HALON

commtouch

Real Security. In Real Time.

Q4 2007 Email Threats Trend Report

Zombie Botnets Come of Age

January 8, 2008

In 2007, botnets came of age, developing into sophisticated peer-to-peer networks that dynamically avoid blacklisting and ferociously fight back against anyone who tries to take them down. The most detrimental botnet thus far was seeded by the Storm worm and has been used to send spam, malware, phishing and even perform distributed denial of service (DDoS) attacks. Botnets were responsible for keeping global spam levels high, averaging 80% throughout the year and peaking in early Q4 at 96%. The year ended with another sharp peak due to a series of holiday-themed outbreaks.

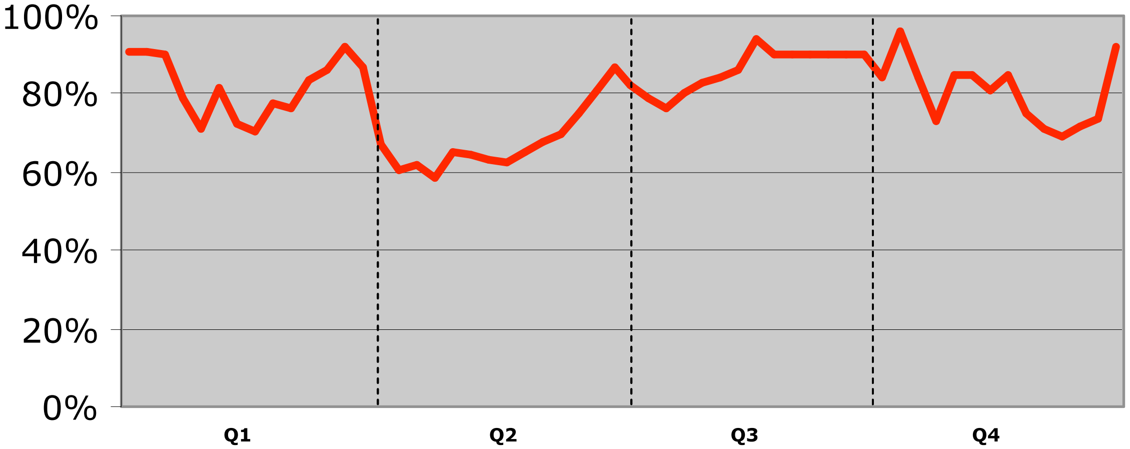
2007 Highlights

- Spam levels reached 96%
- Blended threats combined email, malware and malicious websites
- New types of attachment spam debuted

Q4 2007 Highlights

- MP3 spam outbreak accounted for 7-10% of global spam at peak
- Holiday-related spam and malware outbreaks: Halloween, Thanksgiving, Christmas, New Year’s
- Storm P2P botnet remains an imminent threat
- 70% of spam features sexual enhancers

2007 Global Spam Levels



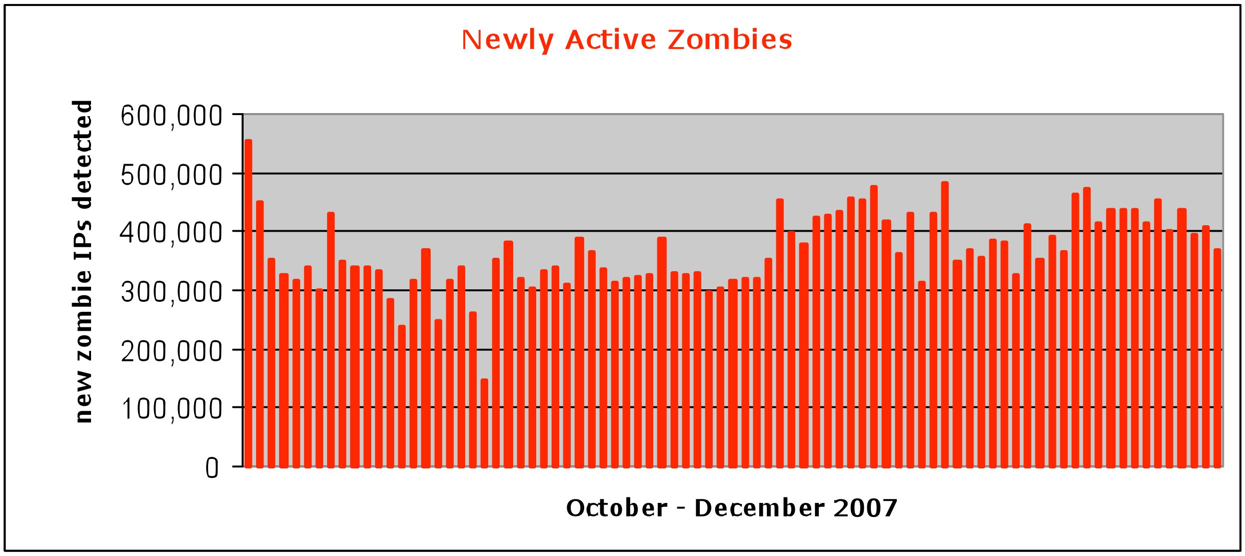
Source: Commtouch Labs

Reported global spam levels are the ratio of 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.

