



Real Security. In Real Time.

Q2 2009 Internet Threats Trend Report

New Trojan Variants Stump Most Major AV Engines

July 14, 2009

Introduction

The major news of the second quarter was the massive rise in email-borne viruses not caught by major anti-virus engines. One explanation for the dramatic rise is the appearance of aggressive new variants of several different Trojans. Anti-virus companies have been unable to produce new signatures in time to protect their customers. Some companies try to develop generic signatures, but these have proven ineffective in an outbreak of this size.

Throughout the quarter, there was an increase in the number and complexity of legitimate sites hijacked by hackers. Once-popular image spam also made a comeback this quarter with new tactics to bypass some anti-spam engines.

Another popular tactic this quarter was the use of current events to appeal to the emotional senses of recipients around the world. Global events including the death of pop superstar, Michael Jackson, and the spread of the swine flu were popular spam subjects.

Q2 2009 Highlights

- Spammers and malware distributors used current events including the Swine Flu epidemic and death of Michael Jackson to spread their messages.
- Sites in the "Health" and "Web-based email" categories topped the list of Web categories manipulated by phishing schemes.
- "Business" was the Web site category most infected with malware.
- An average of 376,000 zombies were newly activated each day for the purpose of malicious activity.
- Image-based spam returned with new tactics foregoing MIME-format standards to bypass some anti-spam engines.
- Spam levels averaged 80% of all email traffic throughout the quarter, peaking at 97% in April and bottoming out at 64% in June.
- Brazil continues to produce the most zombies, responsible for 17.5% of global zombie activity.



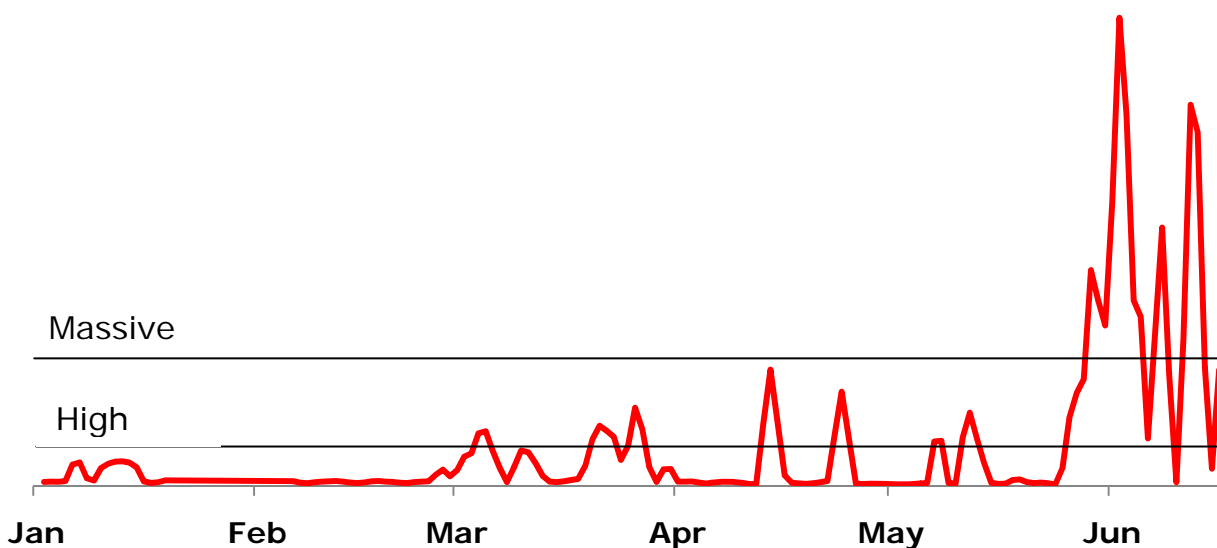
Real Security. In Real Time.

Sharp Rise in Number of Viruses Missed by Major AV Engines

From late May through June, Commtouch Labs identified a sharp rise in the number of new viruses being circulated via email that were not caught by the major anti-virus engines. There were several malware outbreaks whose wide distribution caused malware numbers to temporarily and exponentially increase from the consistently low quantities of malware distributed via email during the past 18 months.

One explanation for the dramatic rise is the appearance of aggressive new variants of several different Trojans. With each new variant, there is a period of time during which anti-virus companies recognize it and then develop new signatures to protect their customers. The companies have tried blocking new variants with a dedicated signature per variant. This method proved inefficient, so security vendors have begun to develop generic signatures to block all variants of the same malware family. As demonstrated by this massive growth, the generic signatures have not proven to work against the recent variants.

Total viruses missed by major AV engines (Q1 & Q2 2009)



Source: Commtouch Labs



Real Security. In Real Time.

