

Internet Threats Trend Report

April 2011





In This Report

Spam declines after Rustock takedown – along with decreased number of daily active zombies	Page 2
Email-borne malware makes a comeback – up to 30% of daily email in late March	Page 4
PDF malware hides in fake Xerox scanner notification	Page 5
Facebook chat and phony Facebook apps used to spread malware	Page 5
Kama Sutra virus accompanies graphic PowerPoint presentation	Page 6
T-Online abused as part of fake antivirus scam	Page 6
Phishers “streamline” business with cloud-based form processing	Page 9
Supporters of change in Egypt fall foul of spam filters	Page 12

Q1 2011 Highlights

▲ 149 billion

Average daily spam/phishing emails sent
Page 2

▼ 258,000 Zombies

Daily turnover
Page 3

▲ Streaming media/ Downloads

Most popular blog topic on user-generated content sites
Page 14

▼ Pharmacy ads

Most popular spam topic (28% of spam)
Page 11

▼ India

Country with the most zombies (17%)
Page 3

▲ Parked Domains

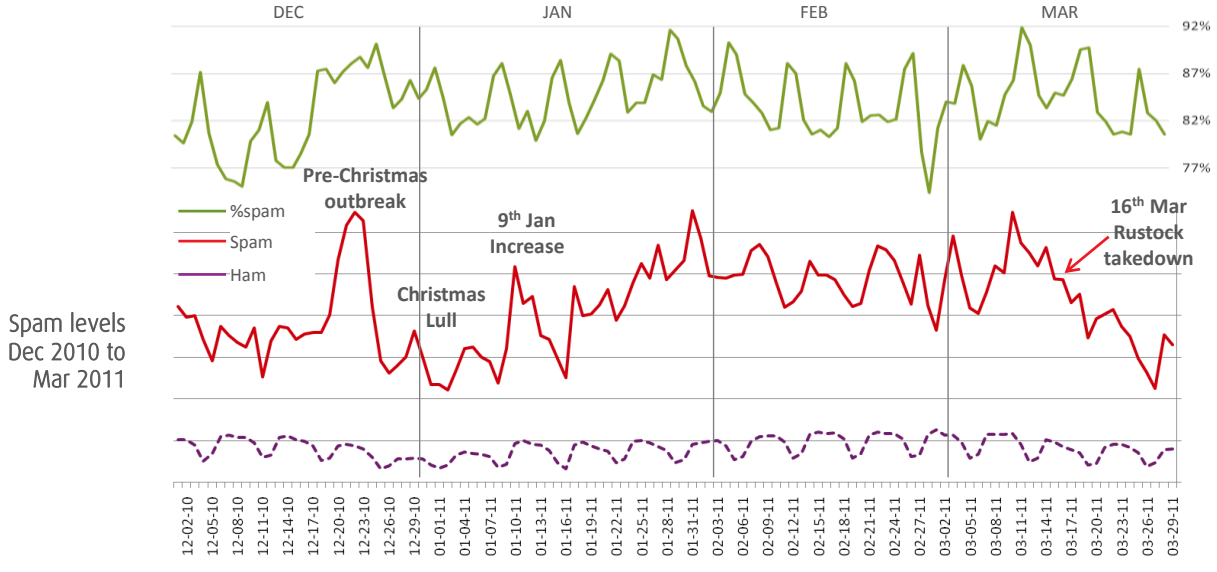
Website category most likely to contain malware
Page 8

Introduction

Statistics related to spam levels feature prominently in this Internet Threats Trend Report, as they did in the report about the fourth quarter of 2010. This is due to the wide variations observed during the first three months of 2011, and the takedown of the Rustock botnet – reportedly responsible for sending around 50 billion spam messages daily. The first quarter of 2011 was also witness to a broad range of attempts to distribute malware, and raised malware levels overall. These attempts included malware sent through Facebook chat, or which used other well-known brand-names such as T-Online and Xerox. The report also describes cybercriminals taking advantage of disused Internet forums and online form-filling services to reduce their costs.

Spam levels drop after Rustock takedown

At the start of the year, Commtouch labs observed the tail end of an unusually low-spam Christmas – New Year period. Around the 10th of January the quiet period abruptly ended and spam levels shot back up to pre-Christmas levels. The daily total jumped 45% compared to the average of the previous two weeks. The increase was attributed to the resumption of activity by the Rustock botnet – primarily sending out pharmaceutical spam.



Spam levels Dec 2010 to Mar 2011

Source: Commtouch

As shown below, average daily spam increased and then stabilized throughout the quarter. The average daily spam sent in February was nearly 165 billion spam emails per day. This was more than October 2010 (162 billion per day).

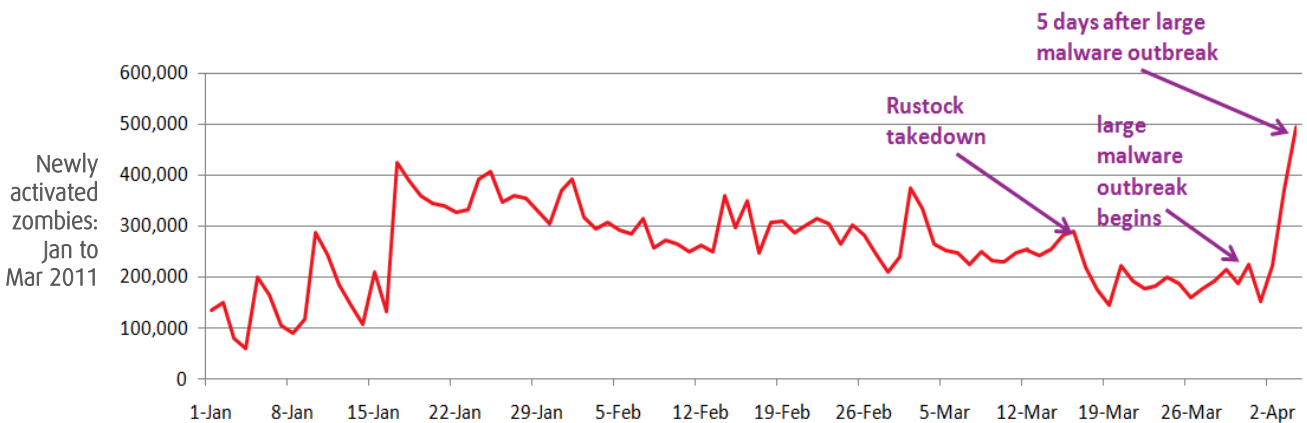
On the 16th of March, it was reported that a group of companies led by Microsoft had confiscated the command and control servers used by Rustock (almost all of which were hosted in the United States). The disconnections coupled with the disruption of the domains used by the botnet effectively disabled the Rustock botnet causing a sustained drop in spam levels. Before the takedown the average daily level in March was near 168 billion spam messages per day. Post-Rustock