A Storm for all Seasons

Perhaps the most menacing threat, both in the passing year and the one ahead, is the Storm botnet. This network of zombie computers is not only massive, but cunning and aggressive. Its peer-to-peer design allows it the agility to easily outmaneuver real-time blacklists (RBLs) by quickly jumping between seemingly endless networks of dynamic IP addresses.

Storm and other botnets maneuver quickly, activating and deactivating dynamic IPs



Source: Commtouch Labs

Massive propagation, stealth activity

During 2007, the Storm botnet was seeded by the propagation of the Zhelatin/Nuwar malware. The server-side polymorphic malware was very effective at bypassing traditional heuristic and signature-based anti-virus solutions. Most end users are likely unaware that they have been infected, since there are few noticeable symptoms and their computer continues to function as usual. All the while, the Storm botmaster can use the hijacked computing power to generate and send spam and malware, host fraudulent websites and malware, even perform DDoS attacks. This botnet is so nimble and dynamic that researchers are unable to estimate how many infected PCs it contains. Traditional IP blocking technologies such as RBLs are unable to keep pace with the dynamic activation and deactivation of the dynamic IPs.

Storm's Self-preservation

The Storm botnet not only knows how to be prosperous and multiply, it is also incredibly resilient. Its command and control is performed in a peer-to-peer distributed mode and therefore its botmaster cannot be tracked, making it almost impossible to take down. The only effective way to protect against Storm, and other botnets, is to dynamically detect and block activity from the infected machines, based on identifying zombie IP addresses. Storm can also defend itself against organized attempts by security groups to take down the entire botnet by performing DDoS attacks against any group or organization that tries to disarm it.

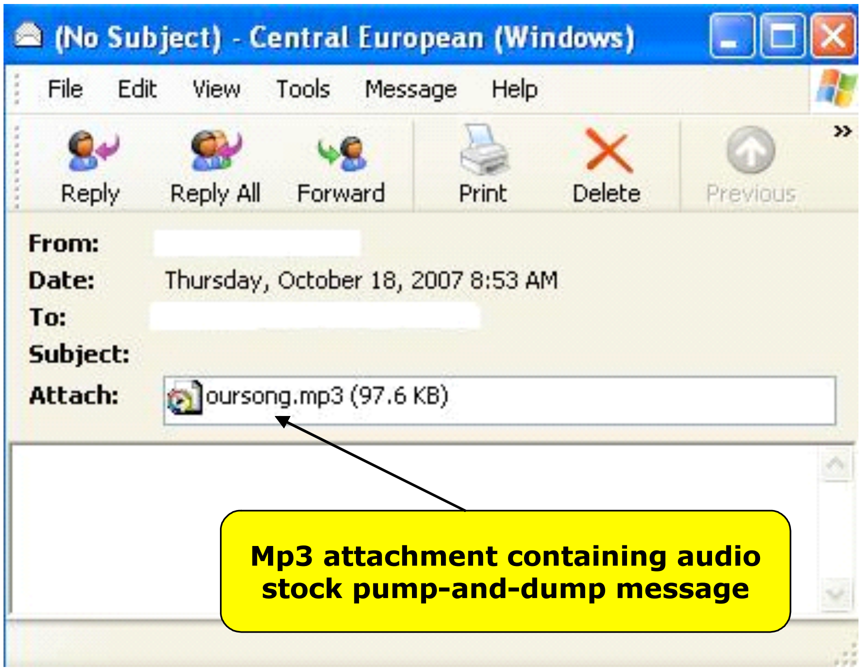
2008: The Perfect Storm?

The Storm botnet was behind much of the spam and malware activity seen in 2007, but this may come to be seen as merely the calm before the Storm compared to what 2008 has yet to bring. Experts agree that it has yet to unleash its full havoc-wreaking potential. The P2P botnet set up by this malware proves resilient to anti-virus and anti-botnet efforts. The most ferocious Storm damage may still lie ahead as the network could be used to perform much more egregious attacks such as massive DDoS and data theft campaigns.

Storm Activity in Q4: MP3 Spam

Throughout 2007, the Storm Botnet was used to generate, host and distribute copious amounts of spam and malware. Among the numerous Storm-powered outbreaks of Q4 was the MP3 spam in which the Storm botnet was used to send a rash of spam messages in October 2007. The email messages contained MP3 attachments with voice messages promoting stocks.

The outbreak was massive, accounting for 7-10% of all global spam traffic at its peak. The email messages themselves were very large, averaging around 85KB. Most of the Subject lines were either empty or innocent "Fwd:" or "Re:", or the name of the file attachment. The MP3 attachment was a randomly machine generated text-to-speech file. The randomization helped the malware evade email filters, but adversely affected the sound quality.