Top 10 Viruses Missed by Major AV engines (May 20 – June 30, 2009)

	MD5 Checksum	Common Name
1	4be0d4b1dbc2d7ba92b6c920388ae4bb	Mal/WaledPak-A
2	fa5f6094f90a001d1fc742c7c036be7a	Mal/FakeVirPk-A
3	2c677cf98d1a4aa1f95ca456a6dfa18b	Troj/Agent-KBE
4	53d15dc652a2534572981bab1e2eddf3	Troj/Agent-JZY
5	c81ba436d85bba944adb74b86c90fae8	Mal/WaledPak-A
6	1396f9770b2702312c76987ca31e6866	Mal/WaledPak-A
7	7d06f4fc766b84faf02a91063946a96b	Mal/FakeVirPk-A
8	de90a24f3dfb5c1c8d4a0a3104f3dd4a	Mal/WaledPak-A
9	ad2b80463042d88056dc104c41e2a03e	Troj/Agent-KBJ
10	c17e6929f32dd05d718c83c2aae219bb	Troj/Dloadr-CMT

Source: Commtouch Labs



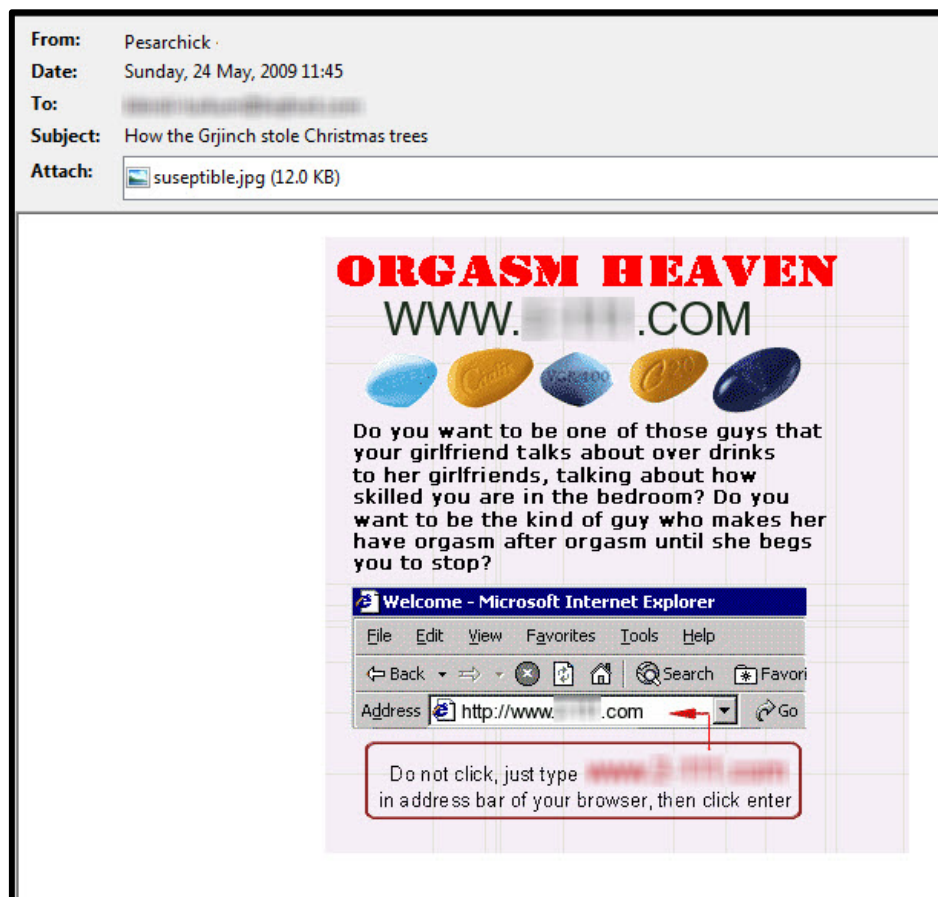
Real Security. In Real Time.

Spam

Companies around the world continue to send millions of unsolicited emails, clogging inboxes and decreasing productivity. This quarter saw a return of image spam and the use of current events to entice readers.

Image Spam Returns

The second quarter of 2009 saw the return of once-popular image spam. These messages, as seen in the recent sample below, consist of an image (usually .jpg), embedded into email messages using new tactics, foregoing MIME-format standards, to bypass traditional spam filters. Spammers discovered that popular email clients like Outlook are not strict about image embedding formats; if an image is found by the email client, even if not inserted in the correct format, the email client will display it. Some anti-spam engines may fail to parse the image and will not detect it, thereby allowing it into the inbox.



Source: Commtouch Labs



Real Security. In Real Time.

United Nations 419 Scheme

419 schemes have circulated the Internet for many years. Examples include emails claiming that the recipient has won \$2,000,000 or that someone found a bank account that belonged to the recipient's long lost relative and that he or she is listed as the beneficiary. These intricate scams have spanned many years and several unknowing individuals have been convicted of fraud or money laundering simply because they were fooled into believing the scams.

