Internet Threats Trend Report
Q4 2010

IceWarp®

commtouch®

IceWarp®

commtouch®
Real Security. In Real Time.

In This Report

Q4 2010 Highlights

▼ **142 billion**

Average daily spam/phishing emails sent

Page 2

▼ **288,000 Zombies**

Daily turnover

Page 3

▼ **Streaming media/ Downloads**

Most popular blog topic on user-generated content sites

Page 12

▼ **Pharmacy ads**

Most popular spam topic (42% of spam)

Page 4

▲ **India**

Country with the most zombies (17%)

Page 3

▼ **Pornography/ Sexually Explicit**

Website category most likely to be contain malware

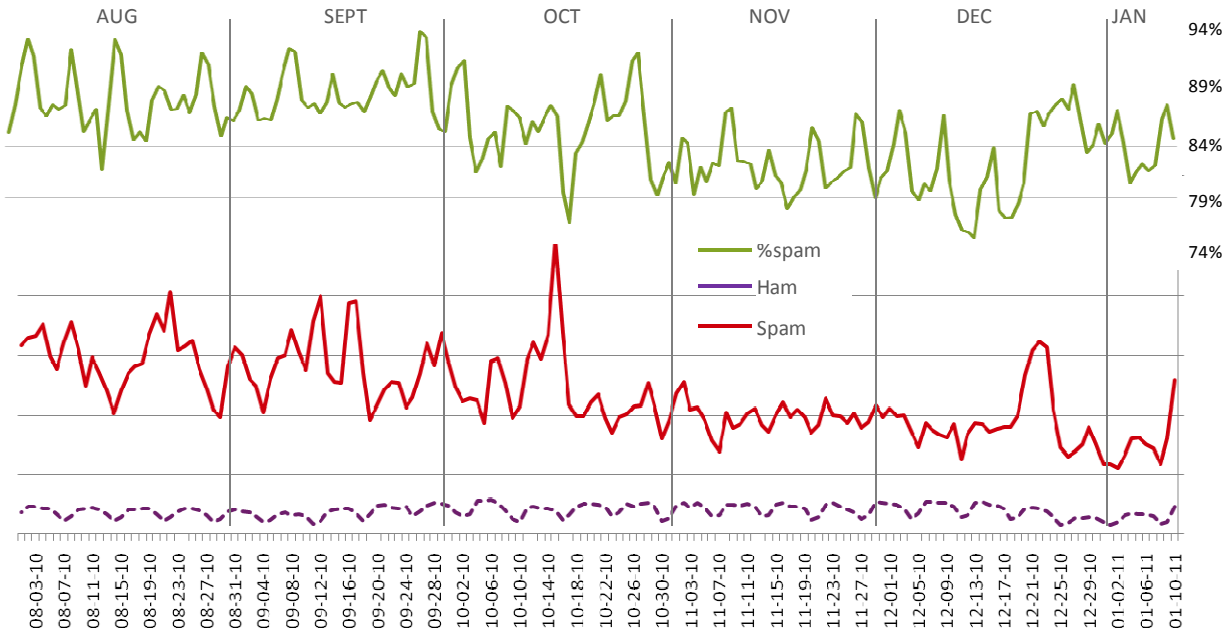
Page 13

Spam declines in Q4 2010

A drop in spam levels was observed at the end of the third quarter and was reported in last quarter's Trend report; however, at the time it was unclear if the reduction was a short-term drop or would be more prolonged. The drop in spam is most likely attributed to the closure of Spamit around the end of September. Spamit is the organization allegedly behind a fair percentage of the world's pharmacy spam. According to reports in October, the reasons for the sudden "voluntary" closure were related to charges brought against the individuals behind Spamit.

Analysis of the spam data for the fourth quarter reveals that the reduction in spam was sustained throughout Q4 2010 except for a brief pre-Christmas surge. December's daily average was around 30% less than that September. The average amount of spam as a percentage of the total amount of email for the quarter was 83%, down from 88% in Q3 2010. The beginning of December saw a low of nearly 74%. The average daily total of spam messages for the quarter was around 142 billion (down from 198 billion in Q3 2010).

At the start of January 2011 as the holiday season ended around the world, Commtouch Labs noted a sudden resurgence in spam levels. The daily total jumped 45% compared to the average of the previous 2 weeks.

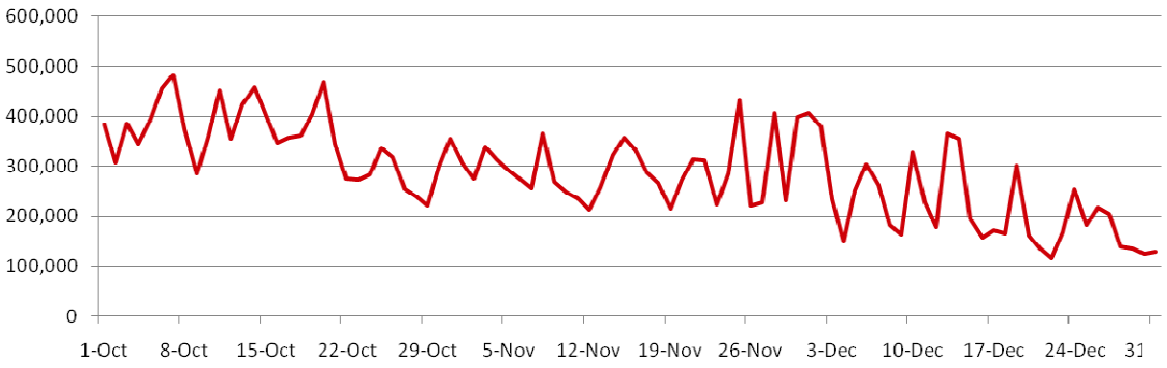


Source: Commtouch

The nature of the spam attacks also changed. The pre-October graph shows large fluctuations in the amounts of spam sent. In Q4 2010 there were generally lower fluctuations – aside from two large outbreaks in mid-October (the quarter's highest percentage at 93%) and mid-December. Previous years have also featured large amounts of pre-Christmas spam, but here too the pre-Christmas outbreak was smaller than most of the large outbreaks this year.

Reduced zombie activity

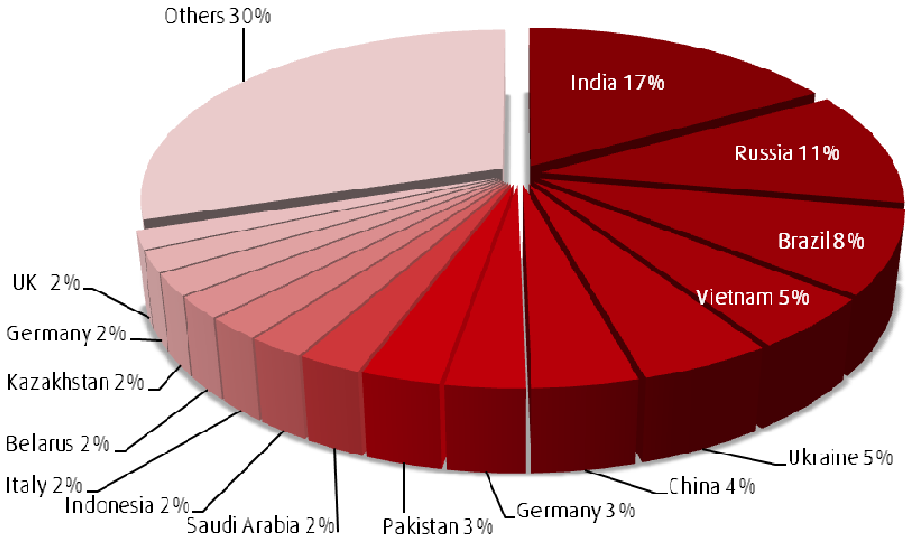
The fourth quarter saw an average turnover of 288,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. This number shows a significant decrease compared to the 339,000 of the third quarter of 2010. The graph below shows the newly active zombies each day throughout the quarter. The downward trend clearly matches that of the spam trends shown above, suggesting that reduced zombie activity is having an effect on botnet spam.