this value dropped nearly 30% to an average of 119 billion messages per day during the last two weeks of the quarter.

Reduced zombie activity

The first quarter saw an average turnover of 258,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. This number shows a further decrease compared to the 288,000 of Q4 2010 and the 339,000 of the third quarter of 2010.

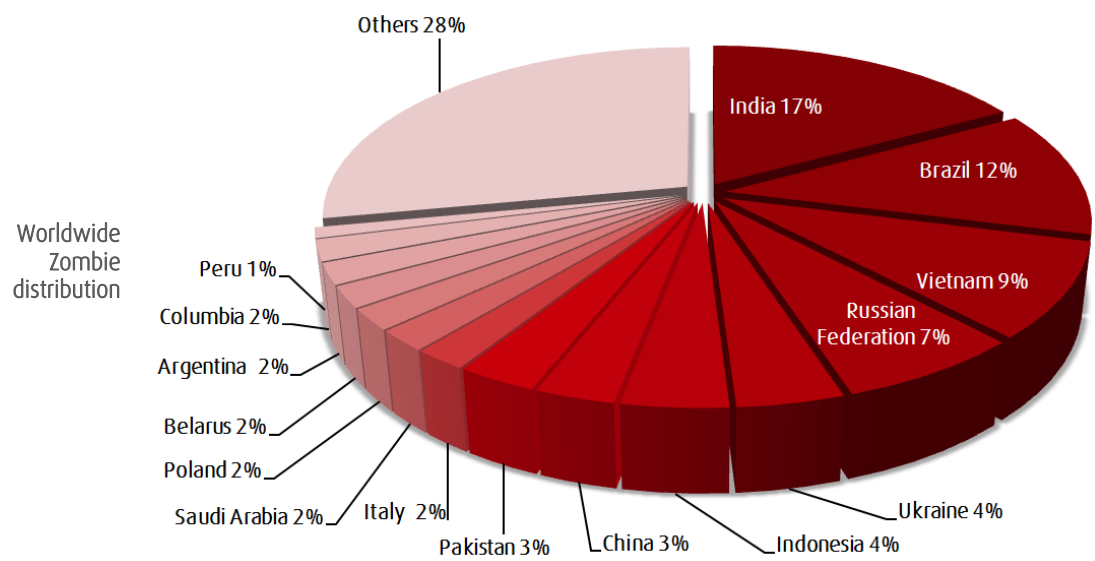
The graph below shows reduced zombie behavior in the 2 weeks after the Rustock takedown – a 25% drop on average. The large malware outbreak that took place at the end of March (see Page 4 below) resulted in large-scale recruitment of new zombies – more than doubling the daily turnover.



Source: Commtouch

Zombie Hot Spots

India again claimed the top zombie producer title hosting 17% of the global zombie population. Brazil, which had dropped to 8% and 3rd place in Q4 2010, returned to second place with 12%.



Source: Commtouch

Russia dropped 3% to 7% and Vietnam moved into 3rd place. The UK, Germany and Kazakhstan all dropped out of the top 15 replaced by Peru, Columbia and Poland.

Malware trends

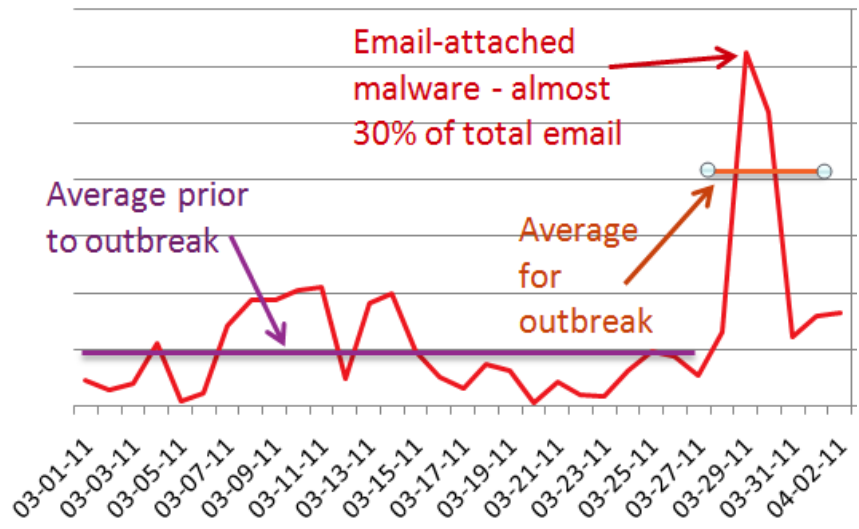
Over the last two years, virus distributors have steadily decreased their usage of email attachments as a means of malware distribution. Web-based methods have become more common as illustrated by several of the attacks described in this report.

