

Q2 2007 Email Threats Trend Report

PDF Spam, Zombies and Blended Malware with Spam

July 17, 2007

One of the most notable events of Q2 occurred at the very end of the quarter – the emergence of PDF spam – and it demonstrates several key characteristics of today's email threats. These characteristics, which will be discussed throughout this report, include: evolving spam techniques, extensive use of botnets, and blended threats.

PDF Spam

A close successor to the now waning image-based spam, the new technique of attaching popular Portable Document Format (PDF) files is designed to bypass many traditional anti-spam engines. During one particularly massive outbreak last week, the Commtouch Detection Center determined that PDF spam comprised 10-15% of all global spam messages during a 24-hour period. Given the fact that these messages are nearly four times bigger than 'standard' spam messages, this increased overall global spam traffic by 30-40%.

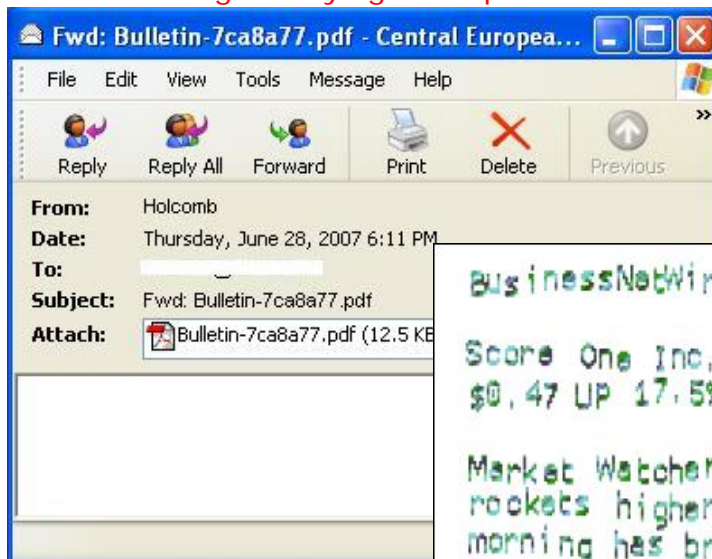
PDF spam comprised 10-15% of global spam messages during a 24-hour period, increasing overall global spam traffic by 30-40%

This new spam-tactic takes advantage of the popularity of the PDF format, which prevents the adoption of broad blocking policies, such as those often enacted against .exe files.

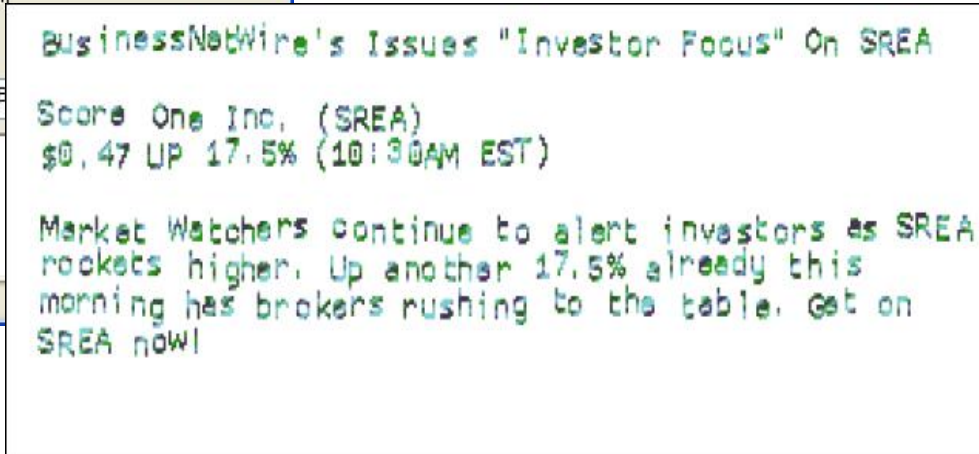
There have been several distinct outbreaks of this type of spam:

- Randomized content, similar to the image-based stock spam we have become familiar with; letters and backgrounds are randomly altered to fetter optical character recognition (OCR) technology.