Source: Commtouch

Zombie Hot Spots

India again claimed the top zombie producer title with an increase of 3%. Brazil continued its drop from last quarter from 2nd to 3rd place while Russia moved up into 2nd place (3rd place last quarter, and 5th place in the second quarter). The US and Columbia dropped out of the top 15 while Belarus and Kazakhstan moved up into 12th and 13th places respectively.

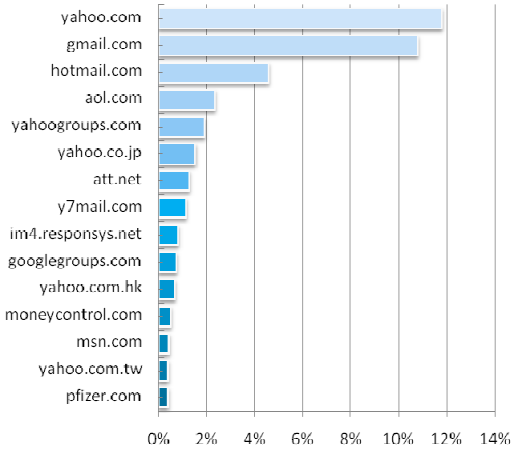


Source: Commtouch

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.

This quarter, gmail.com gets displaced by yahoo.com which takes the top spot. In fact, six Yahoo domains find their way into the top 15. pfizer.com appears in 15th position. This from field is used in "open" pharmacy spam i.e.: the emails do not hide the medical products that they are trying to sell, and in fact try to leverage the pharmaceutical giant's brand by spoofing their domain as the sender.

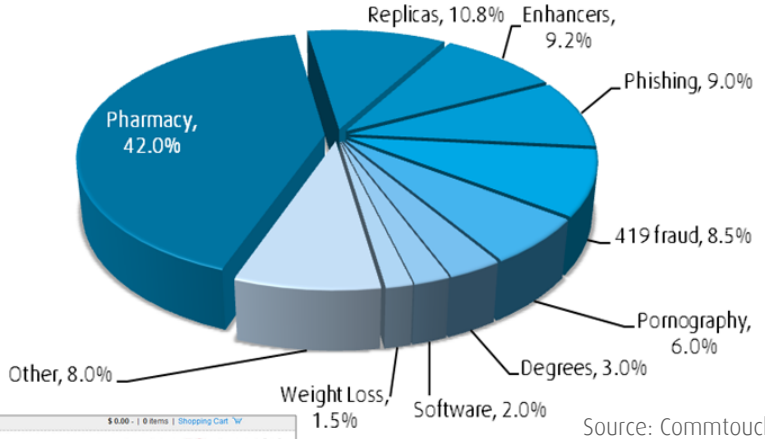


Source: Commtouch

Spam Topics

Pharmacy spam remained in the top spot but continued to drop this quarter to 42%. Most of the other categories gained in percentage as a result, particularly, replicas, enhancers phishing, and 419 fraud.

In an interesting twist, this quarter saw the emergence of online pharmacies supposedly based in the US – a change from the well known Canadian branded stores. The global spread was not limited to the US though – Swiss Pharmacy spam was also distributed.



Source: Commtouch

US and Swiss pharmacy sites

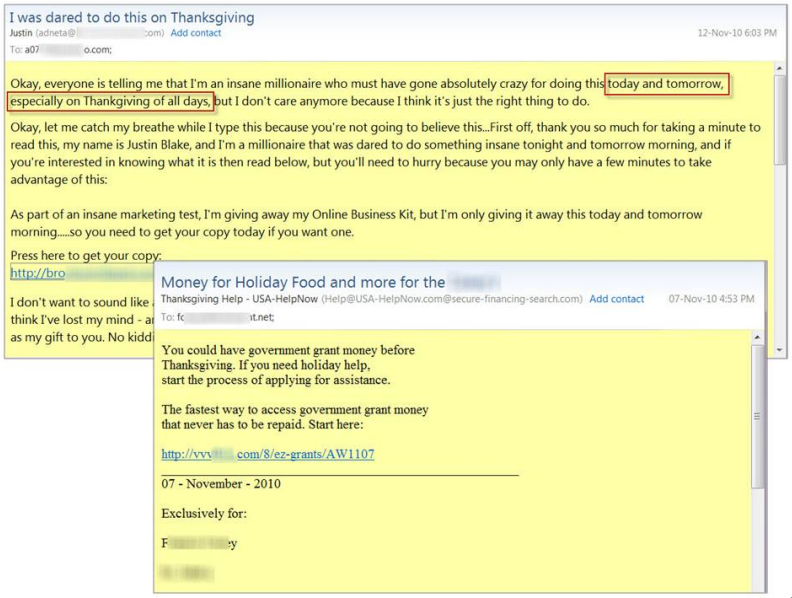
Source: Commtouch

Holiday spam and malware

Spammers predictably used the holidays of the fourth quarter to attract the attention of email recipients. Thanksgiving, Christmas related spam and blended threats featured prominently. The pre-Christmas flood of spam is clearly visible in the spam trends graph above.

The first Thanksgiving example presented below represents a common scam requiring purchase of an "online secret money making" kit. The highlighted text (with the red square) shows a clearly incorrect dating of Thanksgiving. The second example below offers recipients free government funds in time for Thanksgiving. This example also illustrates some "personalization" of the email by using the recipient's name (taken from the email address) in the subject line and also in the closing comments.

Thanksgiving spam samples



Source: Commtouch

Phony Hallmark greeting cards (with bonus malware)

More holiday cheer was spread by malware distributors in the form of emails inviting recipients to view online greeting cards. The "from" fields of the emails contained the incorrectly spelled "Halmark". Clicking on the embedded links led users to a confusing site that contained malware exploiting a range of vulnerabilities in RealPlayer, JAVA, Flash Player and Adobe Reader.