Large email-borne malware outbreaks

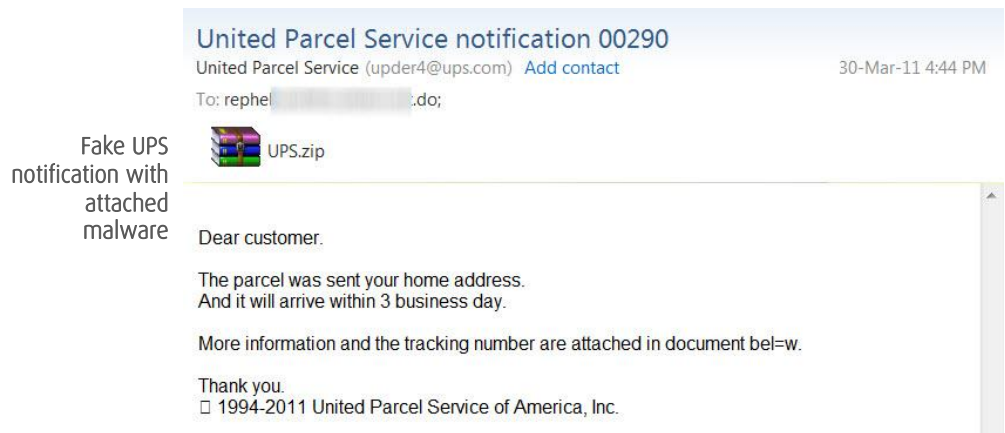
The end of March, however, saw very high levels of emails with attached malware. At one point these accounted for over 30% of all email received. The sudden increase amounted to a 400% difference compared to the running average as can be seen in the graph below:

The majority of the malware came in the form of fake UPS parcel tracking information. Email subjects started as variations of "United Parcel Service notification" and then changed to feature DHL related titles. The attached zip file extracted to an executable – but with a PDF icon. The files were detected by Commtouch's Command Antivirus as variants of W32/Bredolab. The functionality of the malware included emailing out further copies of itself, downloading additional files, and, according to some reports, stealing banking credentials.

Email-borne malware levels: Mar 2011



Source: Commtouch



Source: Commtouch

PDF malware spread in “Xerox scan” emails

February provided another example of email-attached malware. The body of the email describes the PDF attachment as coming from a “Xerox WorkCentre Pro”, a copier/scanner/printer used in offices. Commtouch’s Command Antivirus detects this malicious PDF as PDF/Expl.IQ.

Recipients who opened the file would have seen nothing – there is no text or image content displayed. The PDF file does, however, include JavaScript that targets several vulnerabilities in PDF reader applications. All of these have been patched in the most updated versions of Acrobat Reader.

Once the vulnerable PDF reader application is successfully exploited, a new piece of malware is fetched from the Internet and then installed on the affected system, further exposing the system to other attacks. Command Antivirus detects this file as W32/SuspPack.DA.gen!Eldorado.

Fake Xerox scan email with attached PDF malware



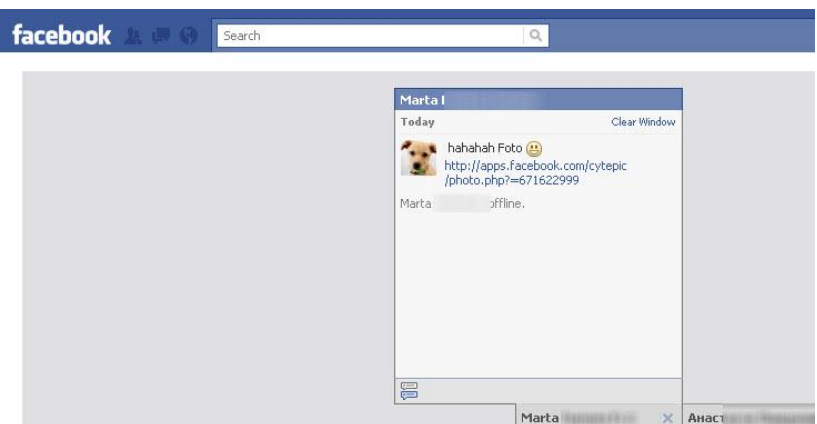
Source: Commtouch

Malware spread via Facebook chat

There were several Facebook malware incidents throughout the quarter. Among them, in January, Facebook chat messages containing malicious links were sent from compromised Facebook accounts.

The messages were typically sent to all of the compromised user’s friends. The distribution of the malware typically included the following steps:

Facebook chat message leads to phony Facebook app and malware



Source: Commtouch

- Phony Facebook application pages were created linking to a website which hosted the malware.
- Compromised Facebook accounts were used to spread chat messages linking to the phony Facebook applications and subsequently to the download of the malware file.
- The malware would then use the newly infected Facebook account to send more chat messages.

The Facebook chat messages included text such as “hahahah foto” and the phony Facebook application pages were also photo-related with names such as “cytepic” and “artephotos”. Facebook removed the phony applications within a few hours.

Kama Sutra Virus

At the start of January the "kamasutra" virus was widely circulated in the form of a link to a downloadable PPT/PPS file.

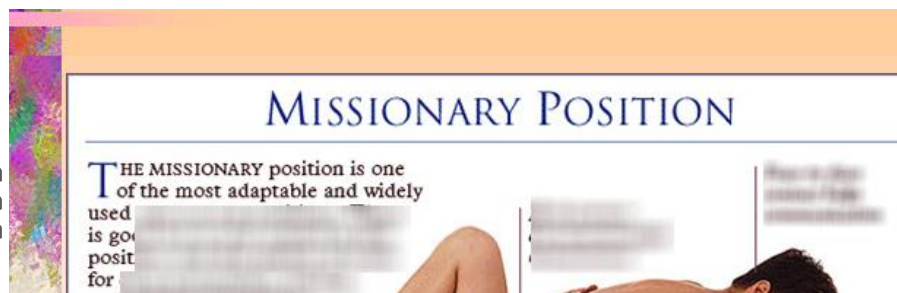
When the "presentation"

