



Q3 2008 Email Threats Trend Report

Blended Threats Continue to Assail Networks and Inboxes

October 15, 2008

Introduction

Internet users got little reprieve during the third quarter of 2008 as email and web continued to be the avenues of choice for Internet threats. Blended-threat emails, particularly hyperlinks to malicious material hosted on the Internet, have become a leading tactic. Blended-threats have become increasingly popular over the past year, due to their relative success at evading many security solutions. Blended threats that contain an element of “hijacking” legitimate content, sites or senders to provide an air of legitimacy was a significant trend this quarter.

Zombie or botnet-generated threats remained high, however reputation-based solutions are continuously improving at blocking them. As a result, spammers enhanced their tricks for “hijacking” positive reputations from senders and sites, in an attempt to bypass even reputation-based filtering systems.

Q3 2008 Highlights

- Spam levels throughout the third quarter averaged 77%, as in Q2, ranging from a low of 61% to a peak of 94% of all email mid-quarter
- Legitimate sites and senders were used by spammers to cloak their illicit activity, including sites like Live.com
- Over half of zombies/bots change their IP address daily
- Germany has the fastest rate of zombie IP address turnover, at approximately 79% per day; China is a close second at 78% per day
- Malware masqueraded as legitimate newsletters such as CNN Daily Top 10 or IE7 Browser updates
- New spam tactics during the quarter included: links to Flash (.swf) files, ASCII art spam, and hidden Bayesian poisoning text combined with HTML tricks



Spammers Cloak Their Reputation

A major trend throughout 2008 that intensified during the third quarter is spammers' increased use of cloaking techniques to hide their poor reputation behind someone else's good reputation. This means that instead of sending email from a known spam IP address or – more commonly – from an infected bot server, spammers are finding new ways to send messages using valid or known mail servers, mainly webmail accounts, which have a reputation as a legitimate email source. Spammers have been forced to adopt these techniques due to the constantly improving filtering tactics used to thwart them. These anti-spam tactics include:

- Stricter implementation of filtering policies by service providers,
- Greater adoption by service providers and enterprises of authentication standards such as DKIM and SPF,
- More widespread use of reputation services that check senders' reputation at the connection level before allowing an email connection to be initiated.

These email blocking maneuvers make it much more difficult for spammers to penetrate their messages into organizations, and has forced them to come up with more creative infiltration methods, including hijacking good reputation to camouflage their own poor reputation.

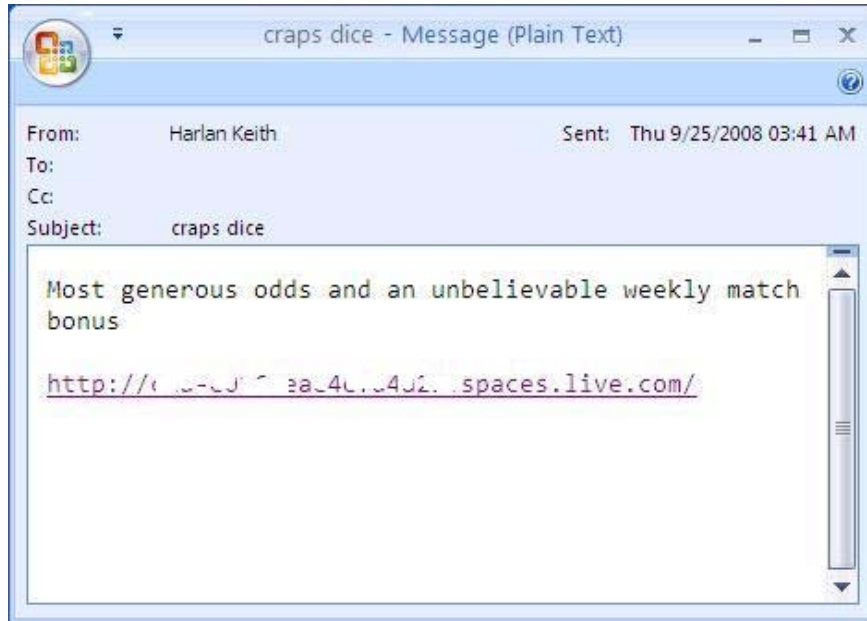
There are several methods spammers use to hijack good reputation, in order to make use of it to deliver their unwanted mail:

- Spammers sign up for thousands of free email accounts, through the use of compromised CAPTCHAs. CAPTCHAs (short for Completely Automated Public Turing test to tell Computers and Humans Apart) are word images used to ensure that a human being is filling out a registration form, as opposed to a machine. Algorithms to break CAPTCHAs are readily available to purchase for illicit use, enabling spammers to generate a nearly unlimited supply of free email accounts from which to send their messages, without intervention.
- In order to gain access to legitimate email accounts without registering them themselves, widespread phishing attacks can persuade enough unwary users to provide their legitimate credentials to criminals. The extensive outbreaks of this sort to the student populations at various universities were described in the second quarter 2008 trend report.
- Spammers often use legitimate hosting sites to host their illegitimate content. They can also create multiple redirection pages on these sites using compromised CAPTCHAs. Sites put in this awkward position recently include: live.com, tripod.com, and photoshosting.com.

Below is a sample email from an outbreak late in the third quarter that took advantage of Microsoft's Live.com site to redirect to a spam casino site.



Sample Blended Threat Message That Hijacked Live.com



Source: Commtouch Labs

Spammer Casino Site Accessed from Redirects from Live.com



Source: Commtouch Labs



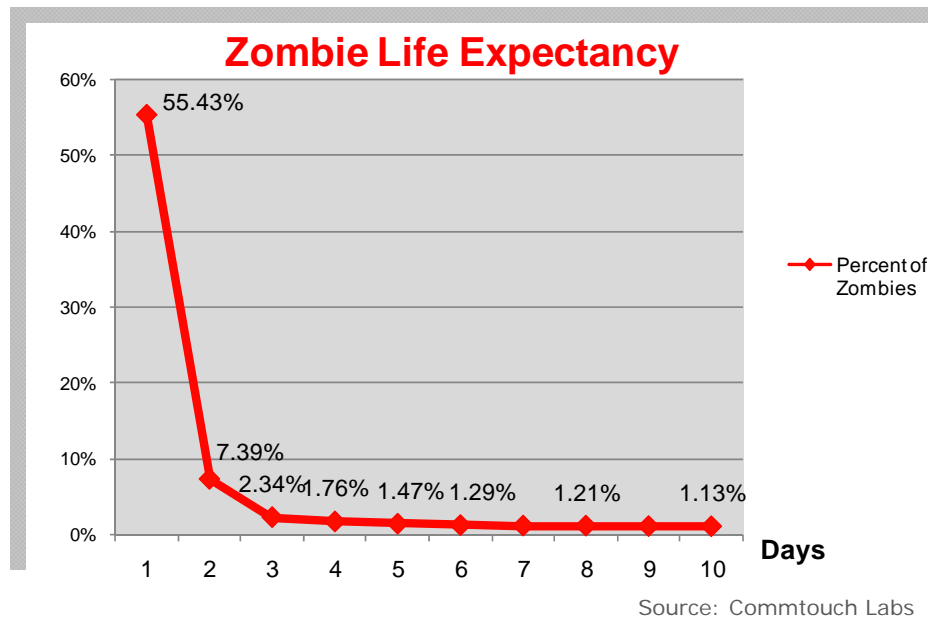
Deeper Insight into Zombie Activity

Zombie/botnet researchers have been studying the size, organization and behavior of botnets for years, but the cunning nature of this enemy has posed many challenges to accurately monitoring and estimating zombie networks. Recent developments at the Commtouch Zombie Lab provide increased granularity and new insights.

Zombie Life Span

During the third quarter, Commtouch labs closely investigated the lifespan of zombies or bots. This research revealed that over 55% of the world's zombies have a lifespan of a single day, when using IP address as the identifier for each zombie. In order to hide their existence from static black lists, zombies are continuously requesting new IP addresses. The graph below shows the distribution of the life expectancy of zombies, demonstrating that any solution that needs to identify or block zombies must be continuously updated in order to maintain its accuracy.