Email Message Carrying PDF Spam



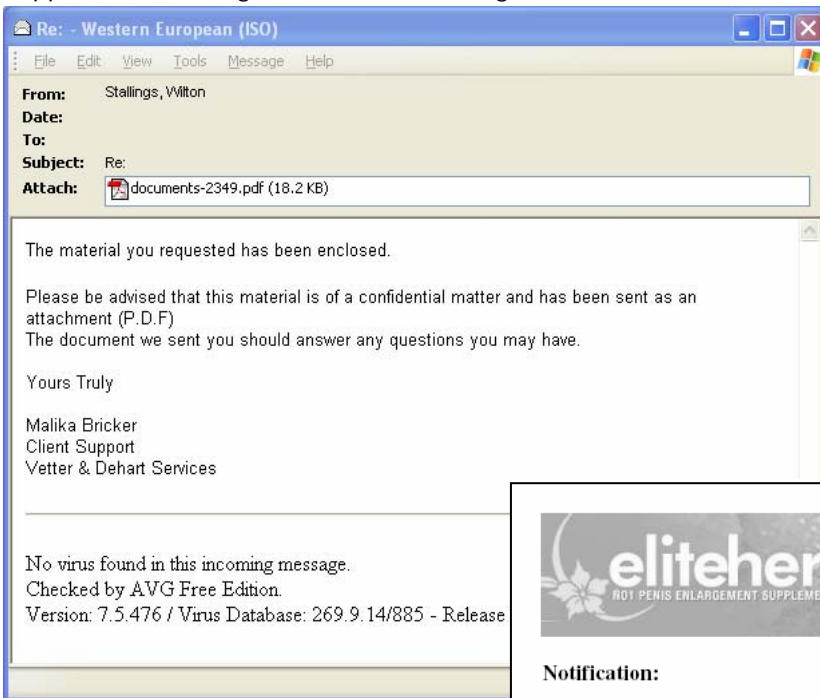
Spam Image Converted to PDF Format



Q1 2007 Email Threats Trend Report

- Professional look-and-feel, which appears similar to legitimate business correspondence. The contents of the messages, however, include sexual enhancers and stock promotions. The example below shows a “Client Support” email, and its attached PDF file.

Sample Spam Message with Attached PDF File
Appears to be a legitimate email message



PDF File Attached to Spam Message
Appears legitimate until you read the text



Notification:

If your penis is still under 6 inches, then don't give up. Eliteherbals has just released a new male growth hormone that has been laboratory proven to gain anywhere from 1-3 inches over a 3 months period.

Living with a small penis is very painful and very embarrassing. Stop getting laughed at in the locker rooms, and start satisfying the girls. With anything smaller than 6 inches, your finger would be more satisfying to a girl than your penis.....

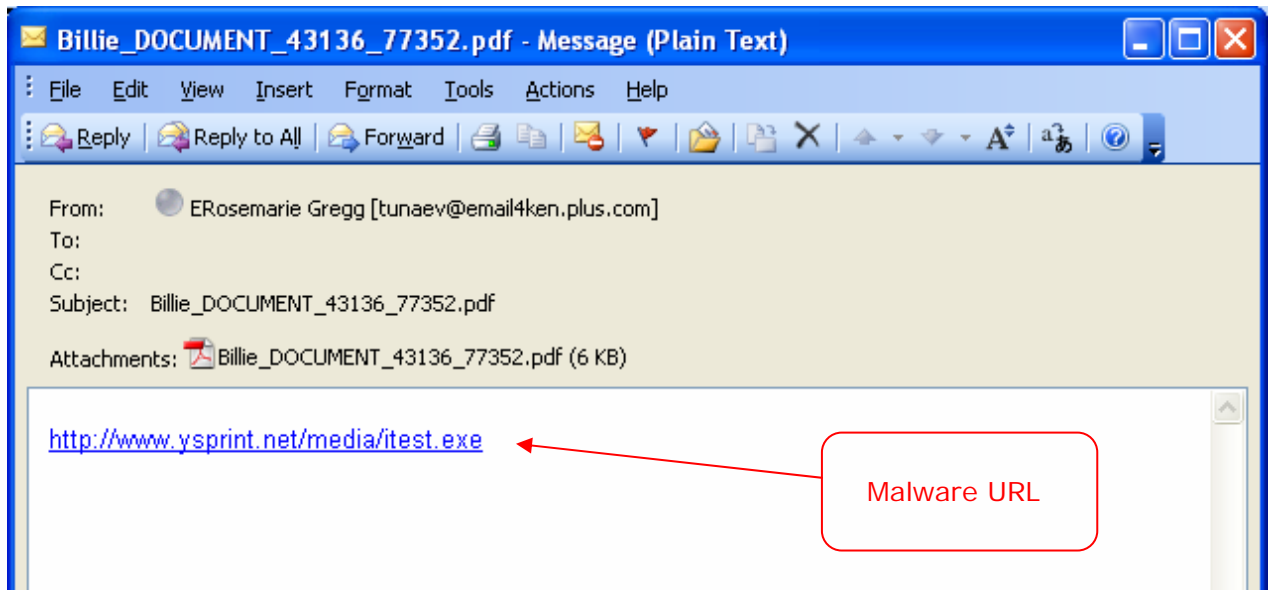
Check us out:

<http://www.>

Todd McFall
Marketing Engineer
Elite Herbals (MegaDick).

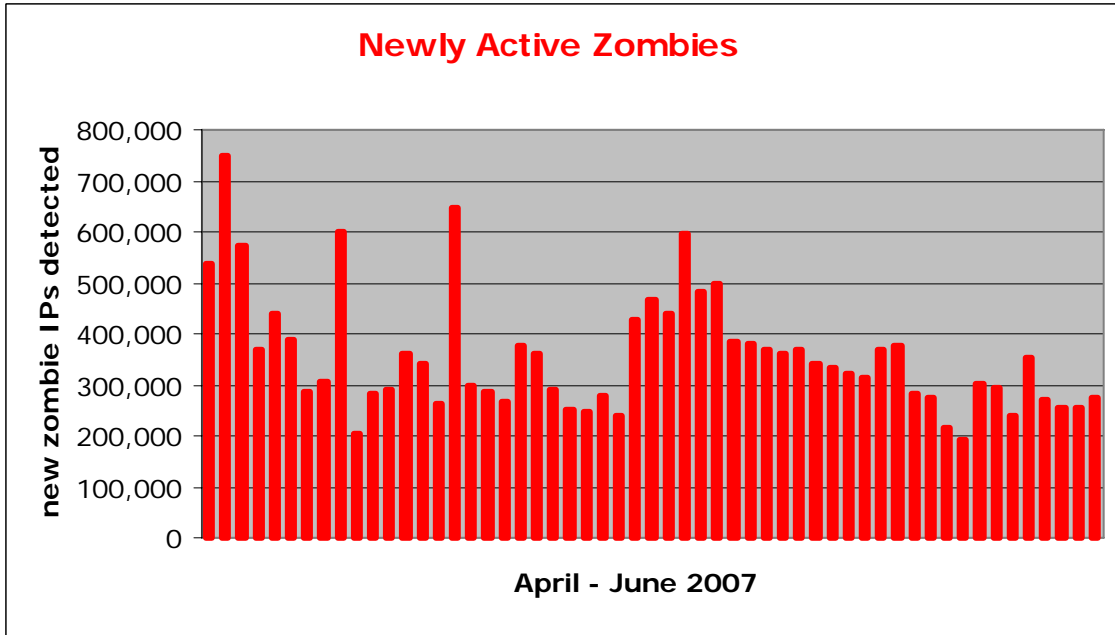
- Combined spam and virus in a single message: the message contains a link to a web site containing malware, and an attachment promoting a stock.