(actually an exe file) was

opened, users were treated to

"illustrated" Kama Sutra positions. In the background the malicious code installation started along with several other activities listed below:

Slide from
Kama Sutra
presentation



Source: Commtouch

The virus creates the following files which are used to display the presentation while installing the malware:

- C:\Documents and Settings\user\Local Settings\Temp\1.tmp\Real kamasutra.pps
- C:\Documents and Settings\user\Local Settings\Temp\1.tmp\Real kamasutra.pps.bat
- C:\Documents and Settings\user\Local Settings\Temp\1.tmp\acrobat.exe
- C:\Documents and Settings\user\Local Settings\Temp\1.tmp\jqa.exe

The following actions are then performed by the virus. Aside from displaying the presentation, these other activities disrupt antivirus activity and reduce the security settings of the infected PC, allowing further downloads of malware and remote control:

- Opens "Real kamasutra.pps" - this is the part where recipients actually see the PowerPoint file without suspecting that other background activities are taking place.
- Registers processes to be executed at system start
- Changes security settings of Internet Explorer
- Creates files in the Windows system directory
- Executes: Real kamasutra.pps.bat"
- Creates a hidden folder: c:\windows\~hpc1230
- Modifies the registry not to show hidden files.

Commtouch's Command Antivirus detected the file as W32/Backdoor2.HDIT.

T-Online used for fake AV

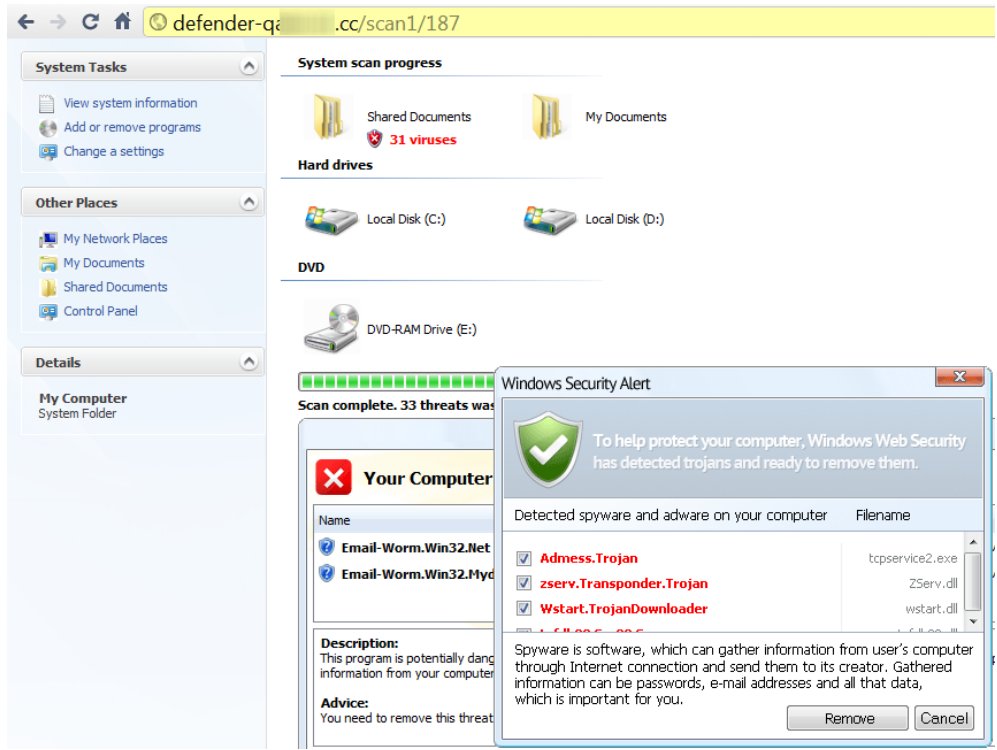
T-Online provides a free homepage service which was abused in March as part of a fake antivirus scam. The malware distributors used the innocent looking link below to lure victims.

<http://jwondersounds.homepage.t-online.de/i----2.html>

April 2011 Internet Threats Trend Report

This T-Online homepage appears blank but contains a JavaScript redirect to an "online scanner". The fake scanner naturally recommends the download of a fake antivirus that extorts money from the PC owner in order to "clean" the infection.

Web-based Fake AV "scan" following redirect from T-Online.de



Source: Commtouch

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	W32/Worm.BAOX	6	W32/Virut.AI!Generic
2	IS/Autorun	7	IFrame.gen
3	W32/Worm.MWD	8	W32/Ramnit.D
4	W32/VBTrojan.17E!Maximus	9	W32/Vobfus.L.gen!Eldorado
5	W32/Sality.gen2	10	W32/Thecid.B@mm

Source: Commtouch

Compromised websites

During the first quarter of 2011, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware or phishing. For the first time in over a year, pornographic and sexually explicit sites have been displaced by parked domains and spam sites as being the most compromised categories of sites. In both these cases though, the hosting of malware may well be the intention of the site owners. The portals category includes sites offering free homepages which are abused to host phishing and malware content (as in the T-Online case shown above).

On the list of Web categories likely to be hosting hidden phishing pages, sites related to games ranked highest, similar to last quarter.