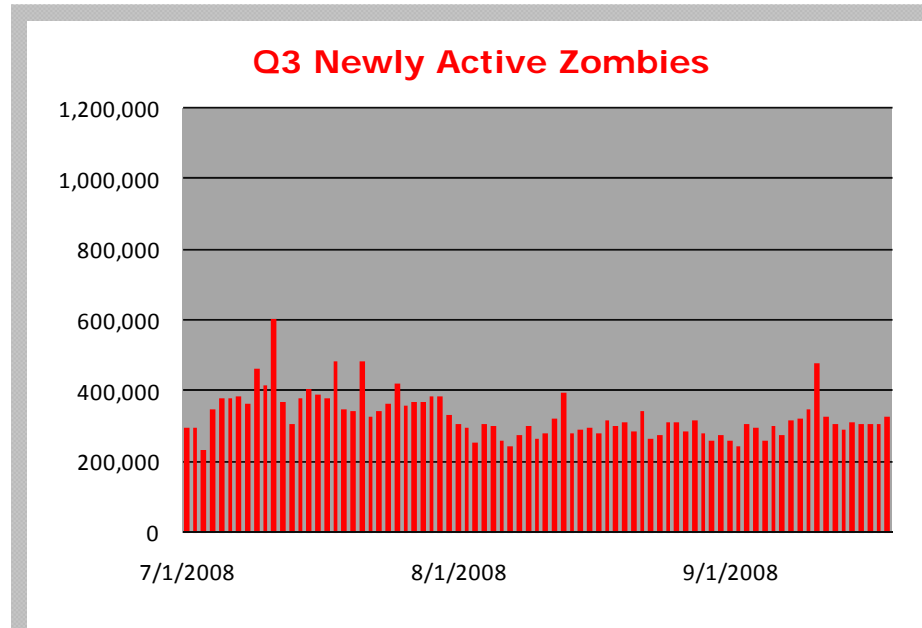
In certain regions the turnover was even faster than that, for example Germany had the fastest rate of zombie IP address turnover, with 79% of daily measured zombies having IP addresses that had not been previously recorded. A close second is China, with 78% zombie daily IP address turnover.





Newly Active Zombies

The lifespan of zombies is very short, and according to Commtouch Labs, there is a turnover of around 330,000 zombies that are newly activated each day. The graph below shows the *newly* active zombies each day throughout the quarter.



Source: Commtouch Labs

Zombie Hot Spots

There is consistency among the top seven ranked domains by number of zombies or botnets – the same domains that are ranked numbers one through seven also appeared on last quarter’s top ten list, although there was some shuffling within the ranks. The newly added domains to the top ten are:

- mtu-net.ru
- ukrstel.net
- airtelbroadband.in

Those that slipped below the top ten ranking among zombie hot spots at the time of this report include:

- brasildtelecom.net.br
- speedy.net.pe
- etb.net.co.

Top 10 Zombie Hot Spots – Average Per Day

Rank	Domain	# Zombies
1	ttnet.net.tr	61,596
2	tpnet.pl	35,565
3	telecomitalia.it	32,509
4	asianet.co.th	28,947
5	163data.com.cn	22,342
6	telesp.net.br	19,379
7	verizon.net	17,918
8	mtu-net.ru	17,815
9	ukrstel.net	16,505
10	airtelbroadband.in	15,998

Source: Commtouch Labs



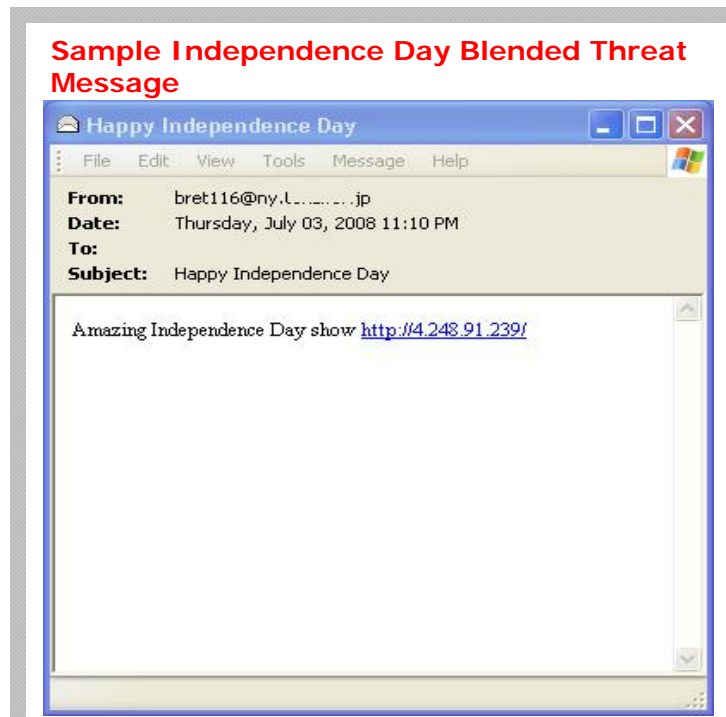
Blended Threats Take Hold Hijacked Elements a Main Theme

During the past year, the tactic of combining more than one method of delivering malicious content has become increasingly prevalent, and those containing hijacked legitimate elements even more popular. In 2007, a stock pump-and-dump spam message was mass-distributed when the spammers hijacked a legitimate HTML newsletter that included web-hosted images and inserted their spam image into the code. The HTML code was so similar to the legitimate version that the message slipped past many anti-spam solutions and the spam image was served. The widespread 'success' of this campaign seems to have sparked a quickly growing trend among spammers and malware writers to host their malicious content elsewhere and simply include a link to it in the body of the email message.

