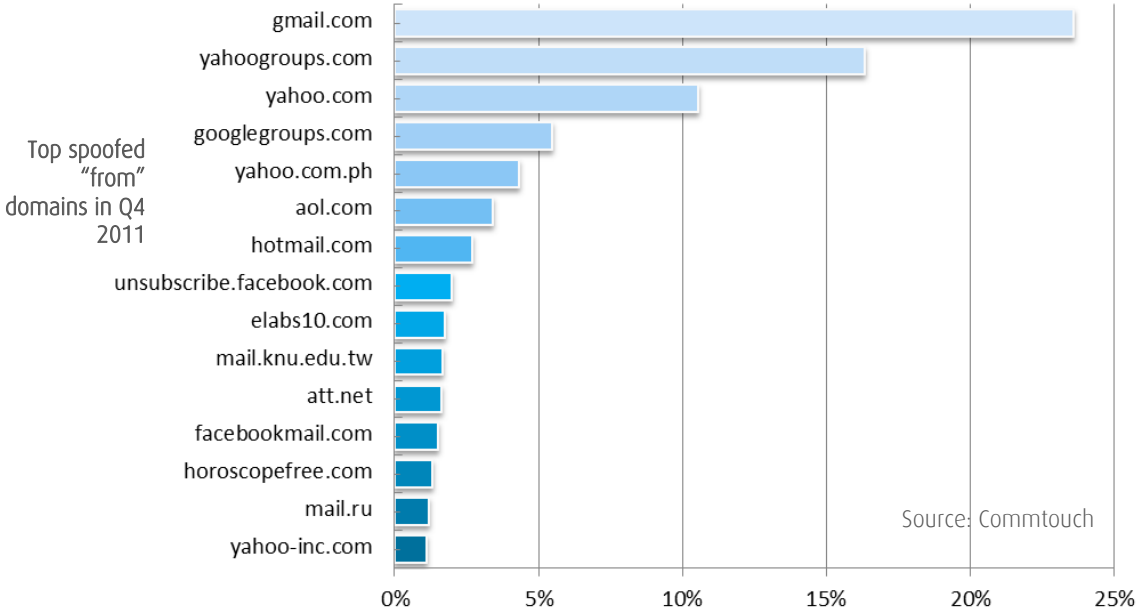
Although this trick has been used in the past, November saw extensive usage made, with outbreaks of several hundred million emails and many thousands of unregistered URLs. Of course a recipient who actually clicked on the links in the first hour or so would not have reached the destination – but the spammers seemed to think that this was worth the reduced blockage.



Source: Commtouch

Spam domains

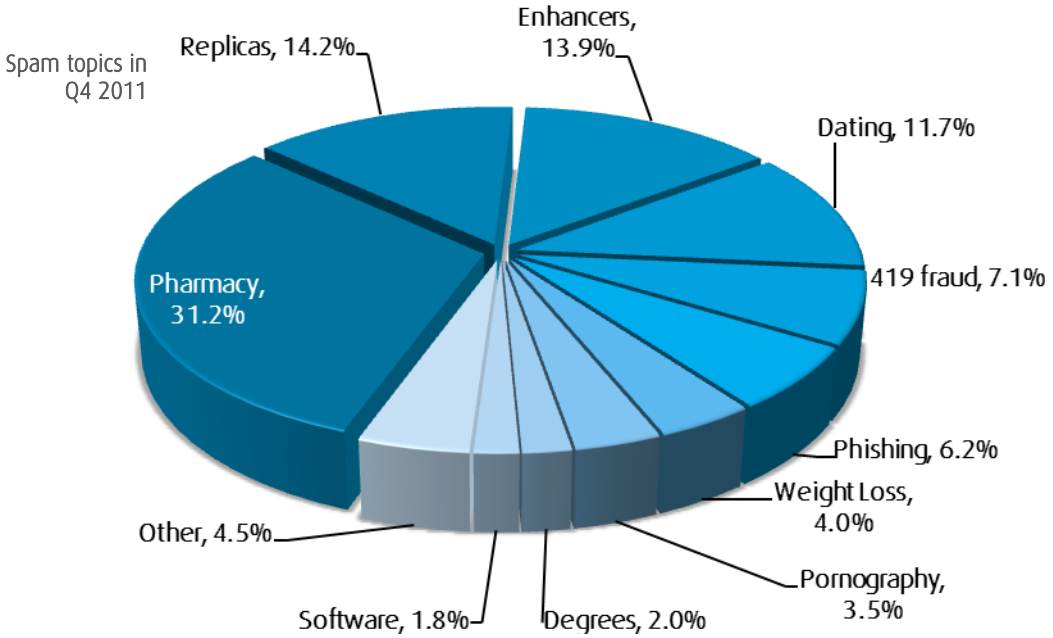
As part of Commtouch's analysis of spam trends, Commtouch Labs monitors the domains that are used by spammers in the "from" field of the spam emails. The addresses are typically faked in order to give the impression of a reputable, genuine source.



