commtouch®

Real Security. In Real Time.

Q3 2007 Email Threats Trend Report

Q3 2007 Email Threats Trend Report

Blended Malware Threats, Attachment Spam Increase

October 16, 2007

During the third quarter of 2007, the use of spam to transmit malware became more sophisticated and pervasive. New blended threat techniques paired innocent-appearing spam with links to malicious web sites. Spammers disguised their messages by introducing new types of attachment spam such as PDF spam and Excel spam, while decreasing significantly their use of image spam. Other experimental techniques came into play, such as utilizing traditional phishing methods to entice malware downloads.

Q3 2007 Highlights

- Global spam reaches all-time high: 95% of all emails
- Spam messages with links to malicious URLs up to 8% of all global email traffic during attack peaks
- Over 11,000 dynamic zombie IP addresses hosted malware web sites for one attack. Leading zombie locations were the United States (36%) and Russia (8%)
- Image spam has declined to less than 5% of all spam, down from 30% in the previous quarter
- PDF Spam was 10-15% of all spam in early July, then dropped significantly; now PDF spam is 3-5% of all spam messages
- Pharmaceuticals and sexual enhancers were the most popular spam topics, at 30% and 23% respectively

The common thread to all of these activities is the utilization of vast zombie botnets; these immense networks of compromised computers are used to launch the blended spam/malware attacks, to host malware web sites, and to generate and distribute the various forms of attachment spam. Zombies, spam and malware are becoming inescapably intertwined.

Blended Spam with Malware Web Site Links

Overview

Blended spam has become increasingly popular as a vehicle for web-based malware attacks. Zombies send spam messages without the usual virus attachments. Instead, they include text of a URL that hyperlinks to a website containing malicious software. The software may attempt to download automatically, known as a “drive-by” attack, or simply try to entice users to download the malware by clicking on a link.

By hosting the malware on websites, virus writers evade anti-virus defenses and Mail Transfer Agents (MTAs) that screen for suspicious executables within or attached to messages. No virus is attached to the message itself so it appears uninfected.

During an average blended spam attack Commtouch Labs identified 1,500 malicious URLs per hour of the outbreak. During outbreak peaks, the total more than doubled to several thousand URLs identified per hour. At these peaks, blended threat messages accounted for around 8% of all spam/virus traffic.

This attachment-free spam appears harmless and coaxes gullible users to visit a malicious website. For example, the link may appear to be an ecard sent by family and friends. In most cases, the virus is installed automatically by exploiting vulnerabilities in the Internet Explorer browser.

Spam Links to Malware Sites

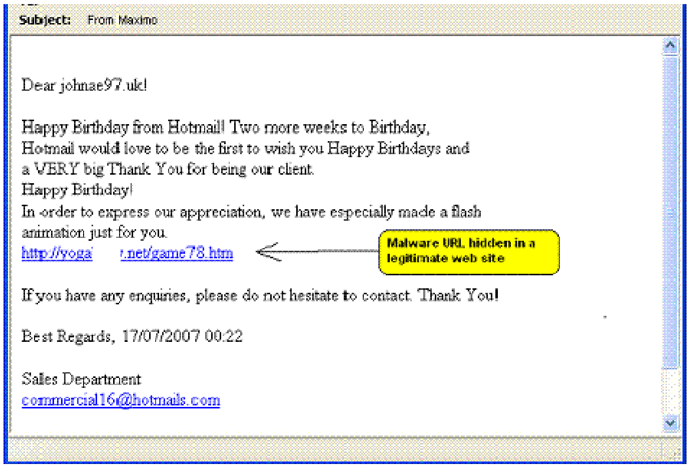
Thousands of malicious URLs per hour during attack peaks. 8% of all unwanted traffic

Malware Embedded in Legitimate Sites

Malware distributors in some cases go to the trouble of embedding their wares in legitimate sites, in order to confuse both the recipients, and their email filters. In order to accomplish this, the malware distributor needs to hack into the legitimate site's web server to place the malware page there. The malware page appears as a single page within an otherwise legitimate domain. If the email filter identifies the site as legitimate, they often will assume that the URL within the site is also legitimate and will allow it through to users' inboxes.

Sample Spam Message with Link to Malware

Appears to be legitimate message with greeting card link



Subject: From Maximo

Dear johnae97.uk!

Happy Birthday from Hotmail! Two more weeks to Birthday,
Hotmail would love to be the first to wish you Happy Birthdays and
a VERY big Thank You for being our client.
Happy Birthday!
In order to express our appreciation, we have especially made a flash
animation just for you.
http://yoga .net/game78.htm

Malware URL hidden in a legitimate web site

If you have any enquiries, please do not hesitate to contact. Thank You!

Best Regards, 17/07/2007 00:22

Sales Department
commercial16@hotmails.com

One of these outbreaks used a different link for every item within the spam message, and each link led to a *different* legitimate site in which the spammer has installed a rogue page.