Blended-threat email outbreaks often use the same old social engineering tactics to lure in unsuspecting end-users. Current affairs, celebrities and holidays are often used to create appealing Subject lines that tempt people to open an unsolicited email and even click on dodgy links inside the message body.

Email Delivers Fireworks for July 4th

As the US was getting in the mood to celebrate its Independence Day on July 4th, spammers took the opportunity to pounce and distributed a glut of malicious messages with a July 4th theme. Subjects like 'Happy Independence Day' and 'Happy July 4th' and inside promised spectacular fireworks displays if you just click on the link. Of course, innocent users were surprised when the link downloaded malware to their computer.



Source: Commtouch Labs



Promise of Gruesome Video Delivers Ghastly Code

In late July a massive blended threat attack used the promise of gruesome videos featuring shocking acts of bodily mutilation and human cruelty. Macabre subject lines did the trick, causing users to open the email message. Sample subject lines:

- snake caught swallowing horse
- boy pokes fork into sister's eye
- boy 4, pulls off sister's ear
- man breaks arm in horror fall
- horses breaks riders skull in freak attack
- raw footage of snake swallowing horse
- kids rob elderly, police open fire
- woman loses foot in shock attack
- horse kicks harrison ford in stomach
- woman loses nose after dog attack
- police open fire on elderly in iowa
- man loses eye in fight

Inside the message was a hyperlink to a web page in the format 'http://.....viewmovie.html' that contained malware. Security solutions with a web component should be able to identify and block links to malicious web content. The trick with this type of blended-threat is that the malware writers hacked legitimate websites and hosted their malicious code there, so many web security utilities were not able to identify one hacked page buried deep within an otherwise legitimate website. Again valid content was hijacked to penetrate traditional email defenses.

Today, blended-threats have become one of the most popular techniques for spam and malware distribution. Presumably, this is because they are still managing to get past common defense solutions. The web component of blended-threat emails poses the biggest challenge, since often times malicious content is hosted either on legitimate sites that have been hacked or on popular public platforms like Blogspot or Flickr. This means that in order to effectively defend against the web-hosted component of the threat, solutions must be able to identify individual URLs with great accuracy.



Camouflage and Cover-Ups

Anti-spam solutions are now very proficient at detecting obvious junk email, so spammers have to invent tricky methods of making their email messages appear legitimate to the very defenses meant to block them.

CNN camouflage

One technique is to camouflage messages to look like popular and legitimate email newsletters. In August, spammers produced a series of convincing counterfeit 'CNN Daily Top 10' headlines newsletters. The email messages were very accurate replicas of the real thing, especially because they served many of the images from the same source as the legitimate CNN newsletters. Clicking on any of the headline links led readers to an automatic download of a malware file called "get_flash_update.exe".





IE7 update cover-up

Another way email-borne malware is disguised is to dress it up like popular system update emails. In an ironic twist, users' desire to defend themselves against web-based threats is turned against them. In this case the email is designed to look like a notification of an update to the popular IE7 web browser. The 'From' address was spoofed to look like a bona fide 'admin@microsoft.com' email address and the disclaimer text at the bottom of the message was taken directly from a real Microsoft message.



Source: Commtouch Labs

These simple tactics give the message a benign appearance and help it to get past both email security solutions and users' suspicions. Users who did click on the link were hit with a nasty executable file.



Doomsday headlines lure users into malware trap

The exploitation of topical current events is a tried and true social engineering tactic. In early July the Storm worm perpetrators used the ongoing nuclear tensions between the US and Iran to spread yet another round of this ever-morphing malware. Subjects claimed that the US had attacked Iran and the email messages featured pictures of huge explosions allegedly from the scene. The payload was a variation of the Storm worm in the form of an executable file called 'iran_occupation.exe'

Website that automatically downloads Storm Worm in the form of "iran_occupation.exe"



Just now US Army's Delta Force and U.S. Air Force have invaded Iran. Approximately 20000 soldiers crossed the border into Iran and broke down the Iran's Army resistance. The video made by US soldier was received to day morning. [Click on the video](#) to see first minutes of the beginning of the World War III. God save us.