This quarter, gmail.com is once again the most spoofed domain. Note the Facebook related addresses (unsubscribe.facebook.com) and facebookmail.com that both feature in the top 15. These are often part of phishing or malware attacks.

Spam topics

Pharmacy spam continued to increase, as it did last quarter, to reach 31% of all spam (around 2% more than the previous quarter). Dating related spam increased from 2.3% to nearly 12% in the last quarter of the year.



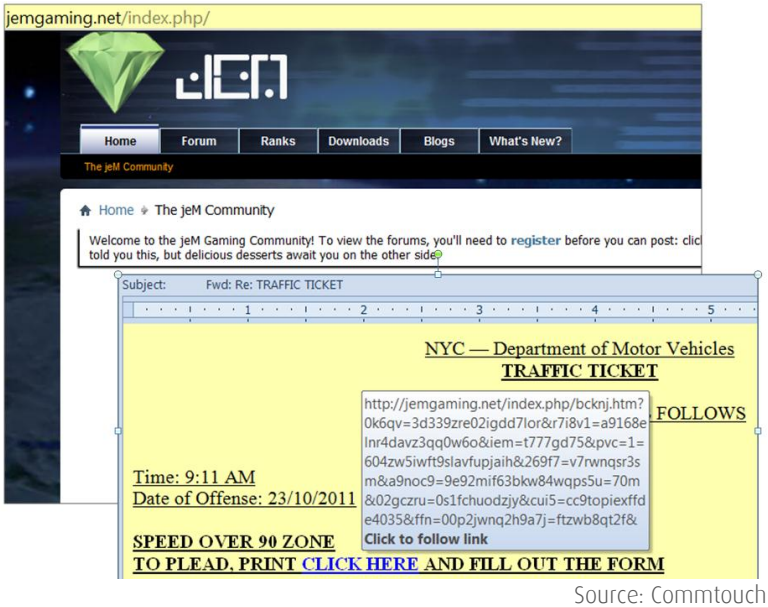
Source: Commtouch

Web security

Compromised websites store malware

Most of the emails carrying malware links in Q4 linked to compromised websites. An example of one of the attacks is shown below. The "speeding fine" link directs to JavaScript malware on a legitimate site called "jemgaming.net".

Homepage of compromised website and email with link to malware hidden on the site



Source: Commtouch

Compromised sites were also used as redirect points to pharmacy and enhancer websites. The majority of the sites use the WordPress content management system – spammers exploited a vulnerability in WordPress or in a plugin in order to hide the redirect pages. Before being redirected users are shown an initial page hidden within one of the WordPress subdirectories (see image below):

Source: Commtouch

Categories of compromised sites with malware

During the fourth quarter of 2011, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware. Parked domains and Portals remained in the top 2 positions with pornographic sites in 3rd position. 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	Entertainment
2	Portals		7	Shopping
3	Pornography/Sexually Explicit		8	Health & Medicine
4	Education		9	Travel
5	Business		10	Computers & Technology

Source: Commtouch

Categories of compromised sites with phishing

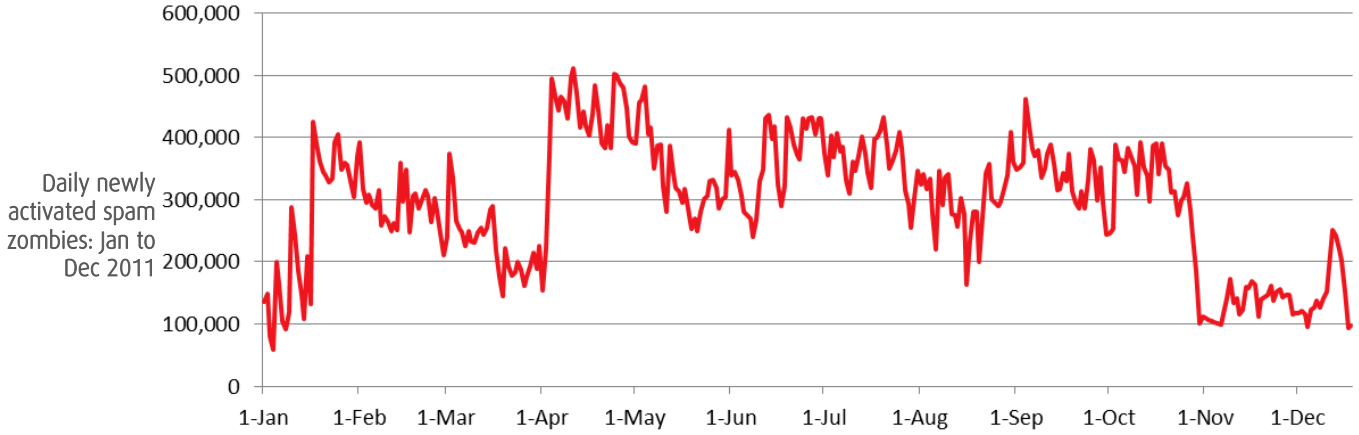
During the fourth quarter of 2011, Commtouch analyzed which categories of legitimate Web sites were most likely to be hiding phishing pages (usually without the knowledge of the site owner). Sites related to games ranked highest, similar to last quarter.