This tactic is similar to an image spam development Commtouch Labs detected earlier this year. As the anti-spam industry started getting better at filtering spam images, spammers started hacking innocent websites and posting spam images there, mass distributing email with a link to the hosted spam image.

Fun & Games with Blended Spam

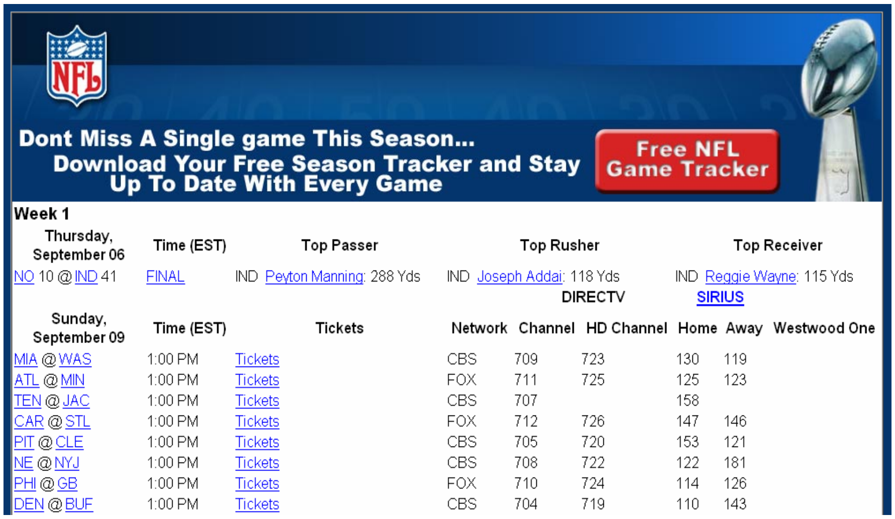
In many cases, these malware sites simply resemble legitimate websites, but are actually forgeries hosted by zombies. Each individual site is online for a matter of hours, such a short time that most traditional IP-address blockers such as Real-Time Black Lists cannot keep up with the pace.

As the National Football League season kicked-off in September, sports fans became a target. Virus writers leveraged blended spam, with messages inviting consumers to download an NFL game-tracker.

The website hyperlinks within the messages used varying IP addresses; during a single hour of the attack, Commtouch identified hundreds of different sites.

The forged NFL website appeared legitimate, resembling an official NFL site complete with logo. It contained links to a “Free NFL Game Tracker” and individual-game ticket sales. However, all links led to a file called tracker.exe – malware, of course.

Sample NFL Spam Message
Invites users to download malware



Dont Miss A Single game This Season...
Download Your Free Season Tracker and Stay Up To Date With Every Game

Week 1

Thursday, September 06	Time (EST)	Top Passer	Top Rusher	Top Receiver
NO 10 @ IND 41	FINAL	IND Peyton Manning: 288 Yds	IND Joseph Addai: 118 Yds	IND Reggie Wayne: 115 Yds

				DIRECTV		SIRIUS		
Sunday, September 09	Time (EST)	Tickets	Network	Channel	HD Channel	Home	Away	Westwood One
MIA @ WAS	1:00 PM	Tickets	CBS	709	723	130	119	
ATL @ MIN	1:00 PM	Tickets	FOX	711	725	125	123	
TEN @ JAC	1:00 PM	Tickets	CBS	707		158		
CAR @ STL	1:00 PM	Tickets	FOX	712	726	147	146	
PIT @ CLE	1:00 PM	Tickets	CBS	705	720	153	121	
NE @ NYJ	1:00 PM	Tickets	CBS	708	722	122	181	
PHI @ GB	1:00 PM	Tickets	FOX	710	724	114	126	
DEN @ BUF	1:00 PM	Tickets	CBS	704	719	110	143	

Another massive attack later in the month inundated users with email messages with subjects like “Wow, Cool Games.” The content of the email messages contained only “Try http://xxx.xxx.xxx.xxx, where the X’s were varying IP addresses.

Country	Sites
United States	36%
Russia	8%
Argentina	5%
Korea	5%
Poland	4%
Great Britain	4%
Romania	4%
India	3%
Denmark	3%
France	2%