From:
Date: Thursday, October 18, 2007 8:53 AM
To:
Subject:
Attach: oursong.mp3 (97.6 KB)

Mp3 attachment containing audio stock pump-and-dump message

Source: Commtouch Labs

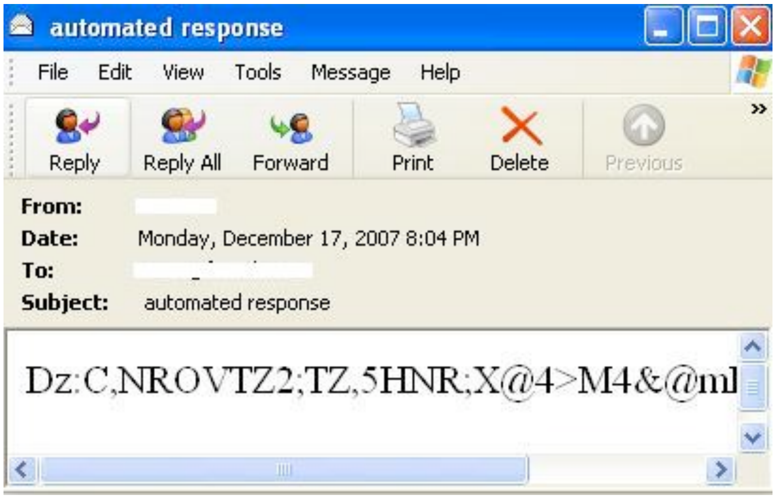
Some security authorities recommended that system administrators block all MP3 attachments in incoming email. They made the argument that this file type is not used for 'legitimate' business purposes and therefore a sweeping anti-MP3 policy would solve the threat without causing any false positives. While MP3 may not be the most popular file format for corporate email users, it is used for legitimate purposes such as recordings of meetings. Therefore relying on an undiscriminating block policy would surely result in some false positives. MP3 spam revealed a blaring weakness in many email defense solutions, the inability to recognize spam without performing some sort of content analysis. Since these solutions were not able to open the file, listen to the message and determine that it was spam, they were unable to detect it at all. This weakness could be exploited in many other popular file formats such as MS Power Point. No system administrator would dare block all email messages with .ppt or .pps attachments.

The answer is not to block by file type, but by spam classification, or virus threat level. Solutions must be able to distinguish between legitimate mail and spam or viruses, regardless of the attachment type.

Address Validation Spam in Q4

A distinct spam strain that trended up towards the end of Q4 2007 is address validation spam. This type of spam usually appears as harmless nonsense or an empty email message sent from an unfamiliar address. Since there is no message or link inside the mail trying to sell phony products or promote junk stocks, the message seems like an innocent mistake or mere garbage and may not even be considered as spam by users. These messages are actually part of botnet owners' efforts to test which email addresses on their distribution lists are legitimate and which are not in use. They mass distribute these empty messages to see if they will go through or be bounced back by the email server. The addresses that are bounced back are considered invalid and removed from the distribution. Then the 'clean' list can be rented out at a higher value to spammers and other cyber villains.

Nonsense messages help validate email



From: [redacted]
Date: Monday, December 17, 2007 8:04 PM
To: [redacted]
Subject: automated response

Dz:C,NROVTZ2;TZ,5HNR;X@4>M4&@ml

Source: Commtouch Labs

Empty address validation messages are a simple yet effective way of bypassing most anti-spam and anti-virus solutions that still rely on analyzing the content of messages to determine whether or not they are malicious. Since these messages contain neither suspicious images or text, nor malicious links or attachments, no content-related basis is found to block them. Only solutions that identify and block the zombie IP addresses used to send the messages are capable of blocking address validation spam, since it will work regardless of message content.

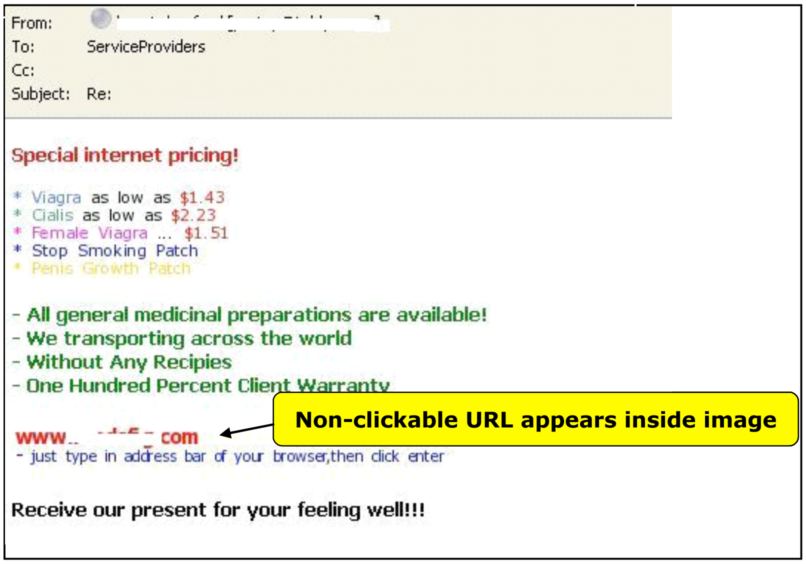
Image-Spam Makes an Encore Appearance

Though the heyday of image-spam outbreaks seems to have passed as other types of spam took their place (e.g. PDF spam which first appeared in July 2007), they made an encore appearance at the tail end of 2007. During December, fresh spam outbreaks featuring images promoting pharmaceutical products and pump-and-dump stock scams were sent.