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

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

Compromised forum sites – free dating site hosting

Source: Commtouch

Cybercriminals often hack websites to hide phishing pages or malware, and they also use this technique for free hosting of spam product pages. In the example below they have exploited inactive forums – or hacked forums – with pages of fixed spam content. The benefit for them is twofold:

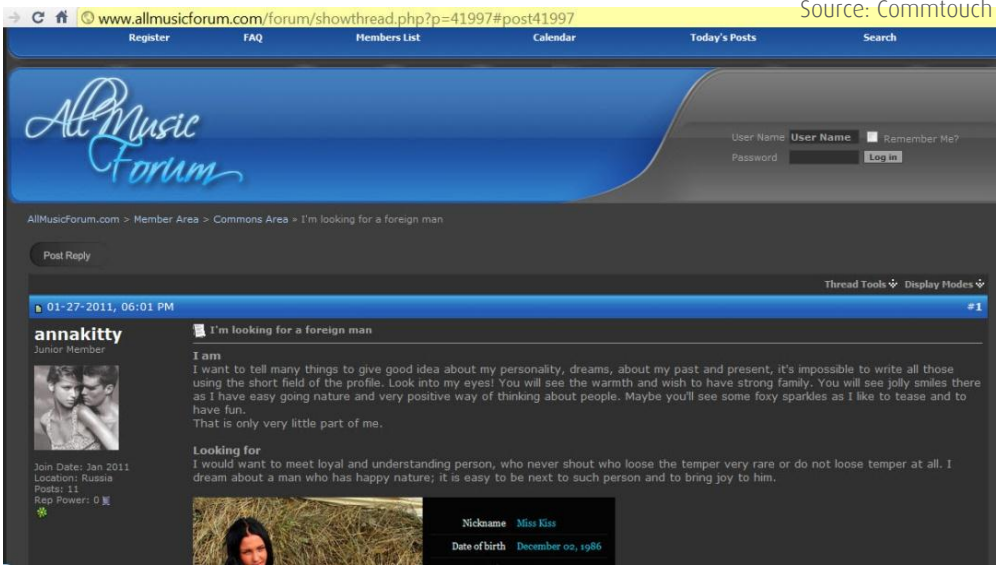
- 1) Free hosting of spam content.
- 2) The forum domains are most likely whitelisted by many URL filtering or anti-spam engines preventing these sites and associated spam emails from being blocked.

The actual legitimate topic of the forum doesn't matter – in this case the same spam content was spread across a diverse range of forums including

April 2011 Internet Threats Trend Report

programming, music, and gaming. Each post includes the same “Russian bride” information as well as links to the parent dating site.

“Gothiic-RPG” gaming forum with spam dating post



“Allmusicforum” with spam dating post

“Improved” Phishing

Source: Commtouch

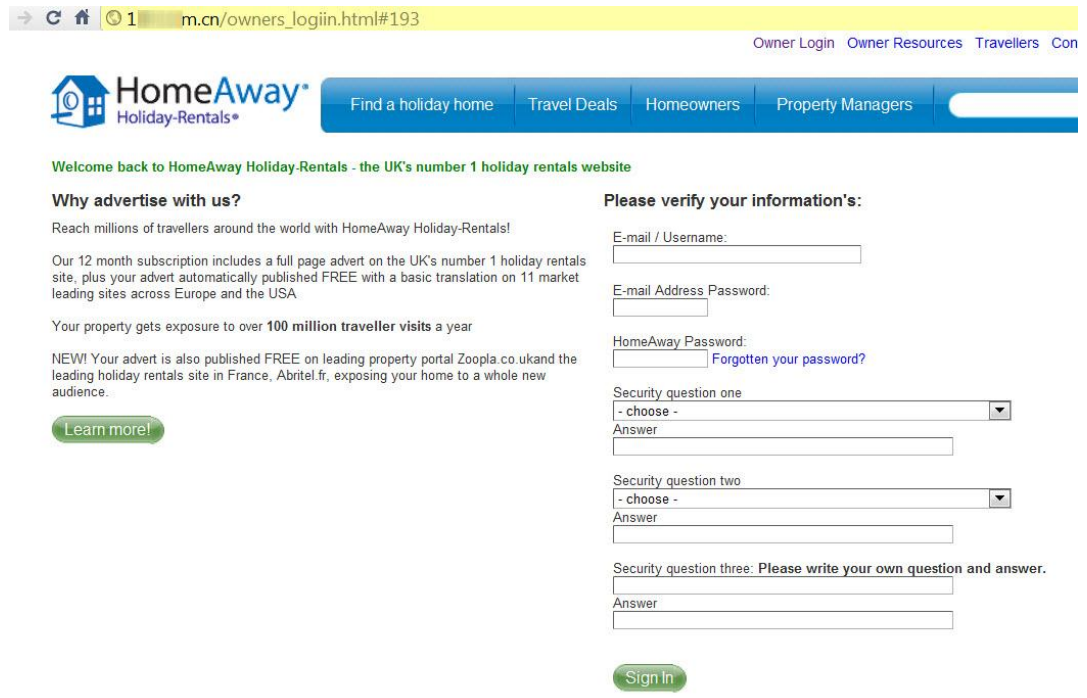
As shown in the table above (Website categories infected with phishing), phishers often use legitimate sites to host their phishing pages. This quarter saw evidence of a further method used by phishers to cut costs and streamline the phishing process. The following stages are involved in a traditional phishing attack:

1. Create the phishing page – either hidden within a legitimate site or hosted on some temporary server.

April 2011 Internet Threats Trend Report

- 2. Send out carefully socially engineered phishing emails including the link to the phishing page.
- 3. Collect data submitted to the page by deceived recipients. In the attack shown below this stage is streamlined.

The attack shown below targets users of HomeAway holiday rentals.



HomeAway Holiday Rentals phishing page uses online form management

Source: Commtouch

A look at the page source reveals that the filled in form is sent to "formbuddy.com" and not collected directly by the phisher. Formbuddy.com offers a similar service to that found in the forms feature of Google docs – cloud-based form result collection and management. The site collects and stores all the responses to the "form" shown above and then emails a neat summary to the phisher (whose login name is "fanek"). In other words the phisher does not have to worry about creating/managing/storing back end form data collection and can more easily scale the harvesting of phished data.