Source: Commtouch Labs



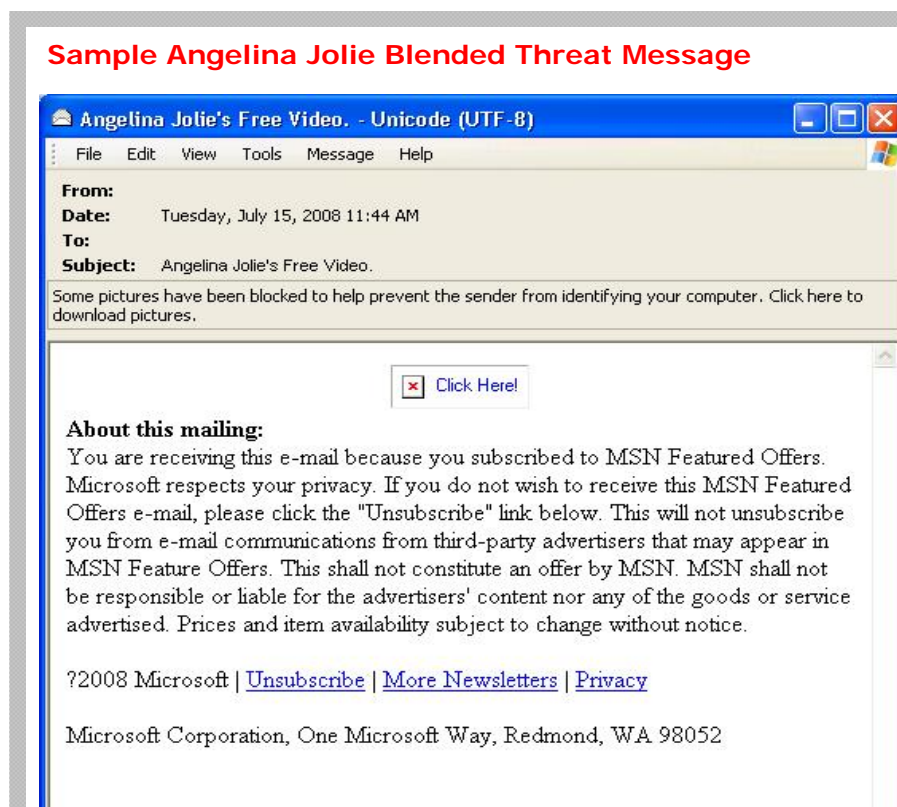
Peeping Toms pay the price

Popular obsession with candid celebrity images aided the spread of more email-borne malware in Q3 as virus writers cashed in on the public's insatiable appetite for risqué images of beautiful movie stars.

An outbreak in mid-July used the celebrity appeal of the actress Angelina Jolie to sting curious users with a nasty virus. Emails were distributed that promised 'Angelina Jolie's Free Video.'

The link inside leads to an executable file that is a lot less appealing. This particular outbreak is remarkably similar to earlier instant messenger messages that also featured a link to an executable file.

Note also the Microsoft system text at the bottom of the message that was "hijacked" to give the message an air of legitimacy with automated email filters.

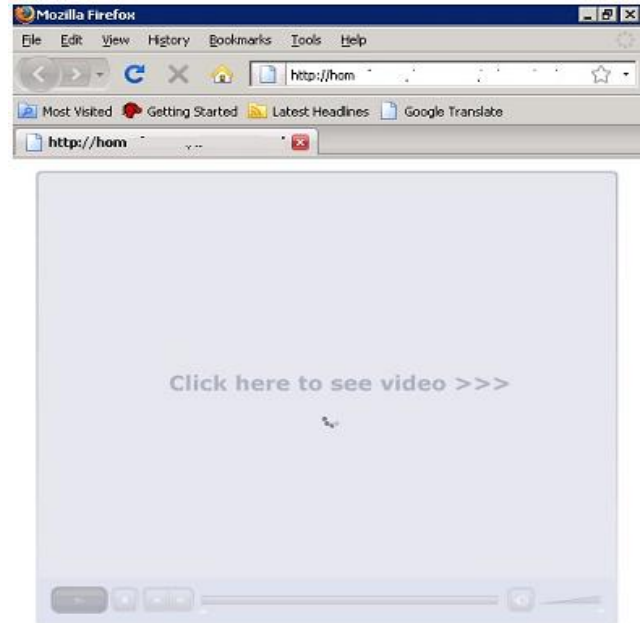


Source: Commtouch Labs



A similar outbreak promised pictures of actress Demi Moore, but instead delivered a blended-threat via an email that included a hyperlink to a fake movie site to view an MP4 of the movie star.