Source: Commtouch Labs

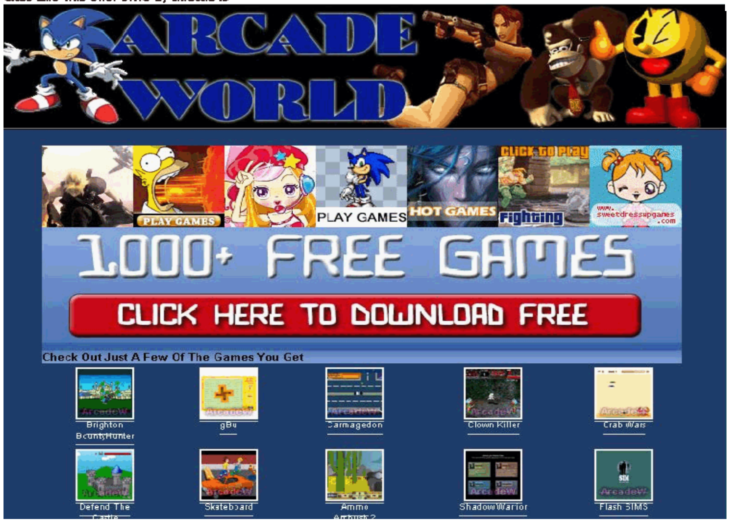
As of mid-September, more than 11,000 separate zombie IPs were hosting the game sites. The top 10 malware site locations were:

The IP addresses used to host these sites are dynamic because they are malware-compromised home computers connected to the Internet via ISPs. The sites stay online for only a matter of hours because spammers and virus writers know that in time most filtering solutions will block messages containing IP addresses known to be malicious.

11,000+ malicious IPs used in a single outbreak

The game sites look remarkably similar to common online games sites, complete with pictures of familiar game heroes such as Sonic the Hedgehog. They are well-designed, look professional, and provide nothing obvious to tip off the user that it's actually a malware site. The attack relies on social engineering to convince users to voluntarily download the virus because it is something useful or fun. The game icons each link to a single executable file designed to download crime ware onto unsuspecting users' computers.

Arcade Game Malware
Sites like this offer infections disguised as games



Standard File Attachments Continue to Penetrate

The use of common file attachments, such as .pdf and .xls was introduced early in the quarter, as they fool many email filtering engines and users alike. Because these types of attachments are commonly used in legitimate email correspondence, any technology that blocks them categorically will cause an unacceptably high number of false positives, i.e. good emails mistakenly blocked. Users are also fooled because these types of attachments do not raise red flags and are assumed to be innocuous. By wrapping the same message in a new format, they bypass most anti-spam engines trying to analyze the content of mail messages. For these reasons the use of common attachment types is expected to continue at least for the near future. Any common file type could be used in the next big outbreak; .pdf, .xls, .ppt, .doc. They can all carry messages or images as well as hyperlinks to URLs, making them an ideal way to get past defenses and reach users.

Like many other types of spam messages, attachment spam is being sent from zombie computers or "bots," typically home PCs that have previously been infected by Trojan malware. Spammers control massive numbers of these bots in vast "botnets" that they rally together to launch global spam and malware outbreaks.

PDF Spam Active Early in Q3 Through Today

Individual spam PDF attacks reached up to 40% of all spam in a single day during one of the earliest outbreaks in the quarter. While PDF spam represented 10-15% of all spam in July, it has since declined to just 3-5% of all spam at the end of Q3. When outbreaks do hit they pose a particularly painful bandwidth problem because these messages are nearly four times bigger than standard spam messages; during the peak of an attack they can increase overall global spam traffic by 30-40%. One outbreak attempted to distribute 14 billion to 21 billion unsolicited PDF messages from zombies around the globe.

Sources of PDF Spam

Country	Sites
United States	24%
Taiwan	14%
China	10%
Russia	4%
167 other countries	48%

Source: Commtouch Labs

PDF Spam

Reached up to 40% of all spam in one day; today represents 3-5% of all spam

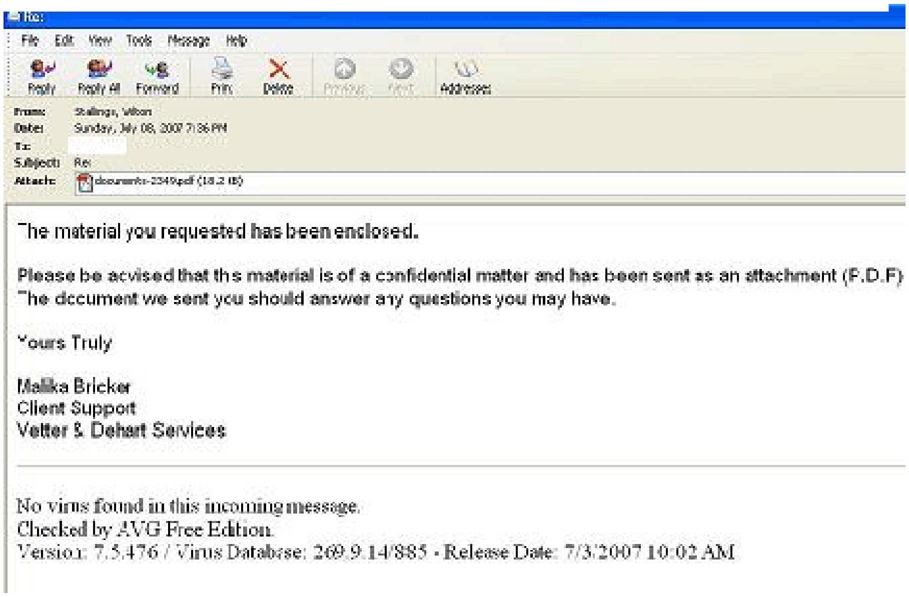
Much of the PDF spam is just a newer incarnation of the old image spam, simply another way of sending visual spam. This simple alteration enabled the messages to penetrate most anti-spam solutions, since many of their heuristics recognize image spam by looking for embedded or attached image files. These heuristics most likely will not catch the same image in .pdf format. Spammers noticed how easy it was to bypass anti-spam engines and have stopped trying to hide their messages with unusual fonts and colors. Instead, they started sending what appeared to be standard business letters in PDF format, but once they are opened, the content revealed is advertising organ enhancers or promoting a pump-and-dump stock.