URLs Appear Inside Images

Often the spam images include a URL that is not clickable, but when typed into a browser leads to the website where featured products may be purchased. This requires that recipients be interested enough in the product to open a web browser and manually type in the URL.

Image-Spam promoting pharmaceuticals



From:
To: ServiceProviders
Cc:
Subject: Re:

Special internet pricing!

* Viagra as low as $1.43
* Cialis as low as $2.23
* Female Viagra ... $1.51
* Stop Smoking Patch
* Penis Growth Patch

- All general medicinal preparations are available!
- We transporting across the world
- Without Any Recipies
- One Hundred Percent Client Warranty

www.. com
- just type in address bar of your browser,then click enter

Receive our present for your feeling well!!!

Non-clickable URL appears inside image

Source: Commtouch Labs

A similar tactic was originally used in stock pump-and-dump spam which also contained no clickable link, just images of the stock ticker symbol. Pump-and-dump did not need a web link, since the goal was to prompt people to buy the stock through their own brokerage firm and artificially drive up the trading price. Now many pharmaceutical image-spam messages also rely on users taking the initiative. The popularity of this social engineering tactic may suggest that there is a genuine interest in purchasing counterfeit drugs or trading stocks based on unofficial tips. More likely, the relative simplicity with which anti-spam engines can block emails that include a clickable hyperlink, may have forced spammers to rely on the more cumbersome tactic.

Holiday-related threats

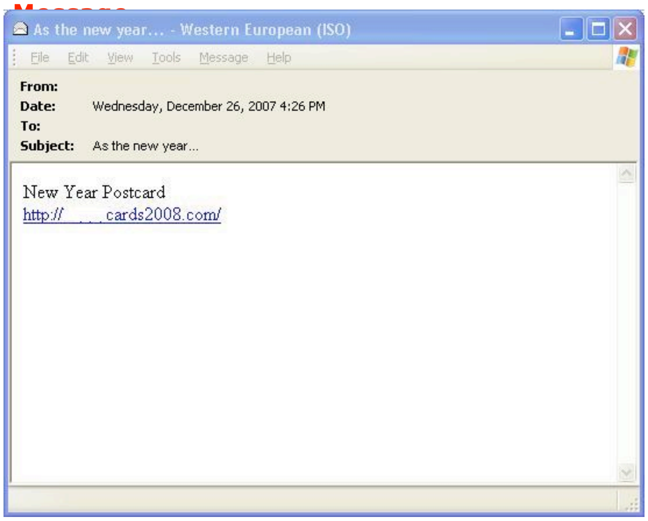
New Year's eCard Malware

The goodwill of the holiday season has been exploited by online scammers who made plentiful use of holiday Subject lines to slip past anti-spam filters and users suspicions alike throughout the quarter. One outbreak at the very end of Q4 blended both holidays and malicious eCards together, just in time for the New Year's Holiday. Samples similar to the screenshot below were first seen in Commtouch Detection Centers on December 25.

Clicking on the link brings the user to a malicious web site that attempts to download Trojan software. Sample Subject lines Commtouch has intercepted include:

- a fresh new year
- as the new year…
- as you embrace another new year
- blasting new year
- happy 2008 to you!
- happy 2008!
- happy new year to [email address]!
- happy new year to you!
- happy new year!
- it's the new year
- joyous new year
- lots of greetings on new year
- message for new year
- new hope and new beginnings…
- new year ecard
- new year postcard
- new year wishes for you
- opportunities for the new year
- wishes for the new year

New Year's eCard Malware Message



From:
Date: Wednesday, December 26, 2007 4:26 PM
To:
Subject: As the new year…

New Year Postcard
http:// . . . cards2008.com/

Source: Commtouch

'Tis the Season to Send Spam

Since many legitimate email messages are sent during this season with holiday related headlines, content filters cannot block these keywords because it would cause unbearable false positives. Once in the end user's inbox, the messages offering easy cash or discounted gifts may actually be more appealing when the holiday shopping rush is in full gear.

Sample Holiday Spam Subject Lines

- (## really fast cash for christmas ##
- ((-----> instant christmas c-a-s-h for as little as $1.00!!
- (cash grant for you! xmas surprise)

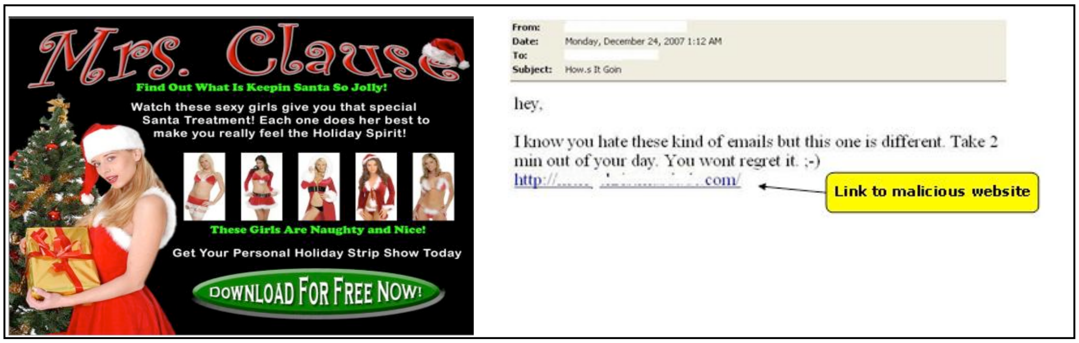
- ... quickmoney ... emergency cash for christmas
- ...[first_name], money for christmas
- what do you want for christmas? how about an easy cash advance?
- (((...........want fast christmas ca$h ???.........)))
- fast money for christmas !
- [skiracing] replicas will be the most memorable gifts this christmas!
- affordable replicas would make perfect gift for christmas!
- maybe stylish replicas are what your folks need this christmas!
- christmas prices for exclusive replicas!
- looking for a better job at christmas time? you may need a degree
- a christmas dream -- getting your degree