Sample Demi Moore Blended Threat Message and the web site to which it links



Source: Commtouch Labs

The Endless Storm

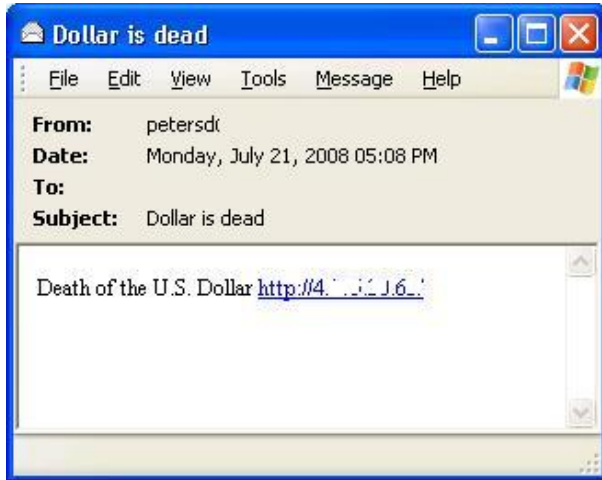
Perpetually morphing into slightly altered forms, the Storm worm continues to be distributed in various email outbreaks. One recent iteration was a scam based on an urban legend that North American countries will soon be adopting a single currency called the 'Amero'. Sample Subjects included:

- Dollar is dead
- No more dollars anymore
- Amero arrives

Those who clicked on the link inside the message were hit with an automatic download of the amero.exe malware (a form of Storm worm, aka Tibs, Nuwar, or Zhelatin). Bear in mind that even though "Storm" keeps re-appearing, each time its form is altered just enough to avoid being detected by many signatures and heuristic rules designed to catch the previous outbreak.



Sample Amero blended threat message and the web site to which it links



Source: Commtouch Labs

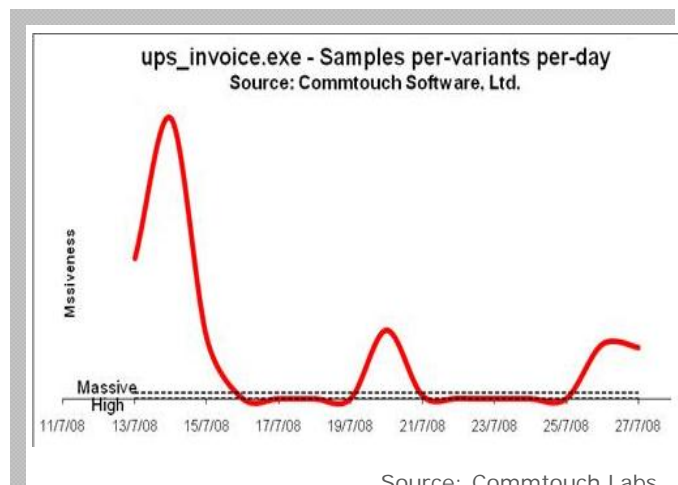
Love is another theme that has shown real staying power in the realm of email-borne threats. Yet another round of amorously themed emails delivered nothing but heartbreak for those poor souls who clicked on the link and downloaded the 'postcard.exe' file. As dull and repetitive as these attacks may seem, they continue to spread the Tibs/Nuwar/Zhelatin (aka Storm Worm) malware and infect new computers.

Attachment Malware: Not Dead Yet

While blended threats were the vast majority of email-borne malware tactics, malware continued to be distributed by more traditional means -- as email attachments -- throughout the quarter.

UPS email delivers malicious attachment

The "UPS" malware was a traditional outbreak of email messages with malicious code attachment. The outbreak was detected by Commtouch when it began on July 13, with a rash of text-based messages claiming not to be able to deliver a package. The recipient was instructed to open the email and reconcile the delivery issue, but instead received a malware surprise. The outbreak came in short, massive waves or bursts. The graph shown here displays the number of samples per variants per day of ups_invoice.exe, the malware attached in those messages.



Source: Commtouch Labs



New Spam Tricks

Unfortunately, junk email messages still constitute the majority of email messages sent across the Internet, and spammers are always trying to invent new tricks to get around traditional content based anti-spam filters.