The popularity of the .pdf format for legitimate business communication makes it difficult for traditional anti-spam solutions to block effectively without causing massive false positives.

Note that in the example below, the spammer added an anti-virus stamp, to increase the appearance of legitimacy of the message.

Spammers Use PDF to Avoid Content Filters

Message itself implies that the PDF was requested and is innocent



From: Stallings, Wilson
Date: Sunday, July 08, 2007 7:36 PM
To:
Subject: Re:
Attach: documents-2349.pdf (18.2 KB)

The material you requested has been enclosed.

Please be advised that this material is of a confidential matter and has been sent as an attachment (P.D.F)
The document we sent you should answer any questions you may have.

Yours Truly

Malika Bricker
Client Support
Vetter & Dehart Services

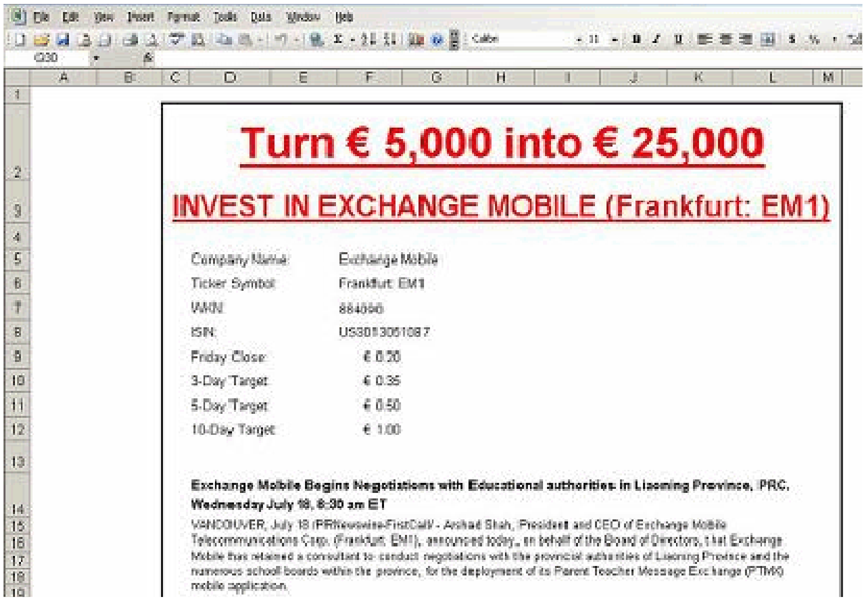
No virus found in this incoming message.
Checked by AVG Free Edition.
Version: 7.5.476 / Virus Database: 269.9.14/885 - Release Date: 7/3/2007 10:02 AM

Excel Spam Experimentation

Excel was a logical progression from the initial spate of PDF spam, which itself was a natural evolution from basic image spam. An early attack of Excel spam promoted stocks in file attachments with names like “invoice20202.xls,” “stock information-3572.xls,” and “requested report.xls.”

Excel Spam Sample

Using Excel is logical choice for stock scams


File Edit View Insert Format Tools Data Window Help
Calibri
11
G30
A B C D E F G H I J K L M
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

Turn € 5,000 into € 25,000

INVEST IN EXCHANGE MOBILE (Frankfurt: EM1)

Company Name:	Exchange Mobile
Ticker Symbol:	Frankfurt: EM1
WKN:	884096
ISIN:	US3013061087
Friday Close:	€ 0.20
3-Day Target:	€ 0.35
5-Day Target:	€ 0.50
10-Day Target:	€ 1.00

Exchange Mobile Begins Negotiations with Educational authorities in Liaoning Province, PRC.
Wednesday July 18, 8:30 am ET

VANCOUVER, July 18 /PRNewswire-FirstCall/ - Arshad Shah, President and CEO of Exchange Mobile Telecommunications Corp. (Frankfurt: EM1), announced today, on behalf of the Board of Directors, that Exchange Mobile has retained a consultant to conduct negotiations with the provincial authorities of Liaoning Province and the numerous school boards within the province, for the deployment of its Parent Teacher Message Exchange (PTMX) mobile application.