In April, an outbreak put new life into the 419 schemes seen in the past. As seen in the example, the email appears to have been sent from the United Nations.

It message states:

"This message is to all the people that have been scammed in any part of the world, the United Nations have agreed to compensate them with the sum of US\$500,000. This includes every foreign contractors that may not have received their contract sum, and people that have had an unfinished transaction or international businesses that failed due to Government problems etc."

They claim to have a database of victims' names and instruct the recipient to contact "Jim" in Nigeria. Jim has \$50,000 for each person that contacts him with bank account information.

To further confuse recipients, the scammers included the United Nations logo and an official-looking footer image.



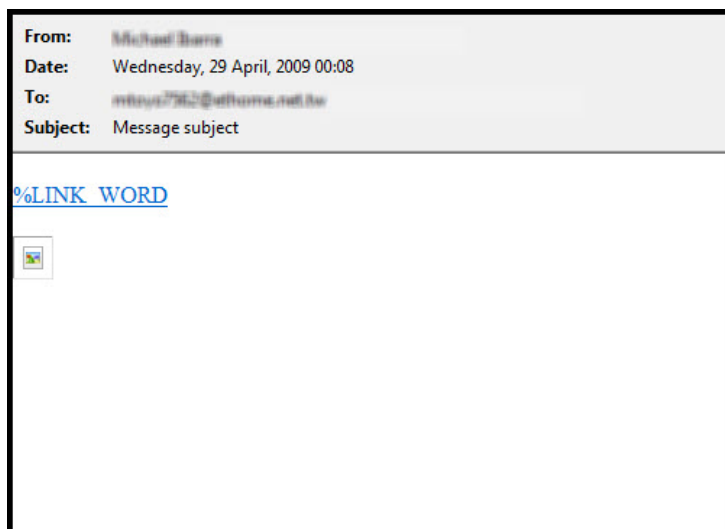
Source: Commtouch Labs



Real Security. In Real Time.

Simple Mistakes Lead to Spam Mess

The mail merge feature has made life easier for administrative assistants and spammers around the world. With mail merge, it is simple to prepare personalized mail for a group of people – whether it's five people or 500 thousand people. Mail merge is not 100% foolproof, and Commtouch Labs identified an outbreak in April proved its fallibility (see sample to the right).



Source: Commtouch Labs

The image is missing and the text is an HTML mess. Upon opening the mail with a text editor (pictured below), it appears that there was a mistake replacing the `%VARIABLE`, where `VARIABLE` should have been replaced by a corresponding value in the spammer's database (e.g. a URL or a name).

```

-----8065629171861215
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
<META HTTP-EQUIV=3D"Content-Type" CONTENT=3D"text/html; charset=3Dbig5">
<TITLE>%TITLE</TITLE>
</HEAD>
<BODY BGCOLOR=3D#FFFFFF LEFTMARGIN=3D0 TOPMARGIN=3D0>
<br>
<a href=3D"http://%R_SUB%HTTP/sports/taichidvd/">%LINK_WORD<br><br>
<IMG SRC=3D"http://%PIC/sports/taichidvd/0.jpg" ALT=3D"" border=3D"0"></a>=
<br>
<br>
</BODY>
</HTML>

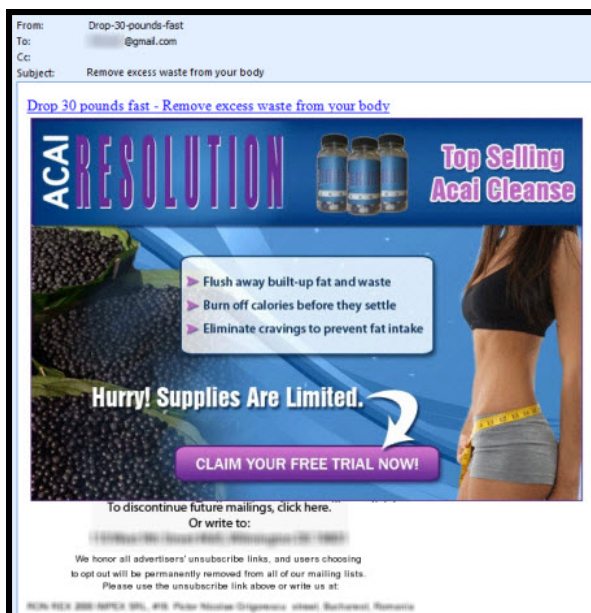
-----8065629171861215--
    
```

Source: Commtouch Labs



Real Security. In Real Time.

Spam Slips Through Gmail Filters



Source: Commtouch Labs

Users of the Gmail free email service have become accustomed to inboxes that are nearly free of spam.