Flash in the spam

In Q3, the use of web-hosted Macromedia Flash files was a new technique initiated by spammers to bypass traditional email filters. This popular web animation format is normally built into a regular web page and programmed to run when the page opens. So most Flash-containing web pages have regular file extension endings (.html or .asp). In this case the spammers linked directly to a hosted Flash file (.swf) that turned out to be a re-direct to a page of pharmaceutical spam content. To make detection even more difficult, the .swf file was hosted on a free image hosting site, again, hijacking the reputation of a legitimate site. Therefore any engine that attempted to block the offending website would also cause a massive amount of false positives, by blocking access to a popular web tool.

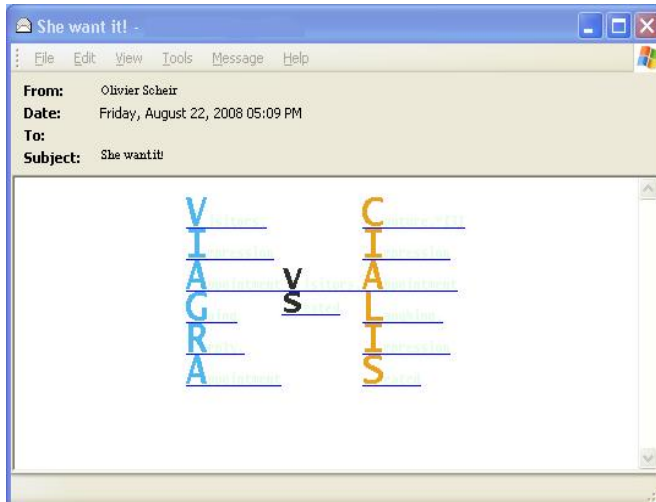
Invisible text hides Bayesian poison

Spammers have been using simple HTML tricks to evade detection for a long time, but in late August they came up with an amusing combination. The pharmaceutical spam message sample below includes the phrase "VIAGRA vs. CIALIS", written in vertical letters to try to avoid detection by content-based engines. But this email has a hidden twist. If you highlight the whole message, a series of common words is revealed. The spammer simply wrote the rest of the letters in white fonts so that it would not be apparent to the reader.

The hidden words were specially chosen because they appear very often in genuine email correspondence, a technique known as Bayesian poisoning that makes the message look even more valid to anti-spam filters that look for statistically suspicious text.



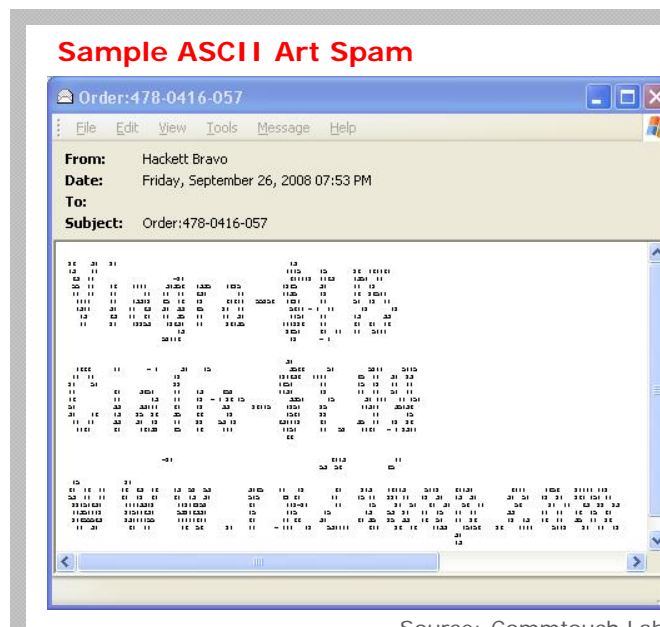
Bayesian Poetry in Vertical Spam Message



Source: Commtouch Labs

ASCII Art Spam

Another technique spammers used to bypass filters was resorting to ASCII art, that is, using random characters to put together a large-scale message such as the one pictured here:



Source: Commtouch Labs

Spammers experimented with this technique in August, then unleashed widespread outbreaks during September.