Storm Variant Stirs up a Blended-Threat Grinch

The day before Christmas, the Commtouch Detection Center spotted a holiday-themed blended threat email outbreak that enticed recipients to click on a hyperlinked URL within the body of the email message.

The link leads users to a malicious website that automatically attempts to download a new variant of the Storm malware onto the user's PC.

New Variant of Storm Malware Download


Mrs. Clause
Find Out What Is Keepin Santa So Jolly!
Watch these sexy girls give you that special Santa Treatment! Each one does her best to make you really feel the Holiday Spirit!
These Girls Are Naughty and Nice!
Get Your Personal Holiday Strip Show Today
DOWNLOAD FOR FREE NOW!

From:
Date: Monday, December 24, 2007 1:12 AM
To:
Subject: How.s It Goin

hey,

I know you hate these kind of emails but this one is different. Take 2 min out of your day. You wont regret it. ;-)
http://...... ....com/

Link to malicious website

Source: Commtouch

Thanksgiving Spam

In November, as United States Thanksgiving approached, a rash of spam was sent with holiday related Subjects. Once again, cyber criminals took advantage of the holiday spirit and tried to infiltrate the inboxes of users who may have let their guard down a bit.

Sample Thanksgiving spam Subject lines:

- date our sexually explicit singles on thanksgiving weekend
- get the cash you need before thanksgiving
- get your thanksgiving cash now!
- need cash for thanksgiving? try us
- lose those heavy thanksgiving meals
- re: thanksgiving pounds, enjoy our complimentary bottle
- Thank Friends with these Thanksgiving Cards

Halloween Dancing Skeleton Blended Threat

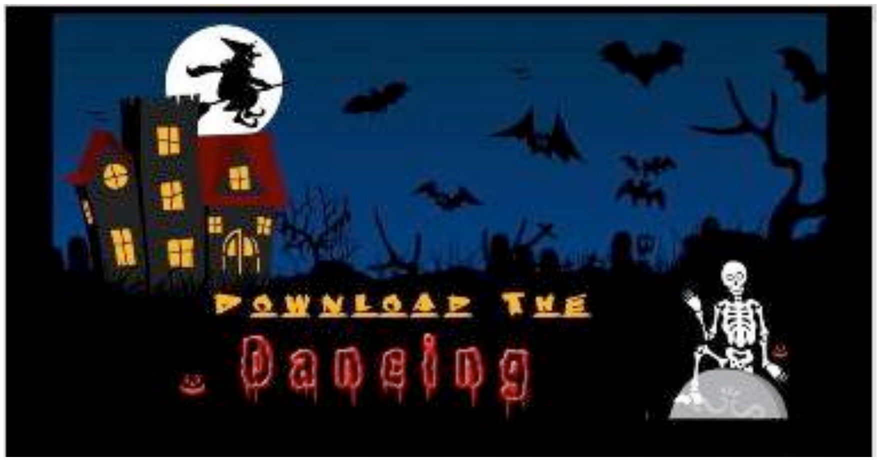
Spammers sunk their fangs into Halloween in October by sending out a barrage of holiday-themed blended-threat messages. The "dancing skeleton" spam attack was distributed in email messages, promising an entertaining Halloween show.

Email Subjects included:

- nothing is funnier this halloween
- show this to the kids
- for people with a sense of humor only
- man this is funny
- dancing bones
- dancing skeleton
- the most amazing dancing skeleton
- watch him dance
- make him dance
- happy halloween

The email messages contained links to malicious web sites. The sites are included in a spam message as an IP address (i.e. http://xxx.xxx.xxx.xxx). When users click through, they are directed to a site that says something along the lines of "Do You Want To See New Funny Sexual Halloween Game with Dancing Skeleton? Just Click Here."