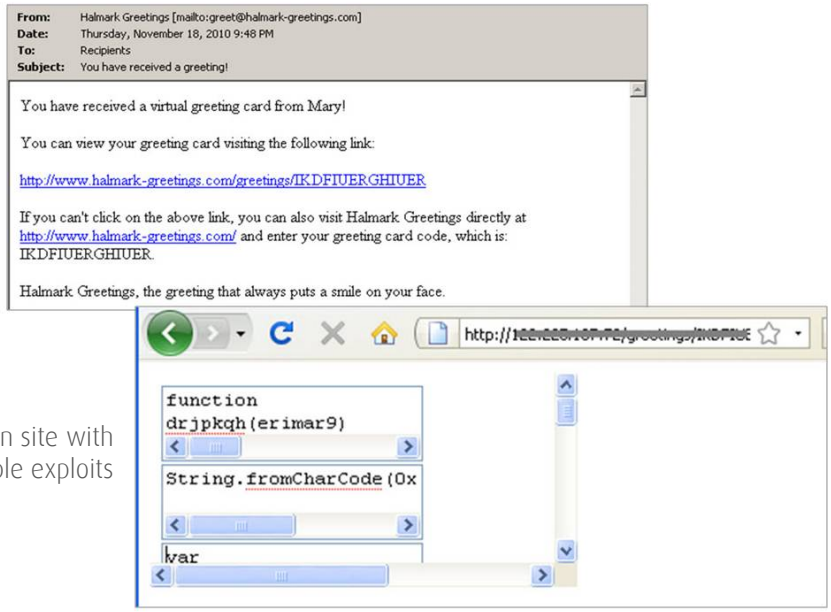
Following a successful exploit the software would download and execute further malware from the following links (Command Antivirus detection is listed on the Right):

- hxxp://122.<blocked>.72/b/ctyvytasbljuxle.jar - Java/ByteVerify.F
- hxxp://122.<blocked>.72/b/bwcucwatjtfo4.swf - SWF/Expl.H
- hxxp://122.<blocked>.72/b/kub.php?i=2 - W32/Poison.U
- hxxp://122.<blocked>.72/b/kub.php?i=7&&&& - W32/Poison.U
- hxxp://122.<blocked>.72/b/dqjmymytbvyzj9.pdf - PDF/Expl.IK

- hxxp://122.<blocked>.72/b/jvkzfnxlgnfz.pdf - PDF/Expl.IL

"Halmark" greeting card

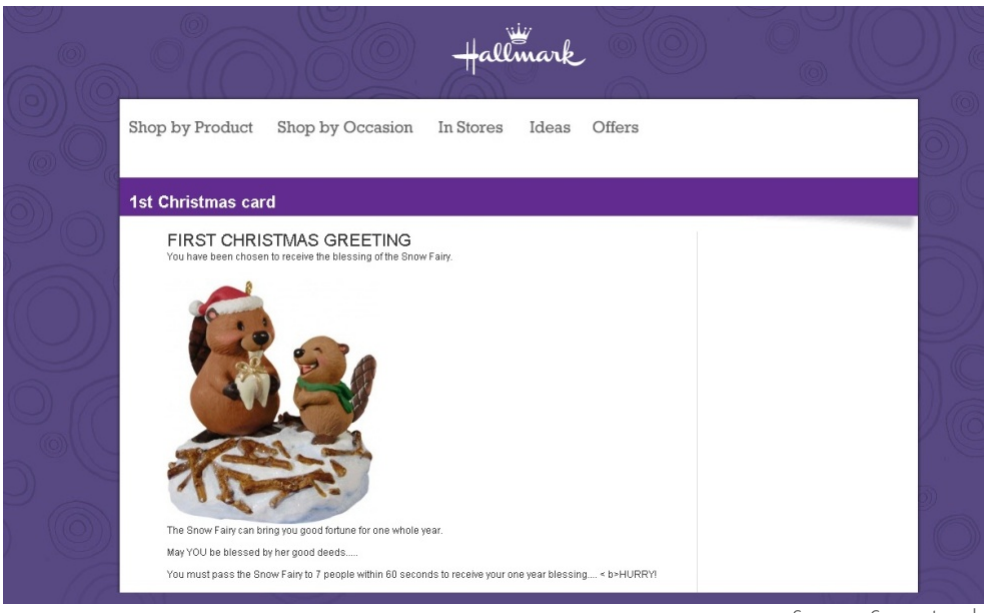
Destination site with multiple exploits



Source: Commtouch

Another selection of fake Hallmark cards circulated at the start of December. The email "card" grabs scripts and graphics from the actual Hallmark webpage to make it appear legitimate. All of the clickable links in the email point to the Hallmark site. The text from the email reads: "The Snow Fairy can bring you good fortune for one whole year. May YOU be blessed by her good deeds.... You must pass the Snow Fairy to 7 people within 60 seconds to receive your one year blessing.... <b>HURRY!"

Phony Hallmark greeting card email with attached malware



Source: Commtouch

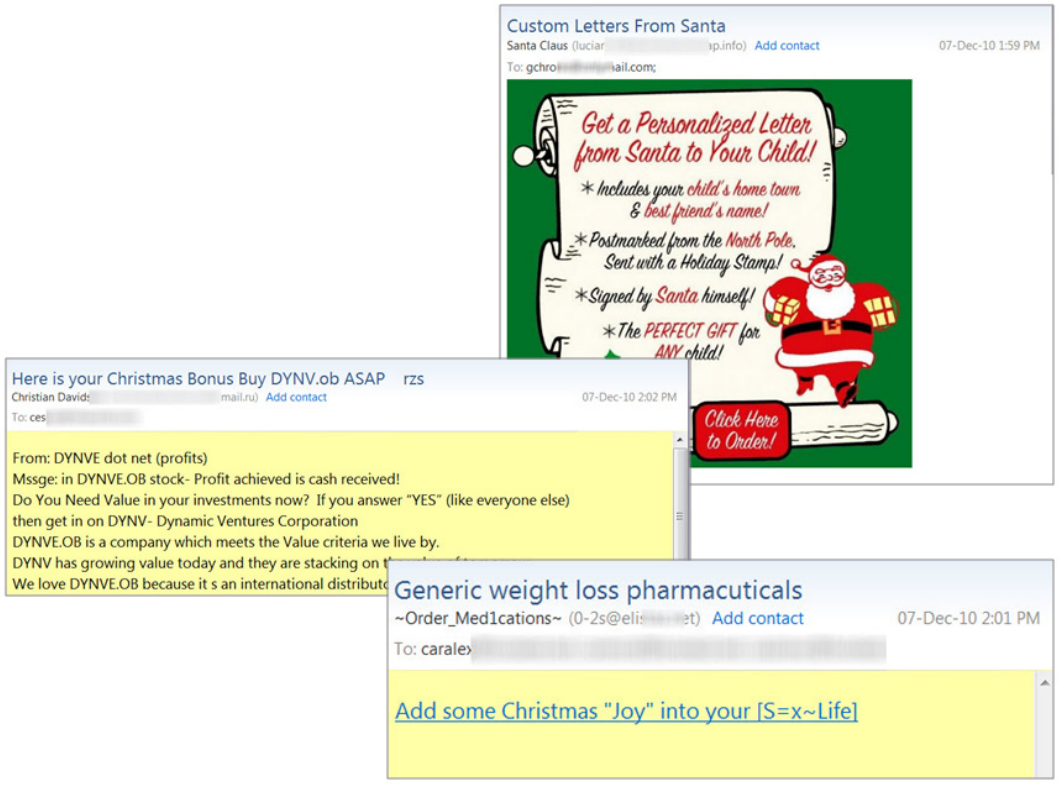
An interesting mix of social engineering, chain letters and malware (the card includes a malware attachment).