Top Spam Topics

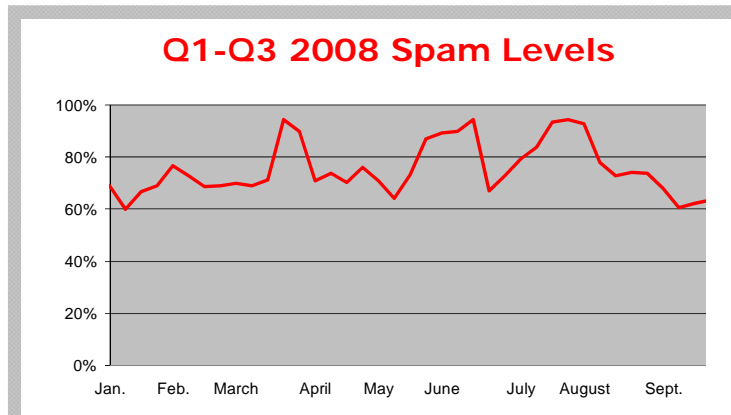
Pharmaceutical spam dropped to 19% of all spam, compared to the previous quarter, where it was the number one topic comprising 46% of all spam throughout the quarter. Sexual enhancers were back in the number one slot, comprising 23% of all spam.

Topics of Spam Email Q3 2008	
Sexual Enhancers – 23%	Jobs/Academic Degrees – 3%
Pharmacy – 19%	Stocks – 1%
Loans – 12%	Casino – 1%
Replicas – 10%	Phishing – <1%
Pornography – 8%	Other – 17%
Software – 4%	

Source: Commtouch Labs

Spam Levels

Spam levels averaged 77% of all email traffic throughout the quarter and peaked at 94% in July.



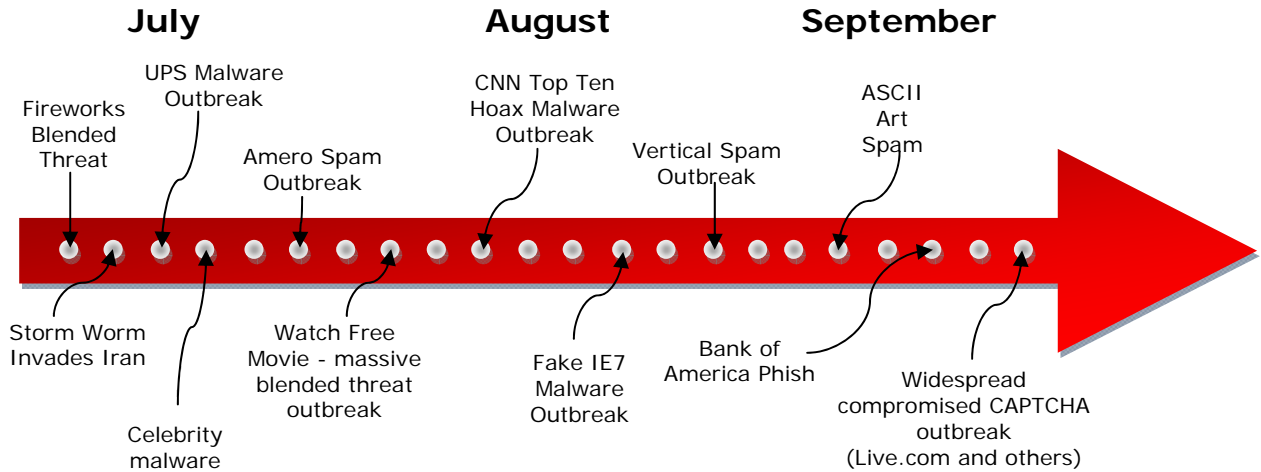
Source: Commtouch Labs

Conclusion

Unsolicited email messages are being promulgated across the Internet at startling rates and the threats contained within them are becoming more and more malicious. Email-borne malware can deliver both viruses and spam in one email, often turning the recipient's PC into a zombie at the same time. Blended-threat messages use multiple avenues to avoid detection, including hijacking legitimate content, sites and senders, in order to increase penetration rates. The mounting use of the web to deliver malicious content embedded within emails means that now highly effective web security has become an essential component of all messaging security solutions.



Q3 2008 Outbreaks in Review



About Commtouch

Commtouch® (NASDAQ: CTCH) is the source of proven messaging and web security technology for over 100 security companies and service providers, thousands of organizations and hundreds of millions of users in over 170 countries.

Commtouch's patented Recurrent Pattern Detection™ and GlobalView™ technologies automatically analyze billions of transactions weekly to identify new spam, malware and zombie outbreaks as they are initiated. Because RPD™ technology does not rely on any content-filters, it is equally effective for all languages and formats, including those with hijacked legitimate content, senders or web sites; it can identify outbreaks of any content- or attachment-type, and is highly effective at blocking spam in double-byte languages.

Commtouch is the proud winner of the 2008 Frost & Sullivan European Messaging Security Technology Innovation of the Year Award.

Stay abreast of the latest 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 nospam@commtouch.com.

© Copyright 2008 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.