Malware writers have used Excel in the past as a carrier for viruses, for example in a series of attacks during June and July 2006 that exploited vulnerabilities in Microsoft software, including Excel, Microsoft Word, and PowerPoint.

Image Spam Outlives its Usefulness

While image spam was a huge nuisance in 2006 and early 2007, it has already become old news. Image spam has been dropping over the past few months due to the increased efficiency of other spammer methods. After earlier peaks in Q1 when image-embedded spam messages constituted as much as 30% of all spam, by the end of Q3 levels had dwindled to less than 5%. These annoying messages have been overtaken by blended threats and PDF spam.

Image Spam

Declined to less than 5% of all spam, compared to 30% in the first quarter of 2007.

Until mid-2007, the main content of image-spam was stock pump-and-dump scams. Today, pornography is the main content for image-based spam, along with pharmaceutical spam, albeit to a lesser extent.

One of the main drawbacks of image spam from the spammers perspective has always been that no hyperlinks could be incorporated into the images. For this reason, stock pump-and-dump (which only pushes people to buy stock, and not to click a link) was a natural fit, and pornography its natural successor. In today’s pornographic image spam, URLs are being embedded into the images. Because of the subject matter, social engineering to induce users to visit the sites is relatively straightforward to implement, even when the links are not clickable.

Other Spam / Malware Experiments

Spammers and malware distributors today face many challenges on their way to reaching users’ inboxes. A variety of commercial email defense solutions are in use, each employing a slightly different technology. Email users themselves have also become much savvier and can often recognize and delete spam and malware messages without even opening them. However, none of this has discouraged the illicit spammers and malware distributors from seeking ill-gotten email profits. They relentlessly engage in experimentation to develop new ways to evade email filtering technology and end users’ defenses.

Phishing Techniques for Malware: Appealing to Familiarity

Leveraging brand names is one technique seen most commonly in phishing, and has lately been used by spammers and malware distributors to initiate consumer action.

YouTube Scam

One threat this quarter took advantage of the popularity of social networking, and used a YouTube teaser to persuade users to download the Storm Worm Trojan. The link appears to be a YouTube viral video link, but it actually links to a rogue web site containing the YouTube logo that asks consumers to download the file. Unprotected Internet Explorer users will have automatic installation.

Phishing Spam Appealing to Your Emotions

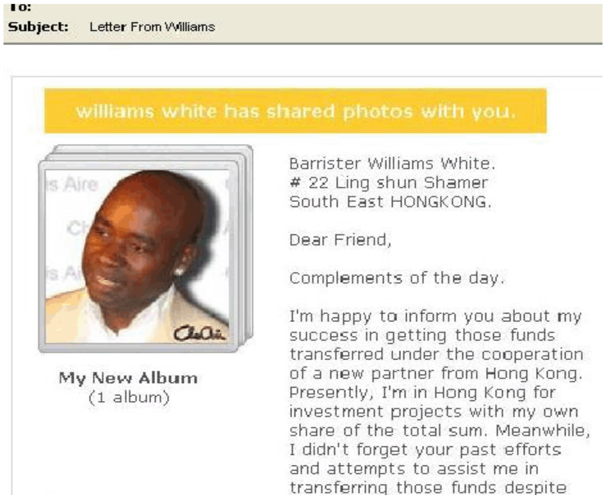
Earlier this quarter, spammers sent an email featuring the seal of the FBI and a photo of the FBI director that claimed to be sent on behalf of American soldiers stationed overseas. This technique is no different than phishers who freely make use of the logos of eBay, Citibank, Bank of America, among others.

Legitimate Site, Illicit Use

Spammers have begun using the ‘send to a friend’ feature commonly available on many websites to mask their identity and slip past security technologies. In the case pictured here, a recent 419 scam (an email message that woos you with free money but ends up stealing yours) was distributed through a photo sharing site, the Kodak EasyShare Gallery. Its an easy way for these scammers to send email without being blocked, since blocking all Kodak EasyShare email messages would lead to vast numbers of false positives.

In order to use these “send-to-a-friend” features, a user must log in and create an email message within the legitimate application. Such a scenario is not scalable for massive outbreaks, but it does suit the small-scale distribution of 419 scams.

Spam from Legitimate Sources
Common mail-distribution sites may be used illicitly



To:
Subject: Letter From Williams

williams white has shared photos with you.

My New Album
(1 album)

Barrister Williams White.
22 Ling shun Shamer
South East HONGKONG.

Dear Friend,

Complements of the day.