Christmas spam

Spam subjects covering every aspect of Christmas and also touching on New Year were used in a range of December outbreaks:

- ca$h to your door before christmas! tax-free!
- christmas information
- date !for the christmas party
- earn extra money this christmas....view attachment
- earn extra xmas cash
- get your $10k or more before christmas !
- i found all christmas presents now
- microsoft xmas promotion winner!!!
- xmas lottery promo 2010 edition....
- fast christmas cash!
- xmas mystery shopper wanted
- meet you at the new years party

In addition, Christmas subject lines were used in a range of messages that included stock scams, weight-loss products and fake greeting cards from Santa.

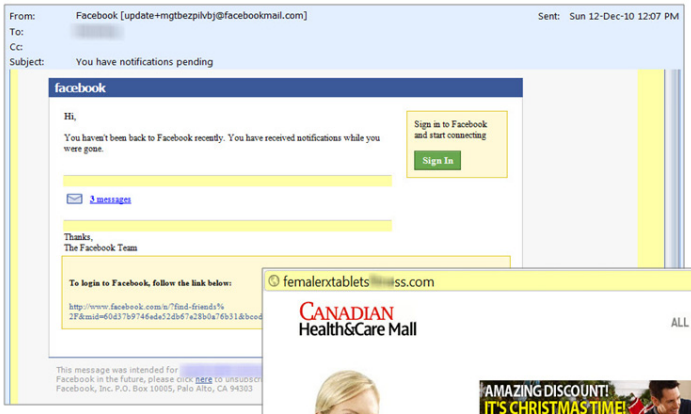


Samples of Christmas related spam

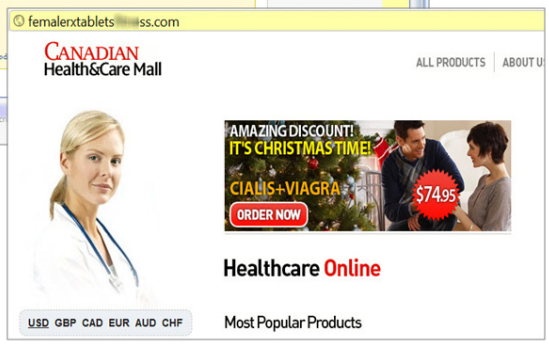
Source: Commtouch

Even fake Facebook notification emails, usually associated with phishing attacks, were repurposed in December to lead to pharmacy sites offering Christmas specials.

Phony Facebook notification emails



Destination pharmacy site with Christmas offers



Source: Commtouch

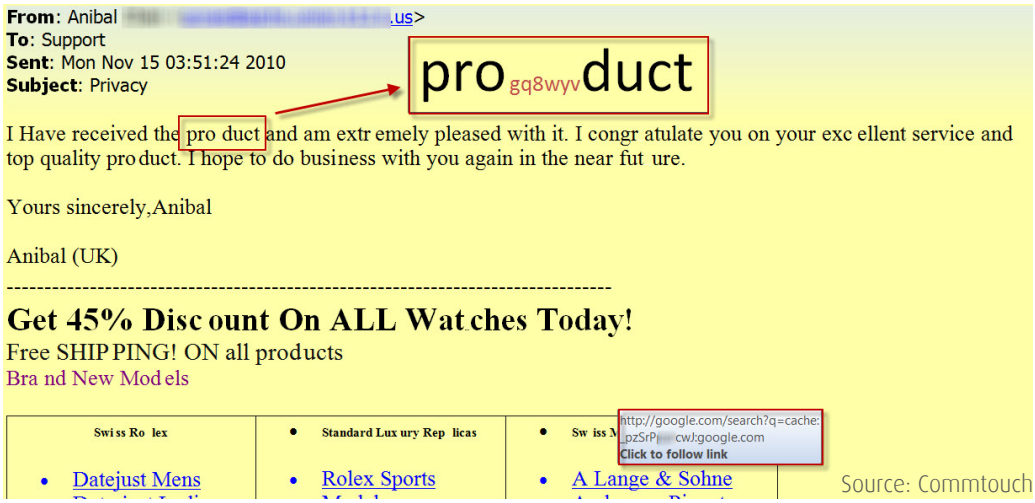
Vintage spam methods resurface

This quarter saw significant amounts of spam that used techniques first seen three or more years ago. In all cases these were combined with more current techniques.

Small fonts and misuse of Google cache

The classic method of using hidden fonts in spam messages was identified in a November outbreak. In the example below, with the subject of "privacy," invisible, random text is used to break up words which might be detected by spam filters. As shown below, the word "product" appears to have a space in the middle of the word (as do the words "extremely," "congratulate," "excellent" and "future"). The space is actually made up of 6 numbers and letters – all with a font size of 1 pt. and colored white. In the image below the text has been enlarged and colored red to make it visible.

Spam with hidden text and Google cache misuse



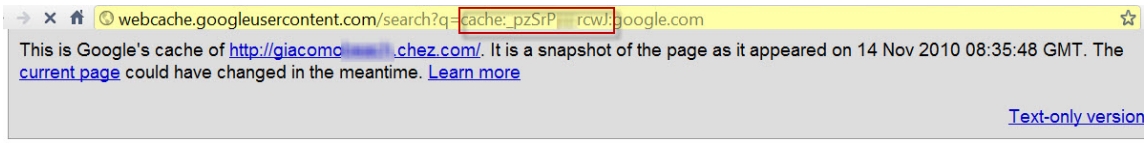
Source: Commtouch

The hyperlinks within the spam message also use an early technique, in that they appear to lead to Google.com. These URLs will not trigger most content-based spam filters since most will whitelist the Google domain.

The newer trick is the use of Google's cache, which is a free service that stores snapshots of old webpages, allowing searchers to access content that may have changed since it was scanned by Google. In this example the link includes Google's cache code: pzSrP–rcwJ. The inclusion of the text ":google.com" at the end of the link is purely "cosmetic" (probably designed to fool readers or content-based scanning engines) and does not affect the destination.

The links lead to the cached version of a seemingly blank page from a site called "giacomo–.chez.com."