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

Source: Commtouch

Zombie trends

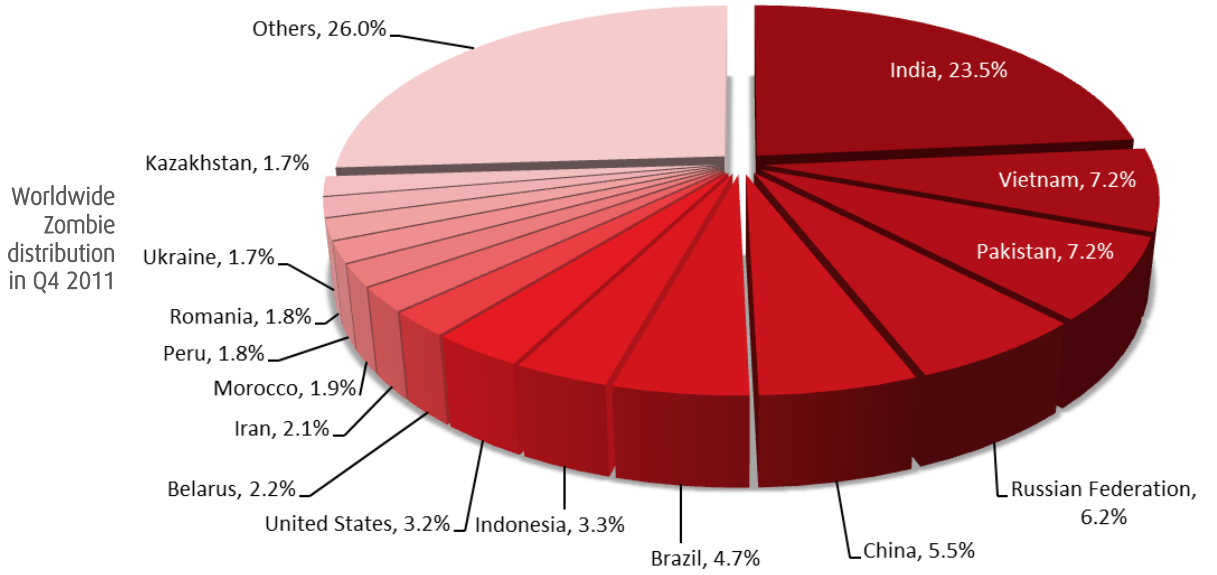
The fourth quarter saw an average turnover of 209,000 zombies each day that were newly activated for sending spam. This number shows a very large decrease compared to the 336,000 of the third quarter of 2011. The large drop at the start of November appears to be a result of the Esthost botnet takedown. Although this botnet was primarily used for DNS changing (redirecting Web requests to malicious sites), it appears that some portion was also used to send spam. The average daily turnover for 2011 was 298,000 zombies.



Source: Commtouch

Zombie Hot Spots

India again claimed the top zombie producer title, increasing its share to nearly a quarter of the world's zombies. Brazil, once a fixture in first position, continued to drop – this quarter to 6th position (a further drop of around 3%). Peru and Kazakhstan joined the top 15, displacing Saudi Arabia and Columbia.