I'm happy to inform you about my success in getting those funds transferred under the cooperation of a new partner from Hong Kong. Presently, I'm in Hong Kong for investment projects with my own share of the total sum. Meanwhile, I didn't forget your past efforts and attempts to assist me in transferring those funds despite

Getting it Wrong

Like legitimate direct marketers, sometimes a spammer’s experiment does not provide the results hoped for. Spam can “fail” due to many reasons, the most common is that it is blocked by email filtering engines, however technical difficulties can also play a part in reducing spam’s effectiveness in the eyes of the spammer.

Zip File Attachments

One outbreak in Q3 featured zip files that could not be opened by common zip file utilities. While the specialization of zip software required allowed the messages to bypass some anti-spam content-filters, difficult-to-open attachments decreased the spam response rate considerably.

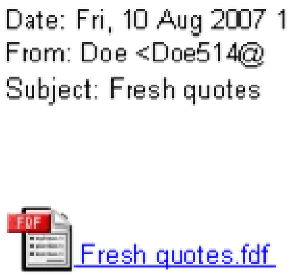
Features of this kind of outbreak included random subject headers such as invitation, alert, notice, unpaid, article, invoice and document with empty message bodies and hard-to-open zip files.

More Experiments

FDF Attachment Spam

Another experiment during this quarter featured FDF (forms data format) files. FDF files are read by Acrobat and other PDF readers. While not especially common, they are a new kind of attack that consumers should be aware of. This particular outbreak of FDF spotted by Commtouch Labs featured stock spam.

Example of FDF Spam
FDF spam is variation of PDF spam



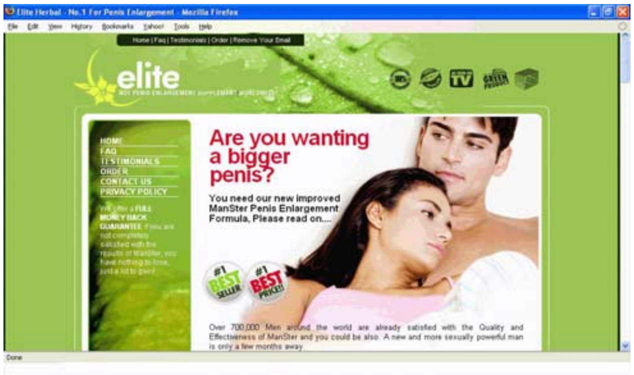
Date: Fri, 10 Aug 2007 16:06 25 +0400
From: Doe <Doe514@ >
Subject: Fresh quotes

Fresh quotes.fdf

New Domain, Old Spam - .mobi sites

The new .mobi domain is being used by spammers. .mobi is the domain intended for sites to be viewed on mobile devices. The .mobi sites are primarily selling replicas (e.g. fake Rolexes). What is most interesting is that the spammers are creating tens of thousands of sub-domains to increase the randomization of the spam messages to try to prevent their messages from being blocked by anti-spam engines.

.mobi Spam Sample
.mobi spam redirects to enhancement websites



Elite Herbal - No.1 For Penis Enlargement - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
Home | Faq | Testimonials | Order | Remove Your Email
elite
HOME
FAQ
TESTIMONIALS
ORDER
CONTACT US
PRIVACY POLICY
#1 BEST SELLER
#1 BEST PRICE!!
TV
Done

Are you wanting a bigger penis?

You need our new improved ManSter Penis Enlargement Formula, Please read on....

We offer a FULL MONEY BACK GUARANTEE if you are not completely satisfied with the results of ManSter, you have nothing to lose, just a lot to gain!

Over 700,000 Men around the world are already satisfied with the Quality and Effectiveness of ManSter and you could be also. A new and more sexually powerful man is only a few months away