Through May and June, however, a bug in the Gmail spam filters changed this. Some Gmail users noticed a sharp increase in the amount of spam that bypassed the filters and ended up in their inboxes.

Spam like the sample to the left - promoting weight loss supplements - bypassed Gmail's spam filters in May.

Another example (pictured below), offers free HD or DVR.

As of the time of publication of this report, Google had not offered an explanation for

this malfunction but at the end of April, an employee assured the community in a Gmail forum that Google is investigating it and looking for a fix. In June, another employee announced that several fixes had been implemented and that spam levels should go back to normal.

Gmail subscribers should remember that Gmail is a free service in beta stage; paid services are typically held to a higher standard than free services.



Source: Commtouch Labs



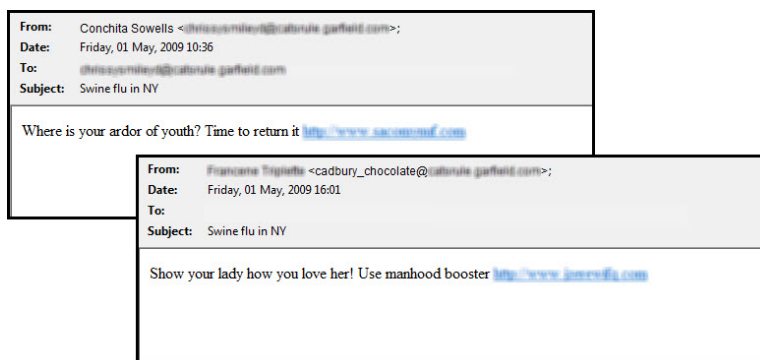
Real Security. In Real Time.

Swine Flu Spam Invades Inboxes Around the World

As the H1N1 flu (also known as “swine flu”) began to make its way around the world and create panic among travelers, spammers tried to cash in on the frenzy. In May, analysts in the Commtouch Labs reported on several spam attacks that incorporated the phrase “Swine Flu” as a means of social engineering — the pandemic was such a popular topic this quarter that recipients would have been more likely to open a message related to it.

Swine Flu Enhancement Spam

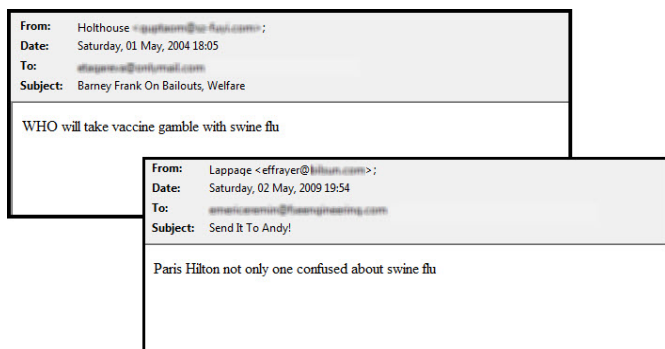
In the first outbreak example (pictured to the right), the emails included “Swine Flu” in the subject line to grab a recipient’s attention. The body of the emails are unrelated to the Swine Flu, but read much like sexual enhancement spam of the past.



Source: Commtouch Labs

The links in both examples led to pharmacy sites featuring sexual enhancement drugs, not a Swine Flu vaccine.

Directory Harvesting Swine flu Spam



Source: Commtouch Labs

A later outbreak was used to harvest email addresses for spammers. it appears that the spammers employed an automatic subject/body generator to formulate random combinations of email subjects and content. In one example, the spammer combined the economic crisis (subject line) with the Swine Flu epidemic (body). The second email combined random names in the subject line with both Paris Hilton and the Swine Flu in the body.

While a harvesting attack is not sent to lure recipients to buy products from various Web sites or download malware, the emails are sent in huge numbers to check the validity of large groups of email addresses. Once valid email addresses have been harvested, spammers use the lists as targets for new attacks.



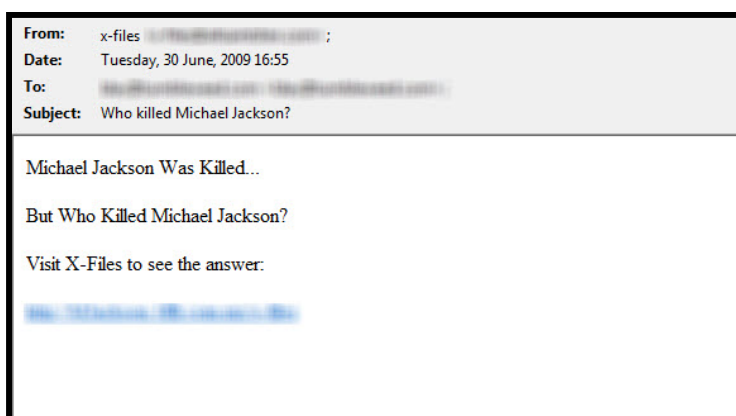
Real Security. In Real Time.