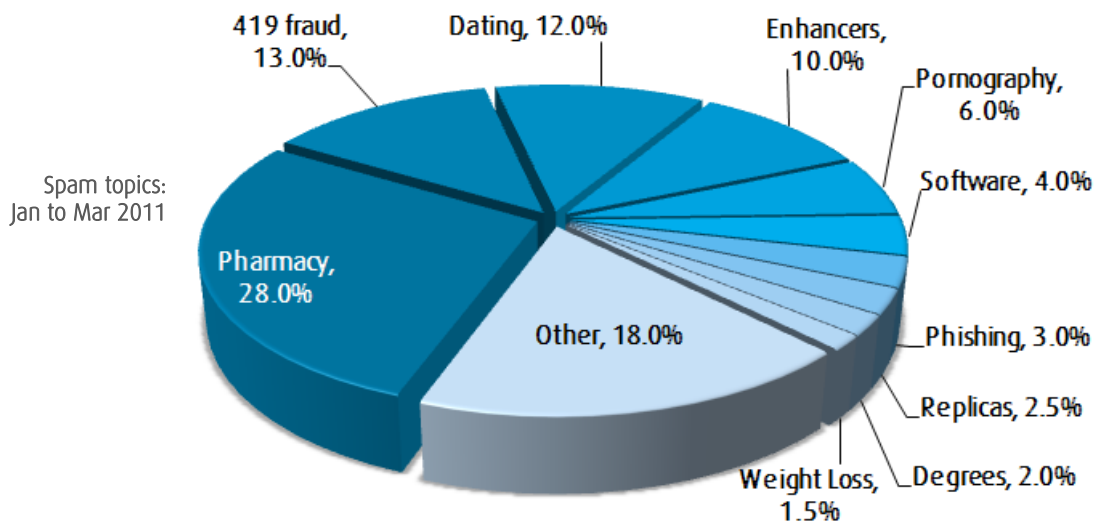
Phishing page source shows use of "Formbuddy" online form management for user "fanek"

```
<br><br> Your property gets exposure to over <b>100 million  
traveller visits</b> a year <br><br> NEW! Your advert is also  
published FREE on leading property portal Zoopla.co.ukand the leading  
holiday rentals site in France, Abritel.fr, exposing your home to a whole  
new audience.<br><br>  
</p>  
<a href="/info/advertise-with-us" class="gtb"><span>Learn  
more!</span></a> </div> </div>  
<h2>Please verify your information's:</h2> <form  
action="http://www.formbuddy.com/cgi-bin/form.pl" method="post"  
id="loginForm"><input type="hidden" name="username" value="fanek"><input  
type="hidden" name="reqd" value="0"><input type="hidden" name="url"  
value="http://www.holiday-rentals.co.uk/">
```

Source: Commtouch

Spam Topics

Pharmacy spam remained in the top spot but continued to drop this quarter to only 28% (down from 42% in Q4 2010). 419 fraud, enhancements, and Dating all increased.



Source: Commtouch

Valentine's spam

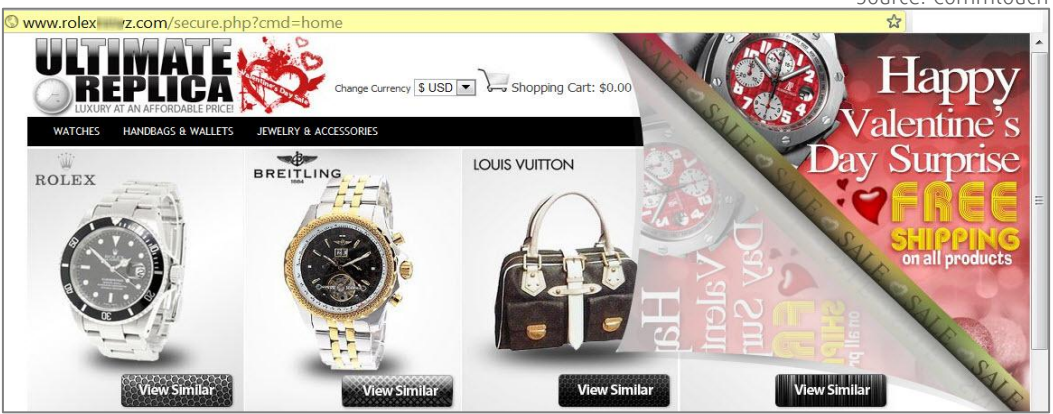
February brought along typical outbreaks of Valentine's Day spam. In fact Valentine's themed subjects had already started appearing in late January. The subjects ranged from dating to replicas to fast cash offers – some examples:

- happy st valentine™s with mydatelab.com!
- valentine day sale now on
- the best valentines gifts
- valentine day jewelry sale
- valentine's day gift !50% off on water resistant wrist watch
- need cash for valentine's?
- save 25% on valentine's day flowers

Destination sites were suitably dressed for the occasion.

Source: Commtouch

Replica website with Valentine's Day theme



Mass emailings support change in Egypt

In addition to the much publicized use of Facebook and Twitter to organize protests, supporters of change in Egypt (and other countries in the Middle East) also used email to spread the word. The emails were spread using the traditional "forward this to all your contacts". The subjects included:

- Stand with Egypt
- All Egyptians are together
- Important ... A must read
- Unrest in Egypt
- A Call to the People and Governments of the Free World
- Save Egypt
- Help Egyptian protesters

The senders of course faced the same dilemma faced by any mass-email campaign i.e.: when do the constant emails from so many sources cross the line and become ... spam. The answer in this case is clearly in the eye of the recipient. For many email users unsolicited email equals spam – some of these appear below.

Samples of emails supporting change in Egypt

From: SALAM YOUSRY eltan [mailto:eltan@com] Sent: Sun 30-Jan-11 3:57 AM
To: [redacted]
Cc: [redacted]
Subject: A Call to the People and Governments of the Free World

We call upon all of you to support the Egyptian people's demands for a life of dignity, liberty and an end of despotism. We call upon you to urge this dictatorial regime to stop its bloodshed of the Egyptian people, exercised throughout the Egyptian cities, on top of which comes the city of Suez.