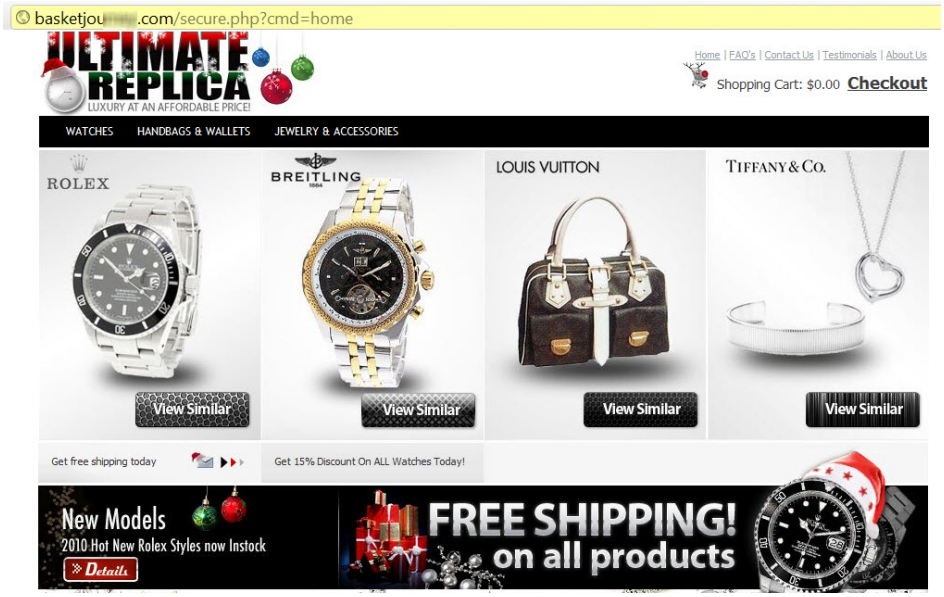
Google cached version of site



Source: Commtouch

However, this cached site includes an embedded script that redirects visitors to their final destination – the Ultimate Replica site (complete with Christmas decorations).

Destination replicas site with Christmas theme



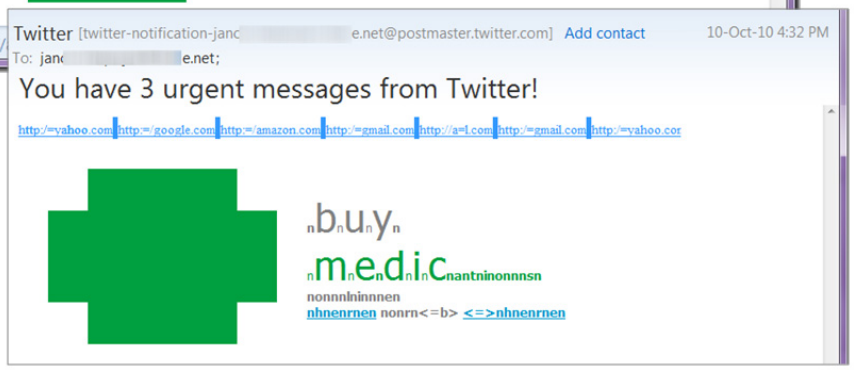
Source: Commtouch

Hidden text and Twitter subjects

A further example is shown below. This time the subject is an attention-grabbing "You have 3 urgent messages from Twitter". Selecting all the text in the message shows the hidden line at the top of the email which includes working hyperlinks to the most popular domains – clearly a tactic to fool content-based scanning filters.

Twitter subject spam

Twitter subject spam with hidden text visible



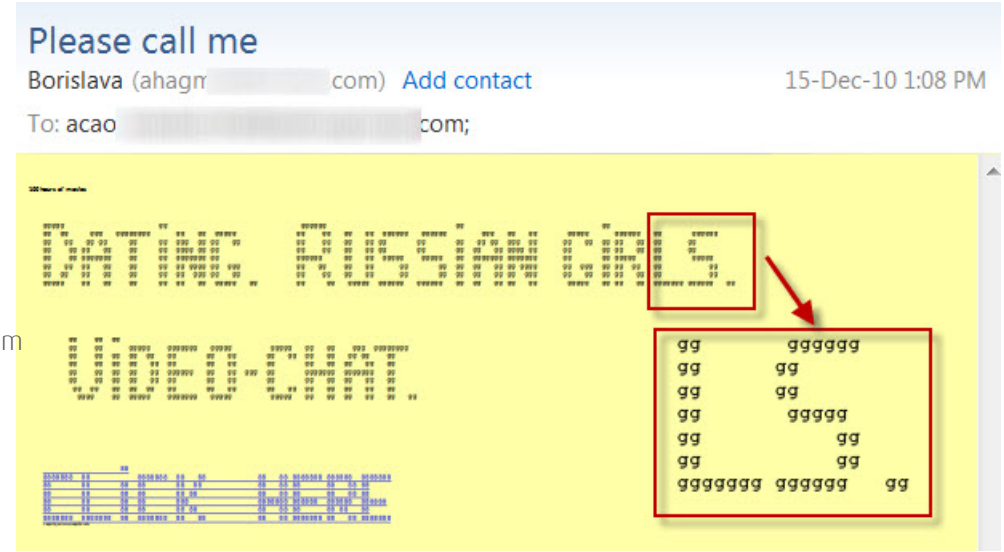
Source: Commtouch

Updated ASCII Art spam

ASCII art spam emails reappeared in December. ASCII art uses cleverly arranged standard keyboard characters as well as extended character sets to create pictures or messages in a kind-of low-resolution graphic.

Spammers have used this technique in the past to evade content-based anti-spam filters – the jumble of characters that is used is simply not detected as spam. This newer version includes a clickable link (previous generations simply spelled out the name of the advertised website).

ASCII art spam



Source: Commtouch

Unicode characters used for malware distribution

A more subtle use of extended character sets was detected by Commtouch partner Openfind Information Technology, Inc. at the start of the quarter. The technique was used to trick users into opening malware executables. The emails include standard "you have received an important document which is attached" text as well as an attachment.

When the archive was opened, the filename appeared to be of the promised .doc or .xls type. However, the filename included a unicode string that effectively hid the malicious .exe or .scr file type.

These are examples of the types of filenames used:

- Costing Cap[U+202E]slx.exe
- Calenda[U+202E]cod.scr

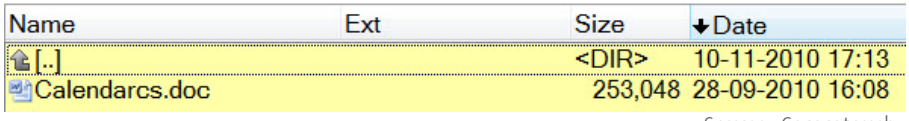
Note the Unicode control characters in brackets: [U+202E]. This code has the function of a "Right to Left Override" (RLO). Any text to the right of this code will be reversed. Thus the final few letters of the examples above appear as:

- exe.xls (appears to be an MS-Excel file)
- rcs.doc (appears to be an MS-Word file)

Since the control code is not actually displayed when the filename is shown in the operating system, the filenames would appear to be:

- Costing Capexe.xls
- Calendarcs.doc (see example below)

File view showing incorrect name



Source: Commtouch

Commtouch's Command AV lab confirms that the file shown above will actually open an embedded MS-Word document – but will also start the malware installation process in parallel.

Web 2.0 trends

Commtouch's GlobalView Network tracks billions of Web browsing sessions and URL request, 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 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.

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

Source: Commtouch

Blogspot, Facebook and Koobface

One of the popular Web 2.0 sites used by Internet villains is Google's Blogger (Blogspot). The quarter began with continued abuse of Blogspot links to distribute the Koobface malware. Koobface (a play on the word Facebook) has been active since 2008. The recent attacks follow an established pattern:

1. Compromised Facebook accounts send a Blogspot link to friends in a message with a video related theme. In the examples below the misspelled "Wow3!

Are you erally in htat videso?" and "You'e beeen filmedd! Haaven't you notficed?".