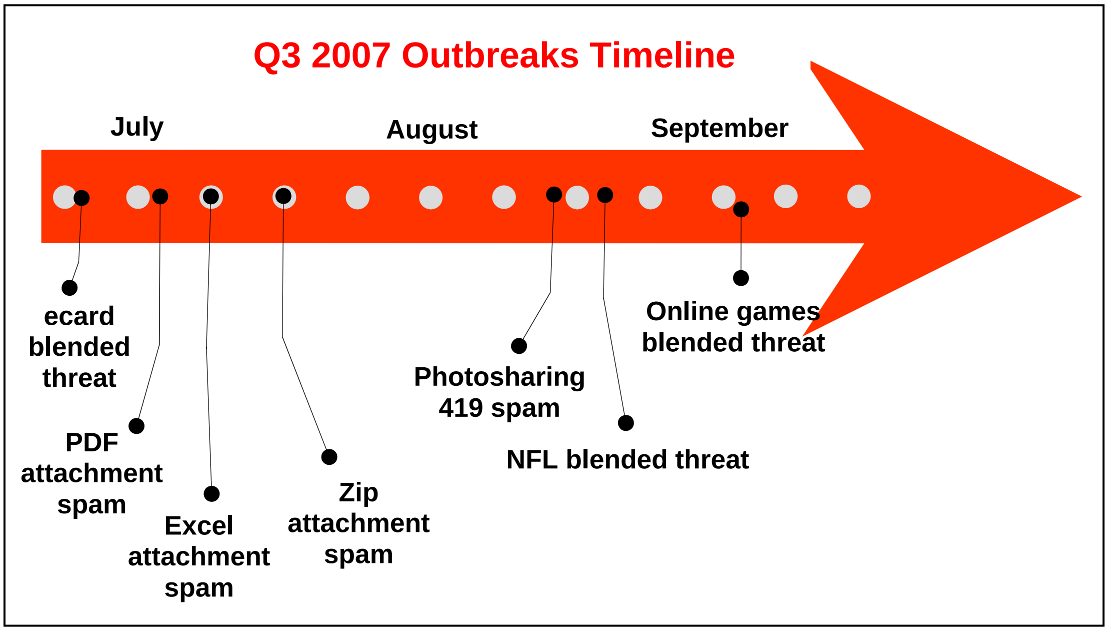
Of the more than 30,000 .mobi sub-domains used during one outbreak, most of the ads were from these three domains: .maloocafe.mobi, .wantbigger.mobi, and .bigisgood.mobi. All three of these .mobi sites led to a sexual enhancement supplement.

Because the spammers want users to view their sites on regular computers and not mobile devices, these .mobi URLs redirect to a standard web site. It's not a significant trend yet, but it appears one or more spammers have latched onto this technique, so broader deployments are possible.

Q3 IN REVIEW

Q3 Outbreak Patterns in Review

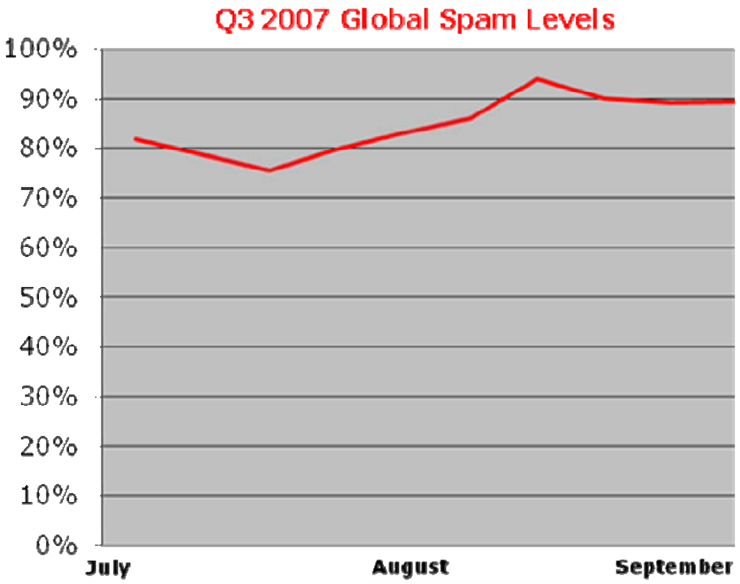
During the third quarter, blended threats and PDF spam have been the most dominant types of unwanted email, and their activities are expected to increase over time. PDF spam may expand to include the use of other common attachment types. Pornographic image spam has remained steady, and its levels are not expected to increase significantly. Other techniques were used throughout the quarter, as outlined in the chart below.



Source: Commtouch Labs

Global Spam Rates on the Rise

Global spam levels are increasing all the time, hitting an all-time high of 95% of all emails sent during a peak in the third quarter of 2007. Individual outbreaks using rapid-burst distribution cause daily and weekly variation, but overall levels remain very high.



Source: Commtouch Labs

Most Popular Spam Topics

Pharmaceutical spam is still the most common spam topic, however it decreased during Q3, dipping from 45% in Q2 to 30% in Q3. Overall sex-related topics continue to be the most popular, as the combination of pharmaceuticals such as Viagra and Cialis with enhancement products totals 53% of spam and 56% if you add in pornography. Non-sexually related subjects are generally split evenly, with 7% stock pump and dump, software 5%, replica products at 4%. All data is according to analysis by Commtouch Labs.