We believe that the material and moral support offered to the Egyptian regime, by the American government and European governments, has helped to suppress the Egyptian people.

We hereby call upon the people of the free world to support the Egyptian people's non-violent revolution against corruption and tyranny. We also call upon civil society organisations in America, Europe and the whole world to express their solidarity with Egypt, through holding public demonstrations, particularly on the coming weekend that follows People's Anger Day (28/01/2011), and by denouncing the use of violence against the people.

We hope that you will all support our demands for freedom, justice and peaceful change.

Extra line breaks in this message were removed.

From: Alaa Ali [mailto:alaa@net] Sent: Sun 30-Jan-11 3:31 PM
To: [redacted]
Cc: [redacted]
Subject: Stand with Egypt (fwd)

Dear friends,

Millions of brave Egyptians are right now facing a fateful choice. Thousands have been jailed, injured or killed in the last few days. But if they press on in peaceful protest, they could end decades of tyranny.

The protesters have appealed for international solidarity, but the dictatorship knows the power of unity at a time like this - they've desperately tried to cut Egyptians off from the world and each other by completely shutting down the internet and mobile networks.

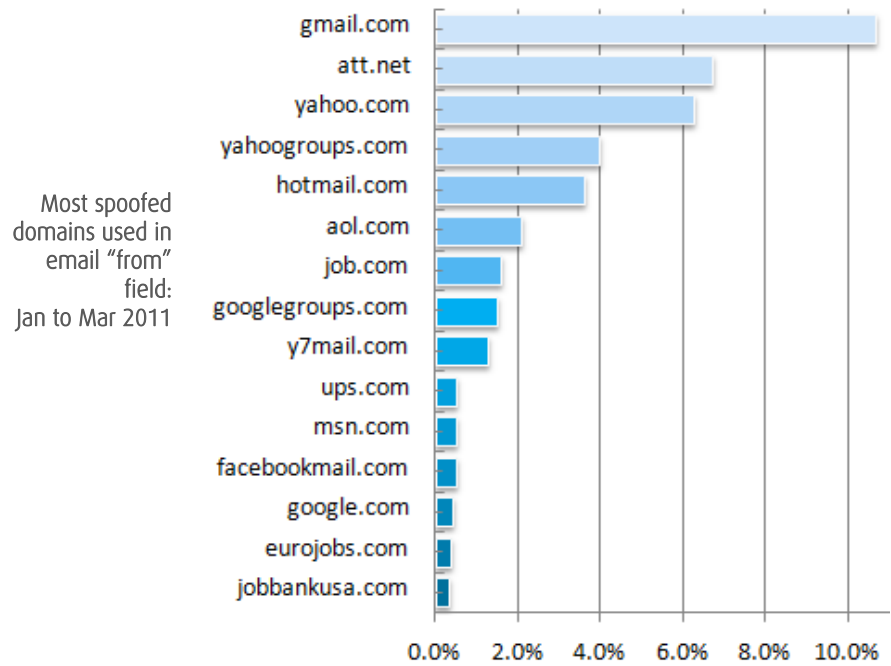
Satellite and radio networks can still break through the regime blackout - let's flood those airwaves with a massive cry of solidarity showing Egyptians that we stand with them, and that we'll hold our governments accountable to stand with them too. The situation is at a tipping point - every hour counts - click below to sign the solidarity message, and forward this email:

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.

April 2011 Internet Threats Trend Report

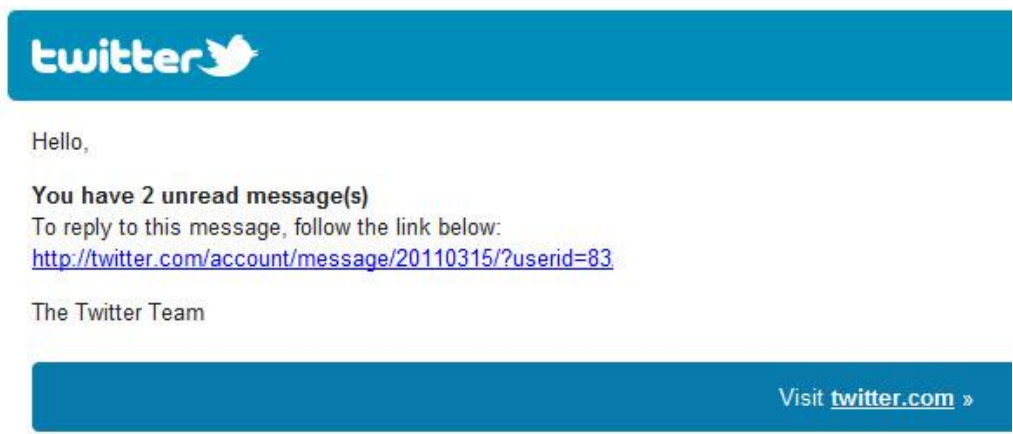


Source: Commtouch

This quarter, gmail.com is once again the most spoofed domain displacing yahoo.com which held the top spot in Q4 2010. 10th place is held by ups.com due to the very large numbers of fake UPS notification emails sent as part of the March outbreak (see page 4 above). dhl.com, used in the later stages of the same outbreak, is in 17th place.

In 40th place was postmaster.twitter.com – used extensively throughout the quarter to distribute fake Twitter notifications with links that led to pharmacy sites.