Koobface generated Facebook messages

Source: Commtouch

2. Recipients clicking on the link are redirected from Blogspot to web pages with video player interfaces that "require" the installation of a video playing component. The install is actually Koobface which compromises the local FaceBook account and continues to spread. Compromised PCs are also used to open new Blogspot accounts in order to provide fresh distribution links.

It was reported in mid-November that the command and control of the Koobface botnet had been disrupted. Reports of several days later stated that the herders had restored communication using alternate servers.

Compromised websites

During the fourth quarter of 2010, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware or phishing. As with previous quarters, pornographic and sexually explicit sites ranked highest in the categories that contain malware. This is not always an indication of a compromised site. The hosting of malware may well be part of the design of such sites.

On the list of Web categories likely to be hosting hidden phishing pages, sites related to games ranked highest. The "Computers & Technology" and "Business" categories showed increased instances of embedded phishing pages compared to the third quarter of 2010.

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

Website categories infected with phishing	
Rank	Category
1	Games
2	Shopping
3	Health & Medicine
4	Computers & Technology
5	Business
6	Streaming Media & Downloads
7	Real Estate
8	Travel
9	Education
10	Pornography/Sexually Explicit

Source: Commtouch

Compromised site – free pharmacy site hosting

In addition to hacking websites in order to hide phishing pages or malware, cybercriminals also use this technique for free hosting of spam product pages. The email below was received in November from a compromised Yahoo account.

Spam from compromised Yahoo account

Destination pharmacy site with Thanksgiving specials

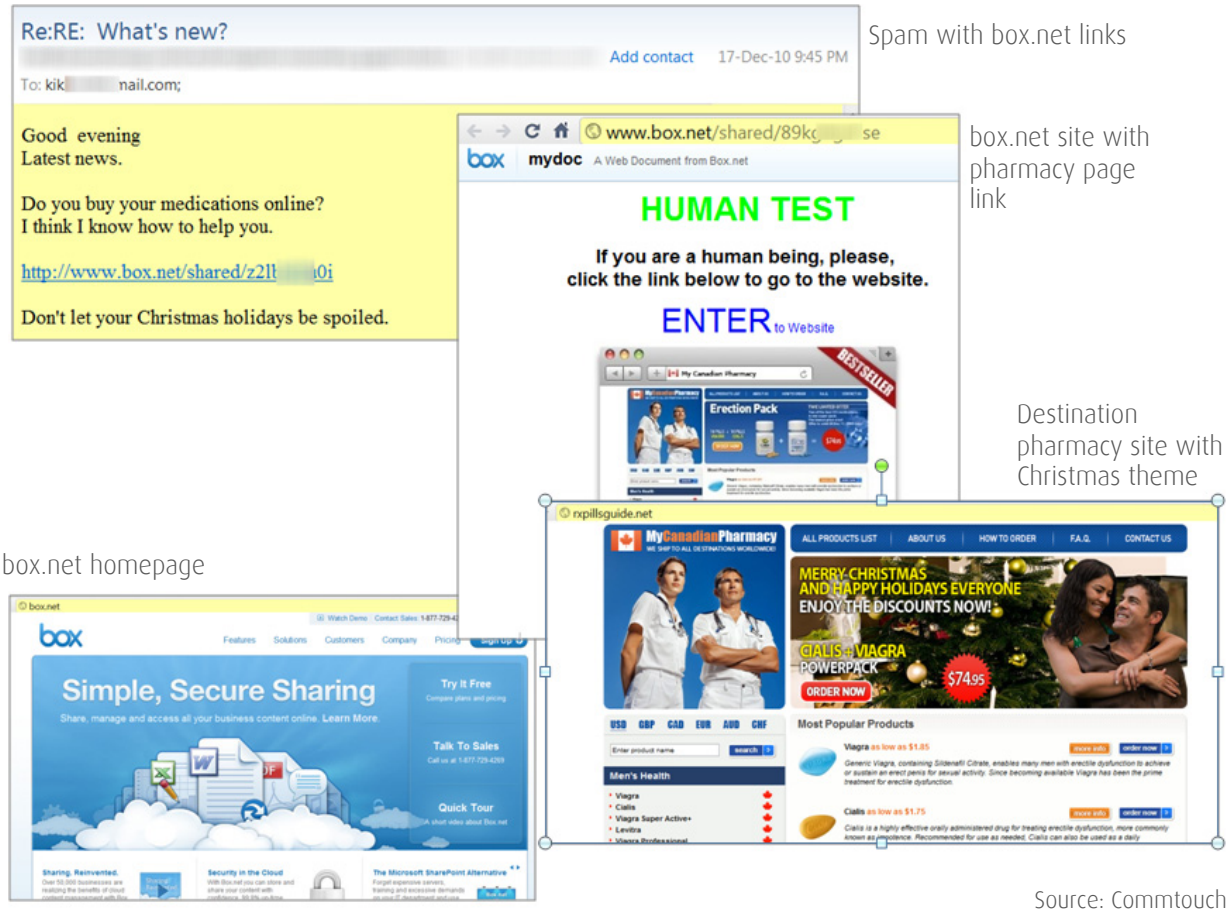
Homepage of compromised site

Source: Commtouch

The link led to a typical Canadian Pharmacy site with Thanksgiving-related specials. Further investigation of the link revealed a compromised site being used to host the pharmacy pages. The genuine homepage of the site (malthousesales.co.uk) is also shown in the image above.

Box.net used for pharmacy site redirect

Any site offering to share user content runs the risk of being abused to host spam, malware or phishing content. Box.net is one such service, offering content sharing and synchronization services for legitimate content owners. In late December, box.net was used to store "documents" that redirected to pharmacy sites. The links to the shared documents were widely spread in pharmacy-related spam. Christmas again features – in the email message and on the pharmacy webpage.



Source: Commtouch

AV Trends

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

Rank	Malware name
1	W32/Vilsel.AG
2	VBS/CDEject.A
3	W32/Agent.GV.gen!Eldorado
4	W32/Viking.DO
5	W32/Wintrim.C.gen!Eldorado
6	JS/Agent.FP.gen
7	W32/VB.AD.gen!Eldorado
8	W32/Pikorms.A.gen!Eldorado
9	W32/FakeAlert.II.gen!Eldorado
10	W32/Damaged_File.gen!Eldorado

Source: Commtouch

Boxing match search results used to spread fake AV

November provided excitement for boxing fans with the WBC Super Welterweight World Title fight between Antonio Margarito and Manny Pacquiao. Peddlers of Fake AV once again saw this as a good opportunity to infect computers via Search Engine Optimization (SEO) poisoning attacks. These infections deliver fake system alerts designed to fool users into buying fake antivirus products.