Email links to malicious website that tries to download



Source: Commtouch

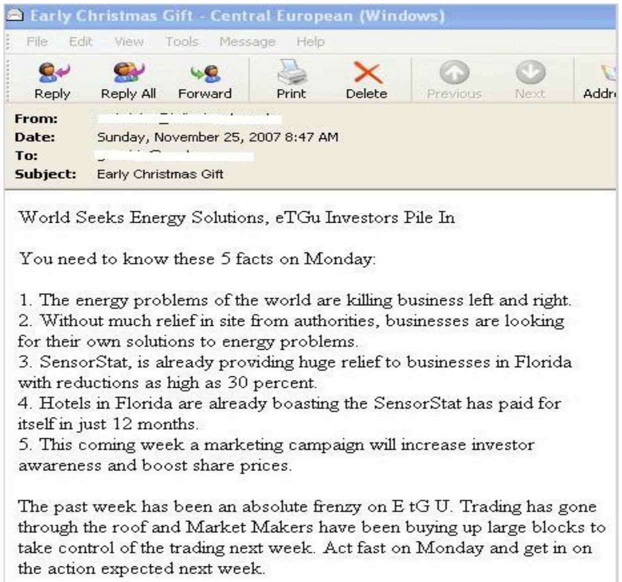
The site tries to automatically download an .mht file (web archive file) which contains malware. This method of distribution is meant to exploit a weakness in the MS Explorer browser which allows automatic downloads. For those using more secure browsers, the website also contains a clickable link to manually download the 'Halloween.exe' malicious code.

Pump-and-Dump Spam Goes Old School

In late November, a pump-and-dump spam, which once pioneered the use of image-spam, went back to basics and sent a plain-old text spam. This kind of low-tech spam can still bypass many content-based filters, since random stock ticker symbols are not typically on the keyword blacklists that these technologies rely on. The Commtouch Detection Center blocked a significant quantity of these spam emails on November 25 and 26.

For the curious out there, here is how the pump-and-dump scam 'performed'. the spam was sent on Sunday and Monday, presumably trying to pump up the price during trading Monday. The graph below is a 2-day slice of a Yahoo! Finance chart for ETGU. It shows the trade volume spiking on Friday. This is likely the spammers buying up the stock at a low price of $0.0004. Then on Monday the price increased to $0.0009 as the gullible started buying based on the spam mail messages.

Holiday Pump & Dump Text Spam


Early Christmas Gift - Central European (Windows)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addr

From: [redacted]
Date: Sunday, November 25, 2007 8:47 AM
To: [redacted]
Subject: Early Christmas Gift

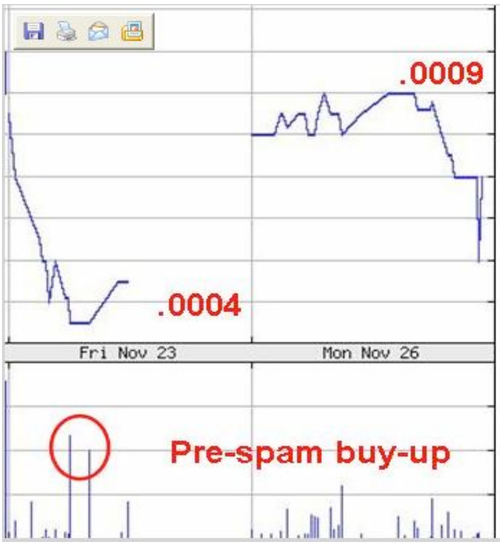
World Seeks Energy Solutions, eTGu Investors Pile In

You need to know these 5 facts on Monday:

1. The energy problems of the world are killing business left and right.
2. Without much relief in site from authorities, businesses are looking for their own solutions to energy problems.
3. SensorStat, is already providing huge relief to businesses in Florida with reductions as high as 30 percent.
4. Hotels in Florida are already boasting the SensorStat has paid for itself in just 12 months.
5. This coming week a marketing campaign will increase investor awareness and boost share prices.

The past week has been an absolute frenzy on E tG U. Trading has gone through the roof and Market Makers have been buying up large blocks to take control of the trading next week. Act fast on Monday and get in on the action expected next week.

Source:
Commtouch



Source: Yahoo!

Surveillance Spam Preys on Guilty Conscience

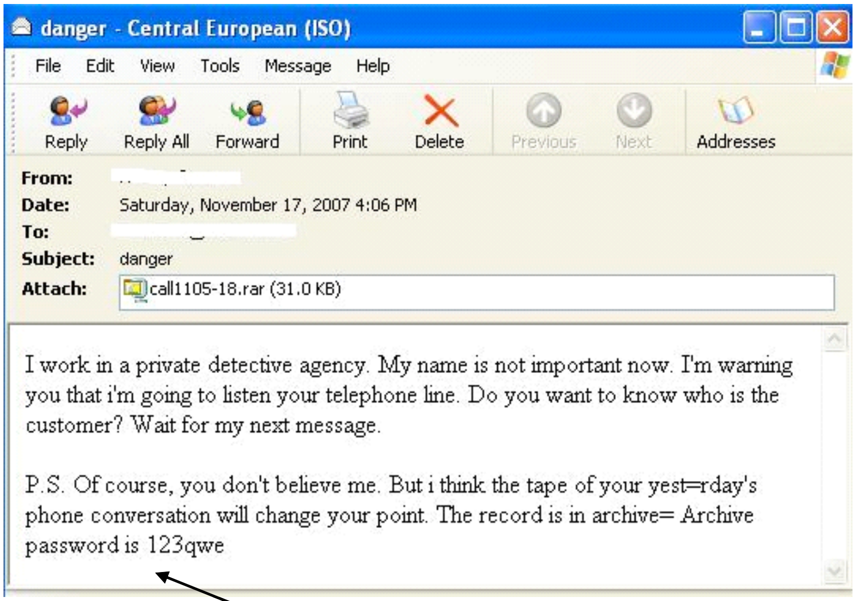
Mid Q4, cyber criminals unleashed an insidious new social engineering tactic that overrides end users' caution with suspicion and fear. The email arrives with subject lines suggesting that the recipient has been under surveillance by a private investigator.