PDF Spam Combined with Malware URL



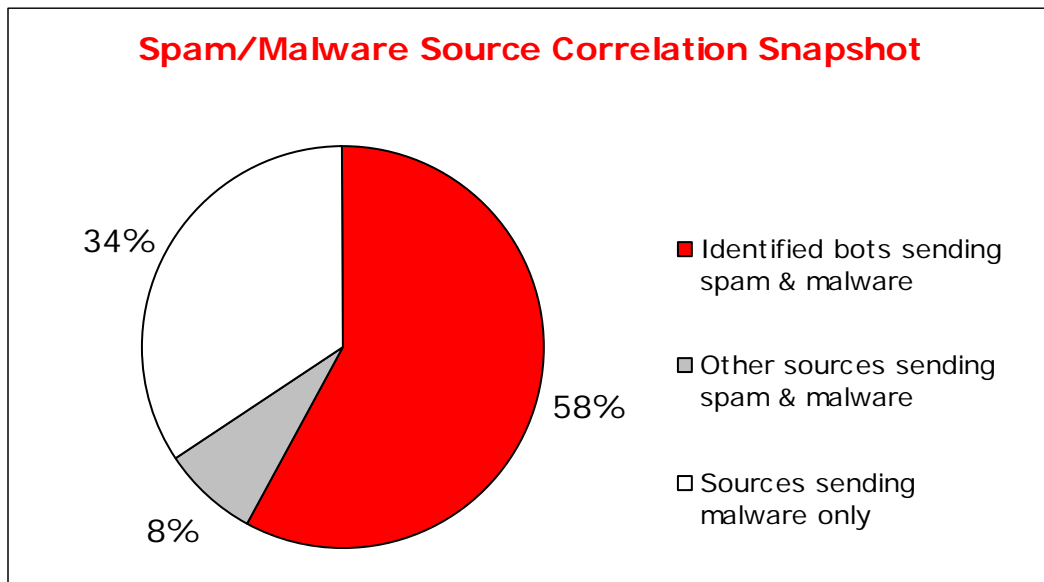
Botnets Expand in Size and Activity

The massive botnets seeded last year continued to grow and regenerate during the second quarter of 2007, and the capability of sending massive amounts of PDF-spam is just one such indicator. Now considered public enemy number one, the Internet security community is searching for an effective tool to combat botnets. This has proven a difficult task due to the dynamic nature of zombie IPs. Real-time Black Lists (RBLs) attempt to gather offensive IPs and block SMTP sessions from 'blacklisted' IPs. This method is minimally effective, since static lists do not reflect the dynamically changing zombie behavior. Botmasters also constantly grow their networks by distributing Trojan malware to recruit new PCs. The Commtouch Reputation Service, which dynamically detects zombie spam-sending activity, registered an average of 343,000 newly activated zombies per day, during Q2 2007.



Source: Commtouch Reputation Service

At the midpoint of 2007, massive botnets have become the focal point for a convergence of nearly every type of Internet threat. After spending last year building up the infrastructure, botnets emerged as a powerful and pervasive tool for spreading spam email. Now that the groundwork is established, botmasters have begun using their malicious networks of zombie PCs to launch blended-threat email attacks that send both spam and viruses. In fact, email is the most popular way to spread malware, accounting for 23% of malware infections according to a recent Computer Economics report. Commtouch research shows over 60% of spam-sending bots also send email-borne malware.



Source: Commtouch Reputation Service

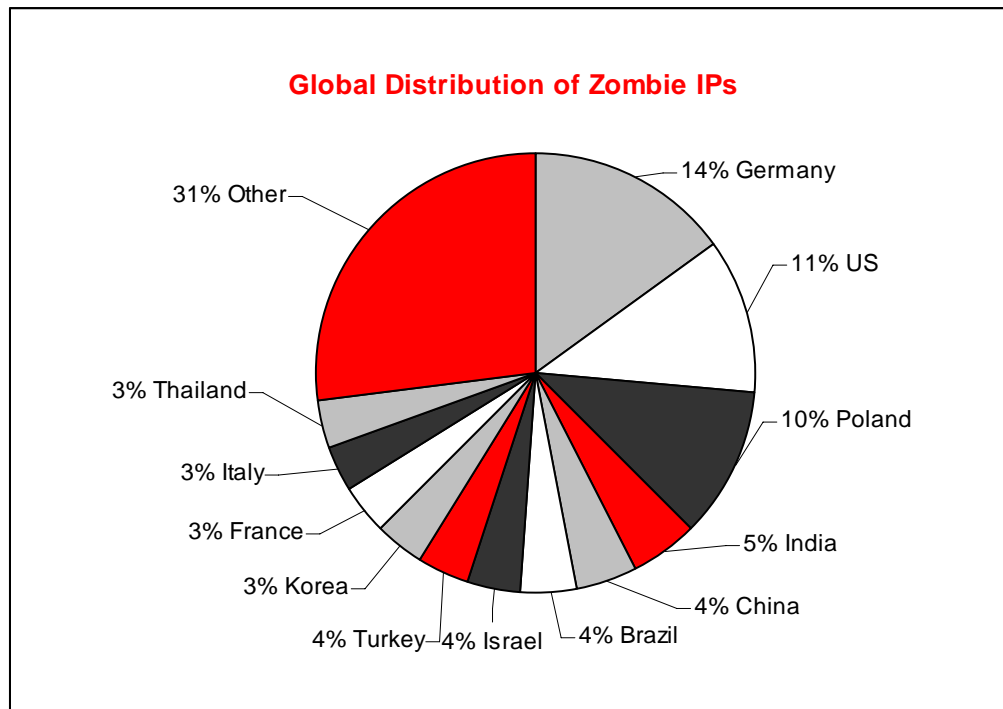
The email-borne malware sent by botnets carries out a variety of malicious activity such as stealing passwords and personal information, harvesting email addresses and launching distributed denial of service (DDoS) attacks. Botnets are now the weapon of choice for all types of malicious activity, and defending against them is becoming increasingly difficult. Traditional defense technologies are falling behind the rapidly advancing malicious tactics, and a new blended-security approach is emerging to answer the call.