Web Security Threats

The Internet has become an indispensable part of everyday life and work, yet the massive growth of data coupled with a rapid increase in the number of individuals with Web access has introduced a variety of security issues.

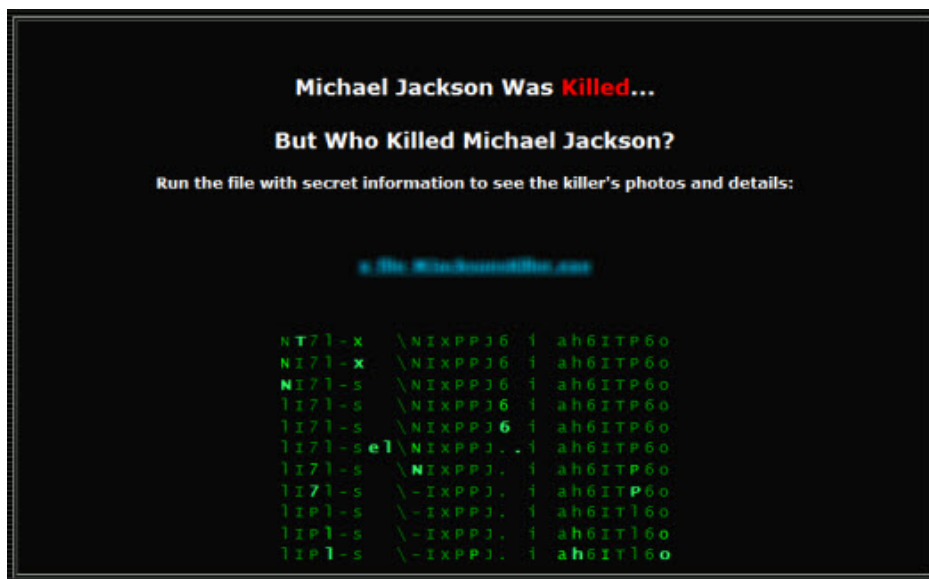
Malware Keeps Michael Jackson Legacy Alive

In the wake of Michael Jackson's untimely death at the end of June, cyber criminals began using his name to flood the world with spam and malware. Shortly following his death, several news sources detailed harvesting spam campaigns that circulated the globe, for spammers to verify email addresses by luring recipients to click on links.



Source: Commtouch Labs

As the hours passed, the campaigns became more sophisticated and morphed into blended threats – spam messages with links to Web sites that contain malware. The outbreak sample pictured here reportedly spread a virus that can disable firewalls and steal personal identifying information, including financial data.



Source: Commtouch Labs

The link in the email led to the page seen below, where one is prompted to download an executable file that contains the data-stealing virus.



Real Security. In Real Time.

Q2 2009 Internet Threats Trend Report

Decoding the %XX characters produced this:

```
<script language=javascript>document.write(
  <script language="javascript">
  funct
  (s.length-
  </scr
  );
dF('*8Hmyr
7Bfxhwnuy6
7Bfxhwnuy*
7Eiwzlxhqjfs3htr*77*7%3E*8G*5F*8H4xhwnuy*8J*5F*8H4mjfi*8J*5F*8Hgti%
7E*8J*5F*8H4gti%7E*8J*5F*8H4myrq*8J5')
</script>
```

Source: Commtouch Labs

The final decoded HTML looks like this (a complex function that creates the redirection code and executes it):

```
<html>
<head>
<script language="JavaScript1.1" type="text/javascript">
  location.replace("http://www.
</script>
</head>
<body>
</body>
</html>
```

Source: Commtouch Labs

The intricate scripting and code produced an HTML redirect to the site pictured to the right, which was also infected with a Trojan.

Typically, these pharmaceutical sites just send spam to boost their sales, but this outbreak included a virus. It was a complicated scheme devised to bypass traditional spam and Web filters and spread a Trojan.



Source: Commtouch Labs

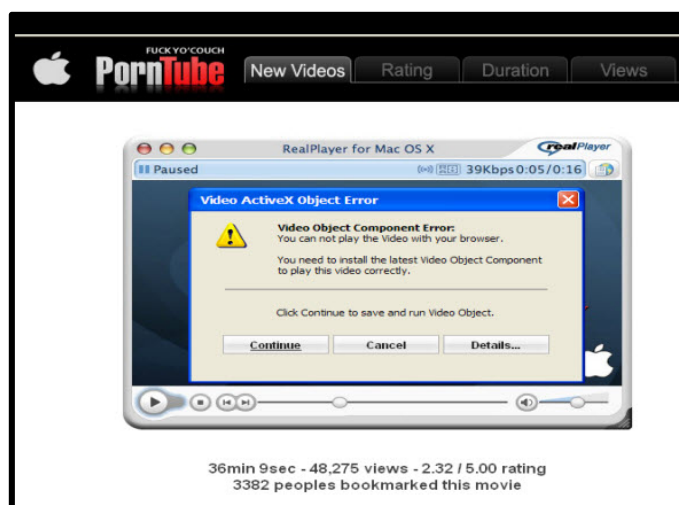


Real Security. In Real Time.