Searching for the keywords "Pacquiao-Margarito Fight" on Google gave the following results:

SEO poisoned search results

Source: Commtouch

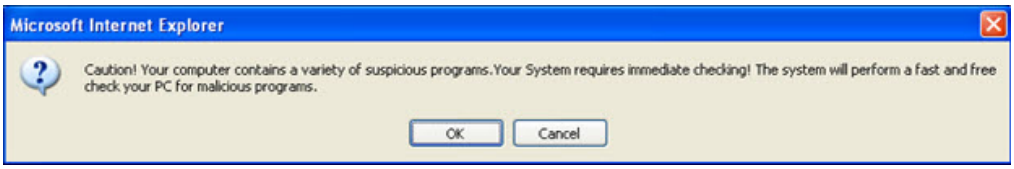
The link redirected differently depending on the Web browser type as well as operating system. Users with a web browser other than Internet Explorer or Firefox for Windows would be redirected to the site "hxxp://adobefeatures ----.CC" which showed the fake Adobe Flash Player update seen below:

Flash player "update" page

Source: Commtouch

Clicking any button resulted in the page insisting you download and install the fake Flash Player update named "v11_flash_AV.exe" detected by Commtouch's Command Antivirus as the malware W32/FakeAV.BAU. Users of Firefox were redirected to the site "hxxp://lazyfirefox-------.CC". Users of Internet Explorer were redirected to pages with fake system messages such as these:

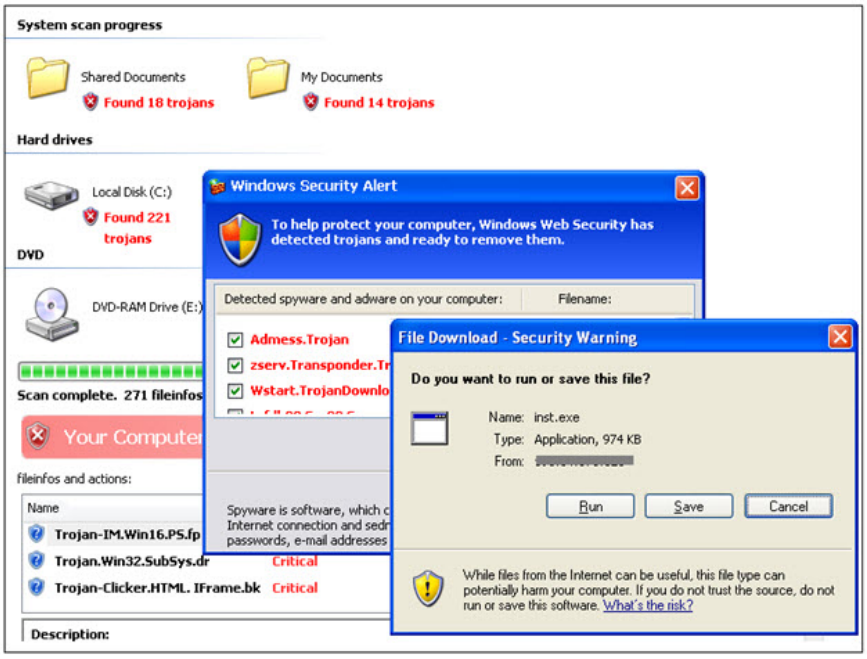
Internet Explorer fake AV message



Source: Commtouch

Clicking any button took users to fake scanning pages – a common method used by fake antivirus to force users to download and execute various malicious files. Fake scan results are shown below:

Fake scan results



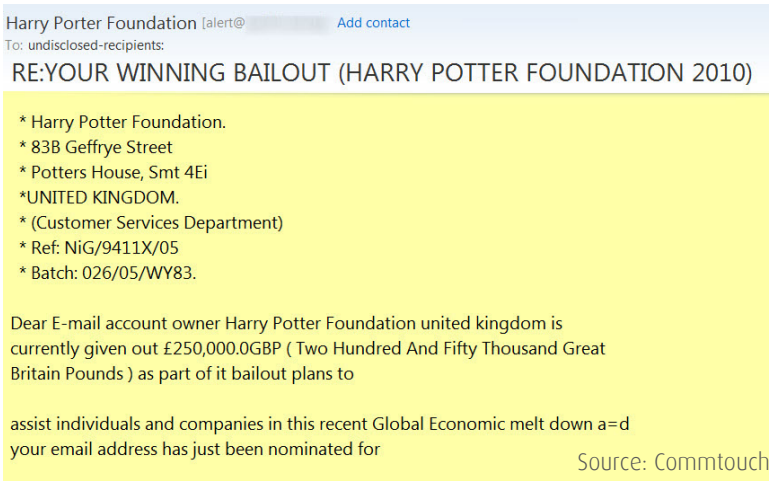
Source: Commtouch

Command antivirus detects the downloaded file "inst.exe" as W32/FakeAV.BAV. MAC or LINUX users got off lightly since they only got redirected to the site "feeds.feedburner.com/goodnewspic" which had no malicious content.

Sillyspam

The Trend Report traditionally closes with a review of the most comical spam topics which are tweeted by Commtouch (Twitter: @commtouch, #sillyspam). This quarter's report instead includes a look back at some of 2010's more amusing phishing emails and spam websites.

- In June the "Harry Potter Foundation" was giving away GBP 250,000 (and they are based in "Potter house")



Harry Porter Foundation [alert@ Add contact
To: undisclosed-recipients:

RE:YOUR WINNING BAILOUT (HARRY POTTER FOUNDATION 2010)

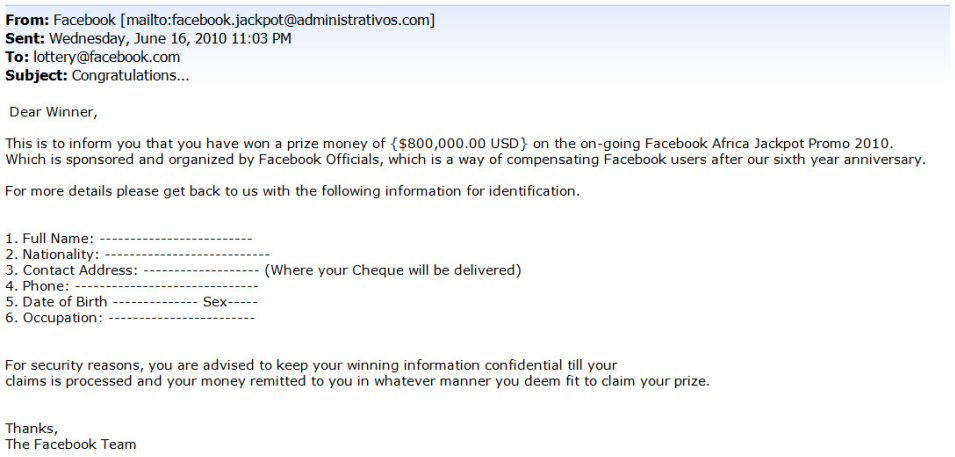
* Harry Potter Foundation.
* 83B Geffrye Street
* Potters House, Smt 4Ei
*UNITED KINGDOM.
* (Customer Services Department)
* Ref: NiG/9411X/05
* Batch: 026/05/WY83.

Dear E-mail account owner Harry Potter Foundation united kingdom is currently given out £250,000.0GBP (Two Hundred And Fifty Thousand Great Britain Pounds) as part of it bailout plans to

assist individuals and companies in this recent Global Economic melt down a=d your email address has just been nominated for

Source: Commtouch

- June also featured the "Facebook Africa Jackpot Promo" giving away $800,000 (to "compensate" you for Facebook's 6 years).