Fake Twitter notifications lead to pharmacy sites



Source: Commtouch

Sillyspam

As always, spammers provided amusement during the first 3 months of 2011 – a collection of favorites:

- February’s overly apologetic spammer probably didn’t convince the many millions of recipients that he really was sorry. Some sample subjects:

- sorry:try to change your potency. tb
 - sorry:bbuyy viiaqra super active plu
 - sorry:viaaqrta sseeexual lifestyle
 - sorry:viaaqrqa – have the courage to
 - sorry:viiaqra – make xseex
 - sorry:viagra profesfional – your v
 - sorry:heaklth specialicsts
 - etc.
- In their attempts to spread huge amounts of malware (see page 4 above), the distributors changed the campaign from “UPS packages” to “DHL packages”. They forgot, however, to change the attachment name resulting in UPS malware being couriered by DHL!
 - The iPad 2 predictably featured in some campaigns but this one was surely supposed to be more personalized than {email address}. Mail merge fail?

Marketing scam email for iPad 2. Subject shows mail merge fail



Apple iPad 2 for {Email Address}

Thanks for Responding (info@... net) Add contact

To: Clifford;

Experience web, email, photos and video like never before on Apple's newest tablet.

You have been selected to get a new Apple iPad 2 – **FREE!**

Participation Required. See below for details.

Continue

Thinner. Lighter. Faster. FaceTime, Smart Covers, 10-hour battery. **BONUS, sign-up today & receive a \$100 iTunes Music Card!**

Source: Commtouch

Source: Commtouch

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.

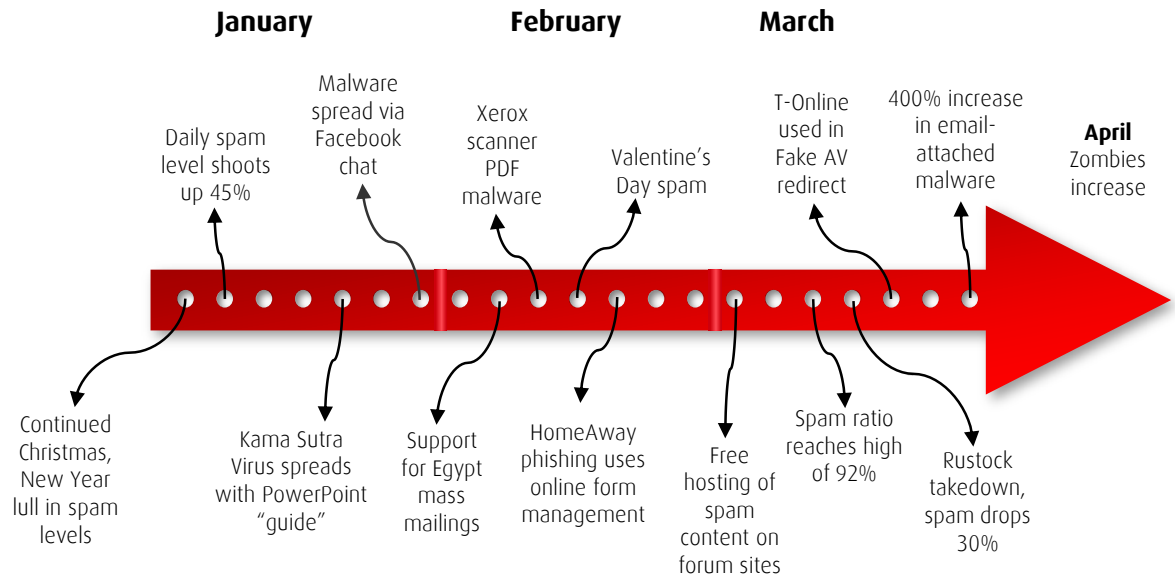
In this quarter's analysis, "streaming media and downloads" was again the most popular blog or page topic, increasing slightly to 21% of user-generated content. The streaming media & downloads category includes sites with live or archived media for download or streaming content, such as Internet radio, Internet TV or MP3 files. Entertainment blogs typically cover television, movies, and music as well as hosting celebrity fan sites and entertainment news.

April 2011 Internet Threats Trend Report

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

Source: Commtouch

Q1 2011 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 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

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/email-security-news/ups-malware-now-sent-via-dhl/>
- <http://blog.commtouch.com/cafe/email-security-news/huge-amounts-of-ups-and-facebook-malware-attachments/>
- <http://blog.commtouch.com/cafe/anti-spam/ipad-2-affiliate-marketing-scams-and-incompetent-spammers/>
- <http://blog.commtouch.com/cafe/malware/t-online-used-for-fake-av/>
- <http://blog.commtouch.com/cafe/anti-spam/has-the-reported-disruption-of-rustock-affected-spam-levels/>
- <http://blog.commtouch.com/cafe/anti-spam/loads-of-phony-twitter-emails/>
- <http://blog.commtouch.com/cafe/phishing/how-to-scale-phishing-by-using-the-cloud/>
- <http://blog.commtouch.com/cafe/anti-spam/free-hosting-of-spam-content-on-forum-sites/>
- <http://blog.commtouch.com/cafe/spam-favorites/the-apologetic-spammer/>
- <http://blog.commtouch.com/cafe/spam-favorites/spammers-feel-the-love-on-valentine%e2%80%99s-day/>
- <http://blog.commtouch.com/cafe/malware/how-pdf-files-hide-malware-example-pdf-scan-from-xerox/>
- <http://blog.commtouch.com/cafe/email-marketing/mass-emailings-support-change-in-egypt-and-now-syria/>
- <http://blog.commtouch.com/cafe/malware/malware-spread-via-facebook-chat/>
- <http://blog.commtouch.com/cafe/malware/kama-sutra-virus-%e2%80%93-a-position-you-don%e2%80%99t-want-to-get-into%e2%80%a6/>
- <http://blog.commtouch.com/cafe/data-and-research/spammers-return-from-holiday/>
- <http://blog.commtouch.com/cafe/data-and-research/spam-declines-30pc-in-q4-2010/>

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)

Copyright© 2011 Commtouch Software Ltd. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch, Authentium, Command Antivirus and Command Anti-malware are registered trademarks, of Commtouch. U.S. Patent No. 6,330,590 is owned by Commtouch.

commtouch[®]
Real Security. In Real Time.