Mac Malware on the Rise

At the beginning of June, security researcher Jerome Segura from ParetoLogic, a Commtouch Security Alliance member, discovered a new Mac OS X malware variant, known as OSX/Jahlav-C.

The file is distributed as a “video codec” or “software crack, keygen” and uses familiar names such as QuickTime.dmg, MacTubePlayer.dmg or crack_photoshop.dmg.



Source: ParetoLogic

Once the user is infected, the payload is that of a DNS changer, where Web links are redirected to adult sites or advertisements, pop-ups are generated for ads or scareware programs (e.g. Rogue Antivirus applications) and the system becomes slower overall and vulnerable to more attacks.

The malicious sites pushing the malware target both PCs and Macs. Depending on the “user-agent,” a system and browser identifier, the “.EXE” file for the PC, or “.DMG” file for the Mac, is delivered.

While the debate still exists whether the Mac is more secure than the PC, Researchers at ParetoLogic assert that it is clear that malware authors are expanding their surface of attacks by adding as many platforms and browsers as they can. The company is observing an increasing number of Mac Trojans in the wild and expect this trend to continue for the rest of 2009.



Malware and Phishing Trends

During the second quarter of 2009, Commtouch analyzed which categories of Web sites were most likely to contain malware or phishing. As expected, pornographic and sexually explicit sites plus sites with streaming media and downloads ranked high in the categories infected with malware. Less expected on the list were the education sites.

On the list of Web categories manipulated by phishing, download sites, Web-based email and social networks continue to fall victim to new phishing schemes.

Top 10 Web Categories Infected with Malware	
Rank	Category
1	Business
2	Pornography/Sexually Explicit
3	Computers & Technology
4	Streaming Media & Downloads
5	Shopping
6	Search Engines & Portals
7	Health & Medicine
8	Personal Sites
9	Real Estate
10	Education

Source: Commtouch Labs

Top 10 Web Categories Manipulated by Phishing	
Rank	Category
1	Health & Medicine
2	Web-based Email
3	Computers & Technology
4	Finance
5	Chat
6	Instant Messaging
7	Search Engines & Portals
8	Social Networking
9	Download Sites
10	Shopping

Source: Commtouch Labs



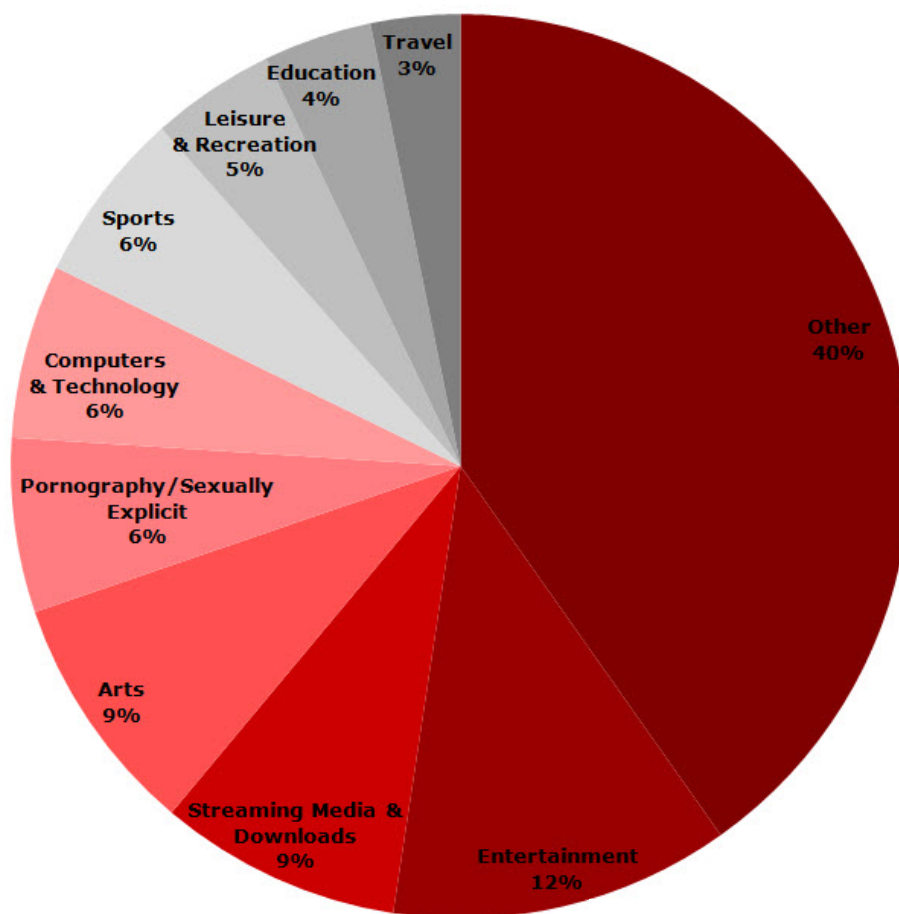
Real Security. In Real Time.