Sample subject lines:

- i'm monitoring you,
- you're being watched,
- your phone is monitored,
- the tape of your conversation.

Upon opening the message, the reader is told that a private investigator has been spying on him and that a copy of a phone call he recorded is in the attached, password-protected compressed file. The message attachment contains malware which appears to be an .mp3 recording, but is in fact an .scr file, an executable type favored by malware writers.

"Surveillance" Malware Outbreak Sample



From: [redacted]
Date: Saturday, November 17, 2007 4:06 PM
To: [redacted]
Subject: danger
Attach: call1105-18.rar (31.0 KB)

I work in a private detective agency. My name is not important now. I'm warning you that i'm going to listen your telephone line. Do you want to know who is the customer? Wait for my next message.

P.S. Of course, you don't believe me. But i think the tape of your yest=rday's phone conversation will change your point. The record is in archive= Archive password is 123qwe

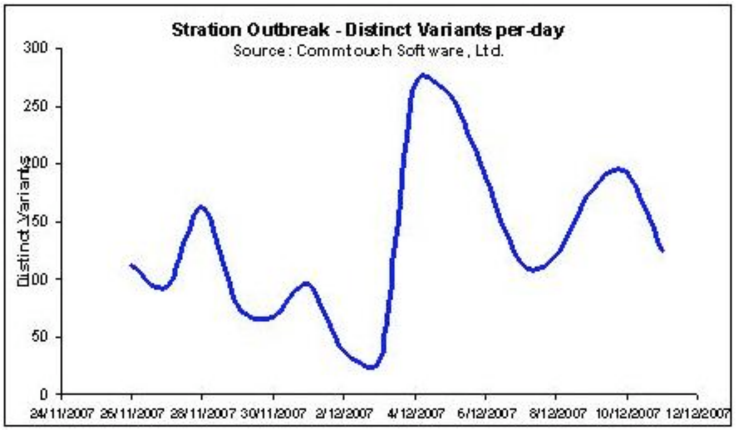
Source: Commtouch

Message contains password to open zip file containing malware

Stration/Warezov Returns

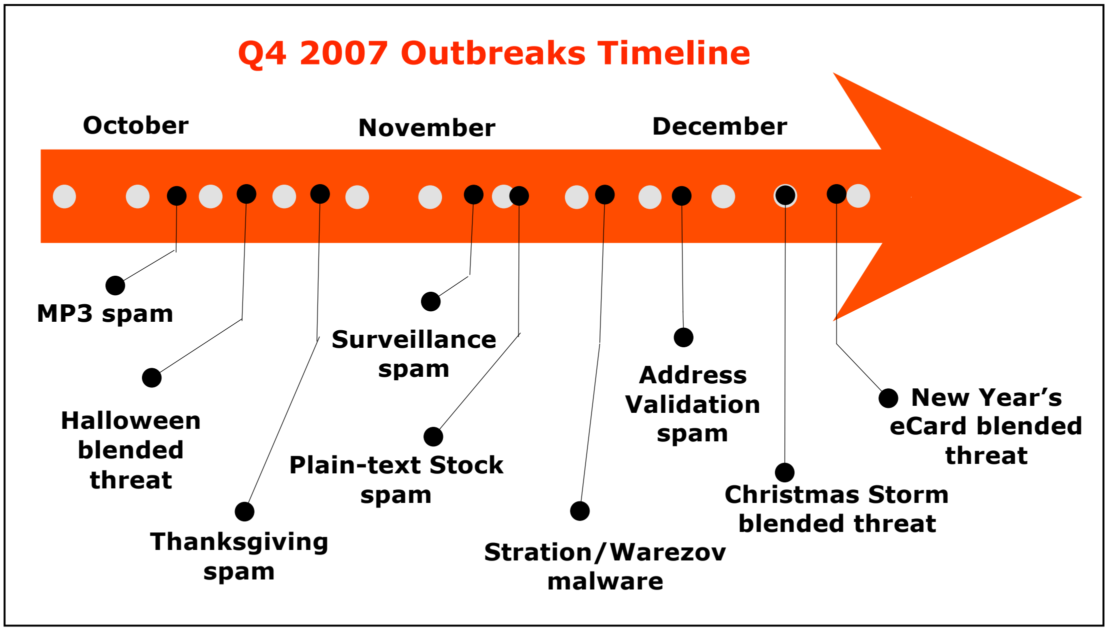
One of the early leading server-side polymorphic malwares, known as Stration/Warezov, reappeared suddenly for a few intense outbreak waves in November and December. The worm remains highly effective against signature- and heuristic-based anti-virus solutions because of its ability to continuously generate multiple characteristics both in the code and carrier email. It tends to attack in short, intense waves to maximize damage in the first few hours before anti-virus signature updates can be released.