Source: Commtouch

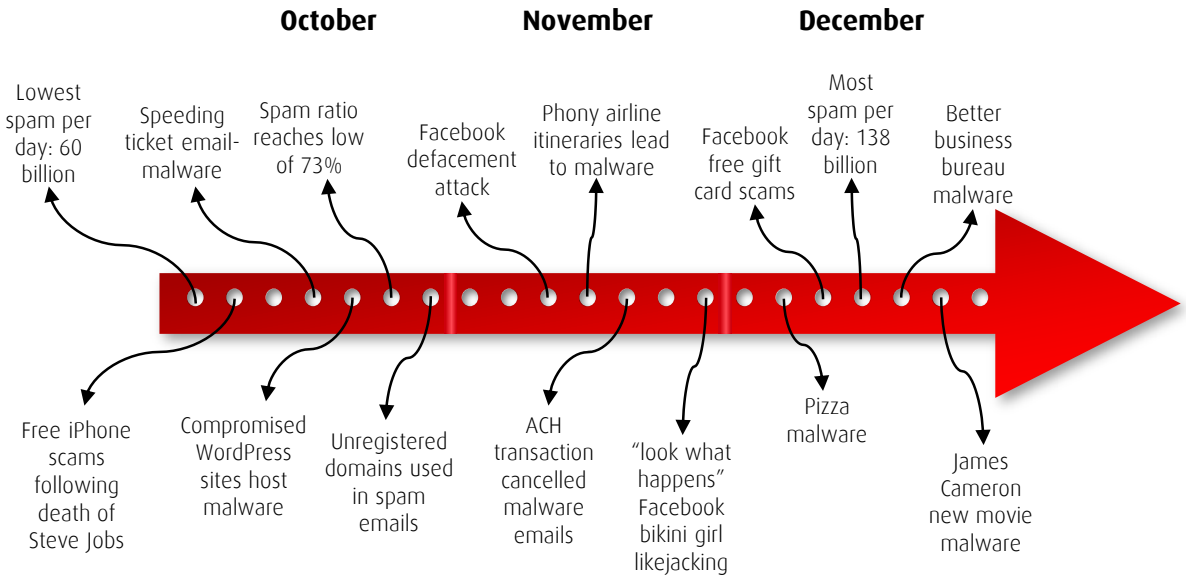
Web 2.0 trends

Commtouch's GlobalView Cloud Security 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. Once again, "streaming media and downloads" was the most popular blog or page topic, but dropped 2% this quarter. The streaming media & downloads category includes sites with MP3 files or music related sites such as fan pages.

Most popular categories of user-generated content						
Rank	Category	Percentage		Rank	Category	Percentage
1	Streaming Media & Downloads	22%		8	Arts	5%
2	Computers & Technology	8%		9	Sports	4%
3	Entertainment	7%		10	Education	4%
4	Pornography/Sexually Explicit	6%		11	Leisure & Recreation	3%
5	Fashion & Beauty	5%		12	Health & Medicine	3%
6	Restaurants & Dining	5%		13	Games	3%
7	Religion	5%		14	Sex Education	2%

Source: Commtouch

Q4 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, email security and antivirus solutions, protecting thousands of organizations and hundreds of millions of users worldwide.

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.
- http://blog.commtouch.com/cafe/web-security/facebook-scams-free-giftcards-for-cheesecake-factory-tim-hortons-and-costco/
- http://blog.commtouch.com/cafe/web-security/look-what-happens-when-you-try-and-watch-videos-of-girls-in-bikinis-on-facebook/
- http://blog.commtouch.com/cafe/web-security/nasty-facebook-picture-attack-based-on-self-xss/
- http://blog.commtouch.com/cafe/data-and-research/a-study-of-malicious-attacks-on-facebook/
- http://blog.commtouch.com/cafe/data-and-research/a-study-of-malicious-attacks-on-facebook/
- http://blog.commtouch.com/cafe/web-security/facebook-the-first-1000-participants-get-facebook-phone/
- http://blog.commtouch.com/cafe/web-security/another-fake-%e2%80%9cfacebook-profile-views%e2%80%9d-application-how-many-girls-and-boys-have-viewed-your-wall/
- http://blog.commtouch.com/cafe/phishing/avoiding-facebook-phishing/
- http://blog.commtouch.com/cafe/malware/%e2%80%9cosama-bin-laden-dead-%e2%80%93-actual-video%e2%80%9d-new-facebook-malware/
- http://blog.commtouch.com/cafe/malware/500-free-credits-from-facebook-%e2%80%93-malware/
- http://blog.commtouch.com/cafe/malware/malware-spread-via-facebook-chat/
- http://blog.commtouch.com/cafe/malware/have-you-seen-how-much-money-james-cameron-spent-on-his-new-movie/
- http://blog.commtouch.com/cafe/email-security-news/would-you-like-some-malware-on-your-pizza/
- http://blog.commtouch.com/cafe/malware/so-now-youre-on-linkedin-whats-next/
- http://blog.commtouch.com/cafe/web-security/compromised-websites-unknowingly-host-malware/
- http://blog.commtouch.com/cafe/malware/phony-delta-american-airlines-itineraries-lead-to-malware-2/
- http://blog.commtouch.com/cafe/anti-spam/increased-usage-of-unregistered-spam-domains/
- http://blog.commtouch.com/cafe/email-security-news/spam-outbreak-makes-large-scale-use-of-compromised-yahoo-hotmail-and-aol-accounts-as-well-as-wordpress-sites/
- http://blog.commtouch.com/cafe/email-security-news/twice-as-bad-traffic-ticket-with-attached-malware/

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.