Web 2.0 Trends

In an analysis of six of the most popular user generated content hosts, entertainment was the most popular subject, covering 13 percent of the generated content. Following closely behind was streaming media and downloads (9 percent) and arts (9 percent). Pornography and sexually explicit content placed fourth with 7 percent.

When evaluating user generated content in relation to malware and phishing, some of the most popular categories appear on both lists. Streaming media and downloads, for instance, are among the top 10 Web site categories infected with malware. They are also two of the most popular categories within user generated content sites.

Most Popular User Generated Content



Source: Commtouch Labs

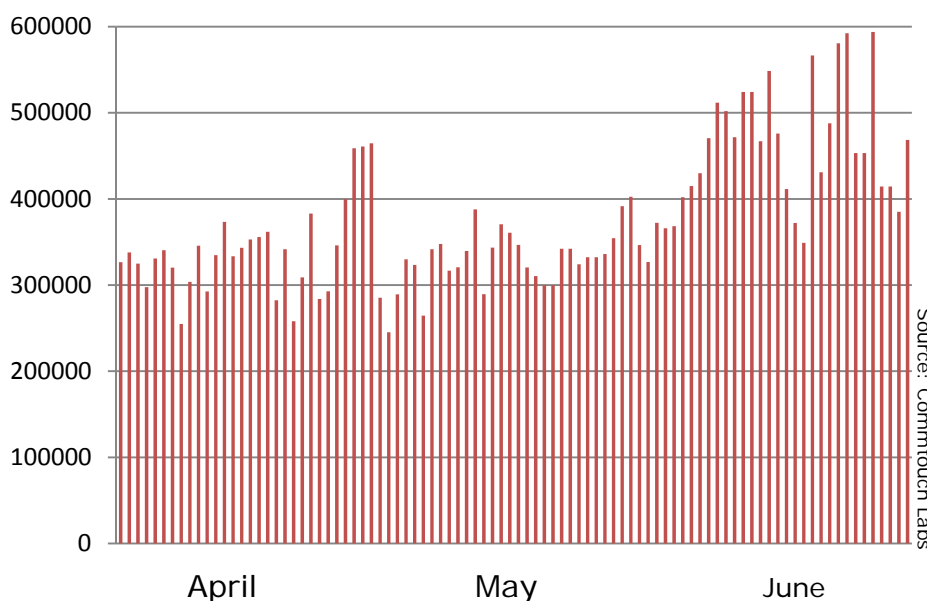


Real Security. In Real Time.

Newly Active Zombies

The lifespan of zombies is very short, and according to Commtouch Labs, the second quarter saw an average turnover of 376,000 zombies each day. The graph below shows the newly active zombies each day throughout the quarter; the increase at the end of May and through June can be attributed to corresponding malware outbreaks.

Q2 2009 Newly Active Zombies



Zombie Hot Spots

The top four zombie-producing domains remained the same as last quarter, with telesp.net.br overtaking tpnet.pl to place in the number one spot.

Brazil continues to produce the most zombies, responsible for 17.5% of global zombie activity according to Commtouch Labs.

Top 10 Zombie Hot Spots – Average Per Day		
Rank	Domain	# Zombies
1	telesp.net.br	30,481
2	veloxzon.com.br	28,401
3	ttnet.net.tr	26,592
4	tpnet.pl	26,443
5	airtelbroadband.in	24,612
6	brasiltelecom.net.br	24,016
7	asianet.co.th	17,565
8	ukrtel.net	14,500
9	telecomitalia.it	13,250
10	verizon.net	8,603

Source: Commtouch Labs



Real Security. In Real Time.