From: Facebook [mailto:facebook.jackpot@administrativos.com]
Sent: Wednesday, June 16, 2010 11:03 PM
To: lottery@facebook.com
Subject: Congratulations...

Dear Winner,

This is to inform you that you have won a prize money of {$800,000.00 USD} on the on-going Facebook Africa Jackpot Promo 2010.
Which is sponsored and organized by Facebook Officials, which is a way of compensating Facebook users after our sixth year anniversary.

For more details please get back to us with the following information for identification.

1. Full Name: ----------
2. Nationality: ----------
3. Contact Address: ---------- (Where your Cheque will be delivered)
4. Phone: ----------
5. Date of Birth ---------- Sex-----
6. Occupation: ----------

For security reasons, you are advised to keep your winning information confidential till your claims is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

Thanks,
The Facebook Team

Source: Commtouch

- In July, the "Freemasons" started sending out random invitations looking for new recruits:

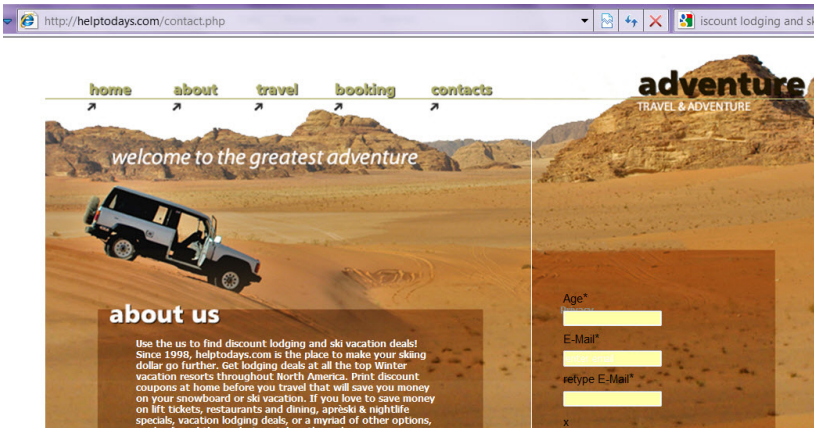
From: SECRETARY GENERAL DESK [mailto:aolreseach@aol.com]
Sent: Friday, July 02, 2010 5:43 PM
To: undisclosed-recipients
Subject: 33 DEGREE MASONIC ORDER IS INVITING YOU!!!

Dear Fellow,
It amaze to receive this Occult message in the mix of new age but your name was given to us and contact by your Local Records Center who wish you all the good
possiblities life always bring to those they loves. Establish yourself today rule this world through the help and cleansing you with Freemasonry Occult Power and members worldwide .
Be warn never share this information with anyone not even your spouse or trusted friends.
This is the secret of the ages was bring to you today.This offer is only available to America,Canada and United Kingdom Nationality only.

IF YOU INTERESTED IN THIS OFFER KINDLY REPLY IMMEDIATELY THROUGH THE EMAILS BELOW OR VISIT OUR WEBSITES
Yours Faithfully
Grand Secretary General
Freemasons' Hall

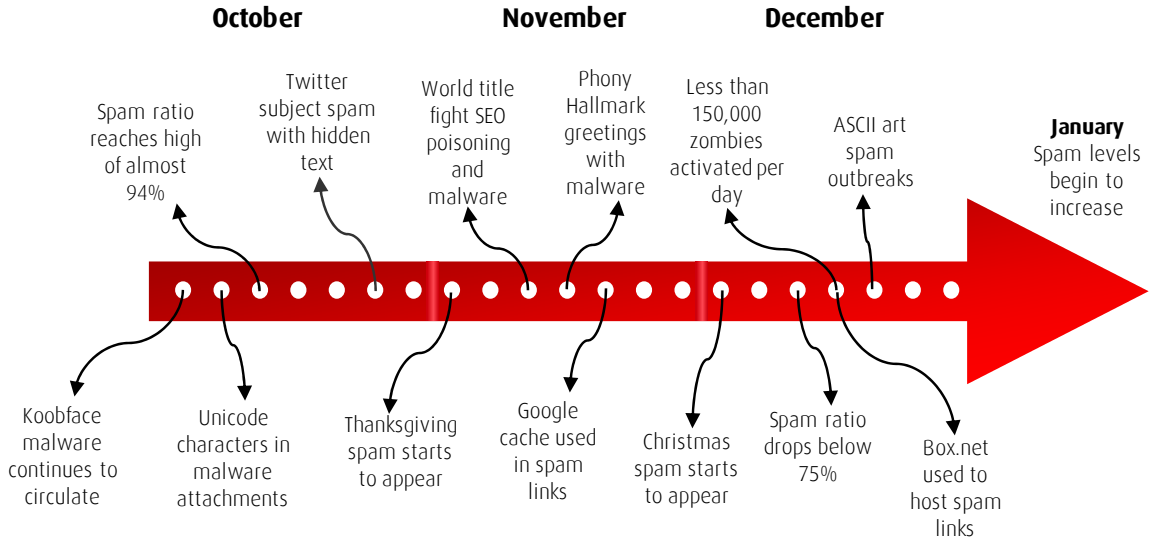
Source: Commtouch

- November uncovered a large number of email harvesting sites (well over 100 domains) that attract users with promises of amazing skiing adventure deals. Although the text deals extensively with ski holidays, the picture (featured on all of the sites) shows a somewhat warmer type of environment.



Source: Commtouch

Q4 2010 in Review



.

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 IceWarp

IceWarp® Limited is an independent software developer, targetting office, ISP and enterprise class communication solutions with over 8 years of track record in the messaging industry. IceWarp® Server is a premium messaging and collaboration platform that provides a full range of services, including secure Email, WebMail, Anti-Virus, multi-layer Anti-Spam, GroupWare, Instant Messaging, VoIP or mobile synchronization. To date it has been adopted in more than 90 thousand installations and is servicing 40 million end users world-wide.For more information visit www.icewarp.com, email us at info@icewarp.com or call 1.888.ICEWARP

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/data-and-research/spam-declines-30pc-in-q4-2010/
- http://blog.commtouch.com/cafe/email-security-news/personalized-spam-from-santa/
- http://blog.commtouch.com/cafe/email-security-news/have-yourself-a-spam-free-christmas/
- http://blog.commtouch.com/cafe/spam-favorites/ascii-art-spam-makes-a-comeback/
- http://blog.commtouch.com/cafe/data-and-research/hallmark-card-malware-run-with-a-difference/
- http://blog.commtouch.com/cafe/spam-favorites/using-google-cache-and-invisible-text-for-spam-redirect/
- http://blog.commtouch.com/cafe/email-security-news/not-a-halmark-greetings-card/
- http://blog.commtouch.com/cafe/email-security-news/compromised-yahoo-account-compromised-website-%e2%80%93-meds-for-thanksgiving/
- http://blog.commtouch.com/cafe/anti-spam/give-thanks-for-anti-spam-this-thanksgiving/
- http://blog.commtouch.com/cafe/malware/pacquiao-margarito-fight-kos-users-with-fake-av/
- http://blog.commtouch.com/cafe/email-security-news/using-unicode-to-trick-users-to-install-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.