Topics of Spam Email	
Pharmaceuticals 30%	Software 5%
Enhancers 23%	Replicas 6 %
Loans & Real Estate 14%	Pornography 3%
Stock Pump and Dump 7%	Other 14%

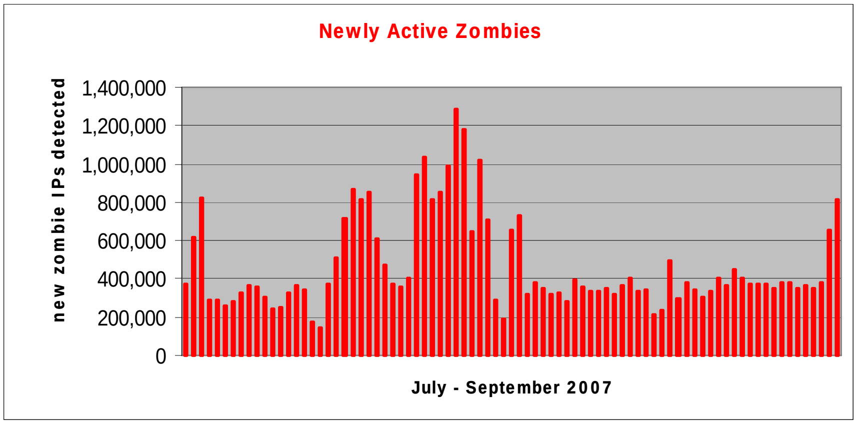
Source: Commtouch Labs

Zombies

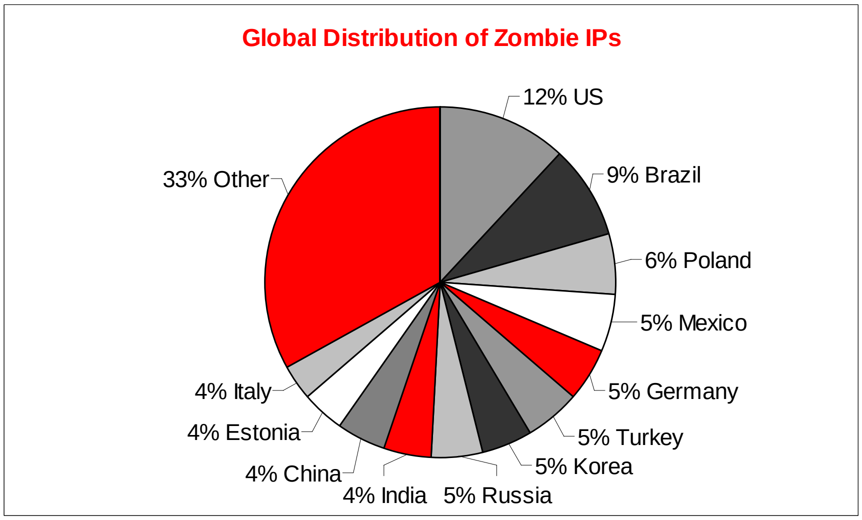
The repeating theme of each of the outbreaks described here are the zombies that are at the heart of the illicit email distribution system. Zombie botnets are providing the vast computing power needed to generate PDF spam and other types of attachment spam, they are distributing the email messages themselves, and they are serving as the hosts to rogue web sites used to infect unsuspecting computers.

Zombies themselves are evolving to be more robust senders. For example, during several of the outbreaks during the quarter, they were observed to be behaving similarly to legitimate MTAs (Mail Transfer Agents). While in the past, zombies could be counted on to simply send messages and not worry if they were ever delivered, today many are keeping track of mail queues and retrying to send messages that were temporarily rejected (or "tempfailed") on the first try. This new zombie feature significantly decreases the effectiveness of a spam-fighting technique known as "graylisting," where legitimate MTAs tempfail emails from unknown senders, based on the concept that legitimate senders would retry and zombies would not. As usual, the spammers have bypassed the "quick fix" with a technological innovation of their own, showing that this underground enemy is truly formidable.

The graphs below show the newly active zombies identified throughout the third quarter, and the geographical distribution of the zombie computers. Note that zombies machines are typically changing their IP addresses fairly frequently, both because they are home PCs that naturally have a dynamic IP address, and also due to the fact that the bot controllers often force an IP address change in order to better hide their activity. Commtouch GlobalView™ Reputation Service identifies between 300,000 and 500,000 newly active zombies per day, on average.



Source: Commtouch GlobalView Reputation Service



Source: Commtouch GlobalView Reputation Service

Conclusion

Attacks spread by “innocent” spam with malware download links are becoming increasingly pervasive. Simple sales spam, including the use of standard file attachment formats will continue to be popular, as they are generating enough business that they remain profitable for spammers. The variety in content and delivery methods requires real-time email defense against spam and malware, reinforced with web vigilance against those same zombie-hosted IP addresses.

Commtouch technology protects against spam, email-borne malware and blocks SMTP sessions initiated by zombies. Commtouch’s Recurrent Pattern Detection™ (RPD) technology delivers extremely high malicious email detection rates and protects against spam and malware attacks in real-time as they are mass-distributed over the Internet. Commtouch GlobalView Reputation Service dynamically blocks spam at the network perimeter based on the reputation of the sender. The combination of Commtouch’s Anti-Spam, Zero-Hour Virus Outbreak Detection and Reputation Services deliver three layers of email defense.

Commtouch Anti-Spam, Zero-Hour Virus Outbreak Detection and Reputation Service 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.

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. Copyright © 2007