Top Spam Topics

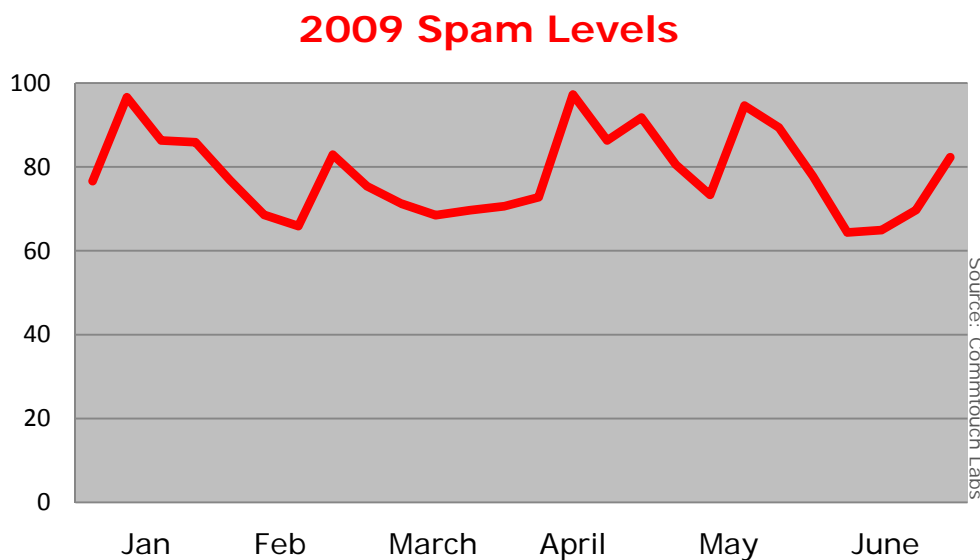
Enhancement spam jumped from 11% of all spam messages in Q1 2009 to first place, with 46.2% of all spam messages this quarter. Last quarter's top spam subject, loans, was not popular this quarter.

Topics of Spam Email Q1 2009			
Enhancers	46.2%	Software	1.3%
Pharmacy	33%	Degrees	0.8%
Replica	10.6%	Other	6.1%
Scams	2%		

Source: Commtouch Labs

Spam Levels

Spam levels averaged 80% of all email traffic throughout the quarter, peaking at 97% in April and bottoming out at 64% in June.

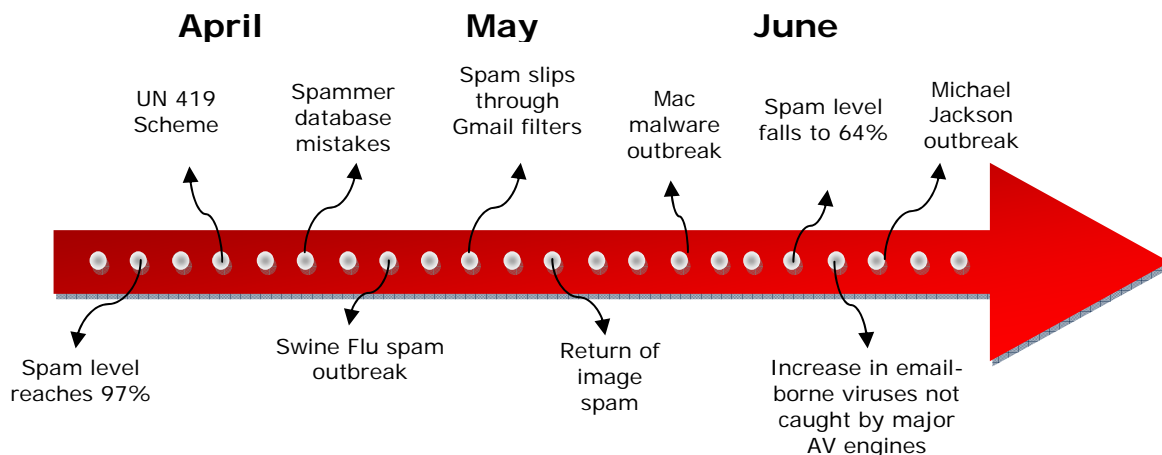


NOTE: Reported global spam levels are based on Internet email traffic as measured from unfiltered data streams, not including internal corporate traffic. Therefore global spam levels will differ from the quantities reaching end user inboxes, due to several possible layers of filtering at the ISP level.



Real Security. In Real Time.

Q2 2009 Outbreaks in Review



About Commtouch

Commtouch® (NASDAQ: CTCH) provides proven messaging and Web security technology to more than 100 security companies and service providers for integration into their solutions. Commtouch's patented Recurrent Pattern Detection™ (RPD™) and GlobalView™ 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 technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures 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 in Sunnyvale, Calif. Stay abreast of the latest messaging and Web threat trends all quarter long at the Commtouch Café: <http://blog.commtouch.com>. For more information about enhancing security offerings with Commtouch technology, see www.commtouch.com or write info@commtouch.com.

About M2 NET

M2 NET S.A. the author and owner of Secure Mail Intelligence!® trademark is a private held joint stock company, provides a range of software and managed services to protect, control, encrypt and archive e-mail communication. Founded in 2000 year M2 NET now becomes one of biggest provider of comprehensive, multi-layer and multi-engine, anti-virus, anti-spam, cryptographic and archiving services in Central European. Currently the software and services created by M2 NET S.A. use more than 500 000 users. Just SMI! is used by more than 350 000 users and dozens of clients ranging from small business to the Fortune 500 located in more than 25 countries."

© Copyright 2009 Commtouch Software Ltd. All Rights Reserved. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.