Malware Snapshot:
hundreds of new variants released in a single day



Source: Commtouch

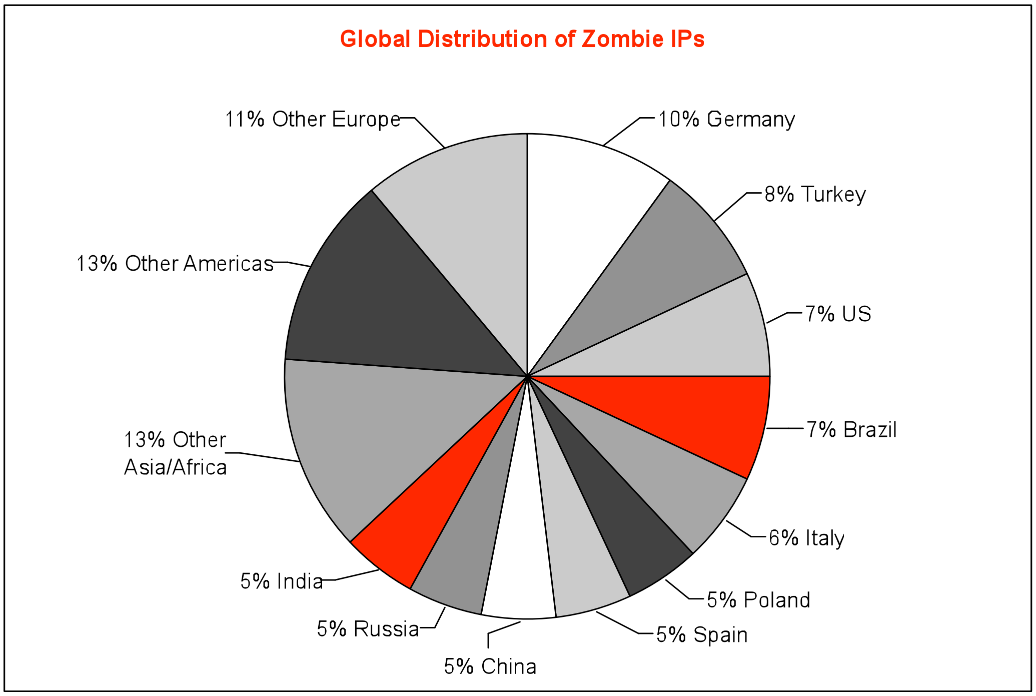
Q4 Outbreaks in Review



Source: Commtouch

Zombie Infections Spread Around the Globe

A snapshot of zombie IPs active on January 1, 2008 shows that botmasters have distributed their malicious networks all around the world. It is precisely this distributed design that allows zombie botnets to dynamically maneuver and avoid traditional IP blocking solutions that are unable to keep pace with the ever changing configurations of dynamic IP addresses.



Source: Commtouch Labs

Most Popular Spam Topics

At the tail end of 2007, spam emails touting sexual enhancement aids took a sweeping lead over all other types of offers. Counterfeit replicas came in second place at 10% of all spam. Replica offers were particularly popular around the holiday gift buying season.

Topics of Spam Email

Sexual Enhancers 70%	Stocks 3%
Replicas 10%	Financial 2%
Software 6%	Pornography 1%
Gambling 4%	Other 4%

Source: Commtouch Labs

Conclusion

In 2007, botnets grew significantly and have become more sophisticated in their operations. These highly distributed networks are capable of performing all types of malicious attacks (spam, malware, phishing, DDoS), and are becoming virtually impossible to take down. Traditional IP blocking technologies such as RBLs are unable to keep pace with the dynamic activation and deactivation of the endless number of dynamic IPs. Only security solutions capable of detecting and classifying malicious activity in real-time are able to provide a barrier against this growing threat.

About Commtouch

Commtouch technology protects against spam and email-borne malware and identifies zombies in real time. Commtouch's Recurrent Pattern Detection™ (RPD) technology protects against spam and malware attacks as they are mass-distributed over the Internet. Commtouch's GlobalView™ technology dynamically blocks unwanted mail at the network perimeter based on the reputation of the sender and identification of zombie traffic, and is capable of offloading over 80% of malicious traffic at the network edge. Together, Commtouch's Anti-Spam, Zero-Hour™ Virus Outbreak Detection and GlobalView Mail Reputation Service deliver three complementary layers of email defense.

Commtouch solutions have been selected by scores of licensing partners, who integrate these services into their security appliances, software gateways, managed services, and client software applications. For more information about enhancing security offerings with Commtouch technology, see www.commtouch.com or write nospam@commtouch.com.

About Halon

About Halon Security Halon Security, headquartered in Gothenburg, Sweden, develops and manufactures IT security products with hardware firewalls as their specialty. Standard with each firewall is BSD, the market's safest operating system. Advanced functionality for antispam and antivirus, Quality of Service, the ability to schedule every services, hardware failure avoidance, and Internet provider switching enables Halon Security firewall users to get maximum IT security and performance. Today, Halon Security's firewalls are available in Europe, Asia, and the Americas. For more information go to: http://www.halonsecurity.com.