The Spam Sent Around the World

Having a large network of zombie PCs grants spammers access to endless bandwidth to generate and send massive amounts of spam, while hiding behind a highly distributed network of dynamic IPs. The global distribution of zombie IPs demonstrates that botnets reach every corner of the earth. In a 24-hour sample from a recent PDF-spam outbreak, the messages were sent from no less than 185 countries. The number of messages sent from each IP address ranged from a single message to several thousands.

In a recent PDF spam outbreak, messages were sent from 185 countries.

The chart below shows the global distribution of active zombie IPs for a randomly sampled 24-hour period during the quarter.

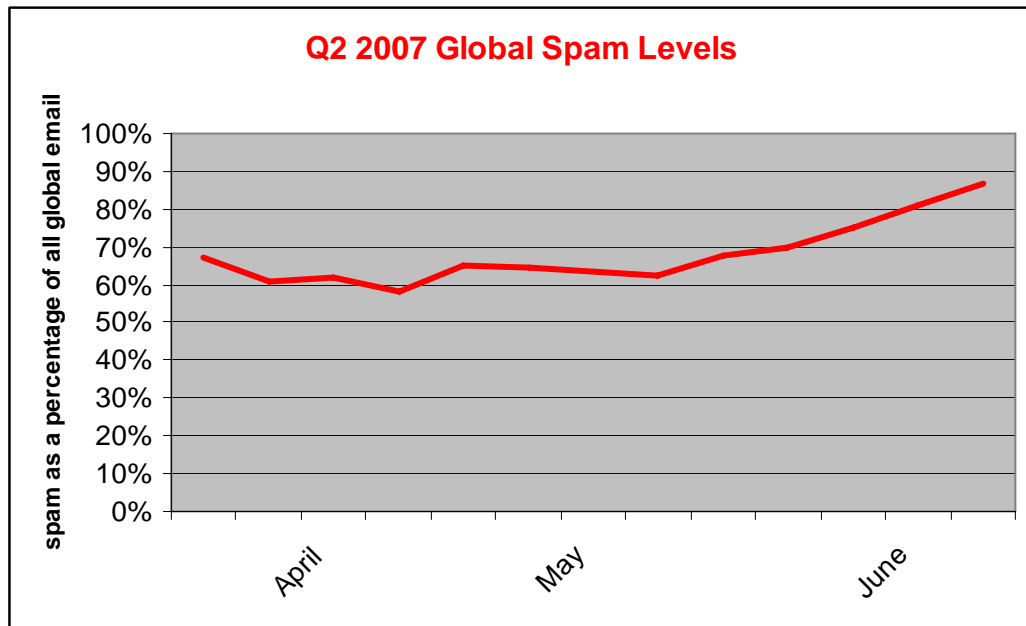


Source: Commtouch Detection Center

While bots are found in every country with Internet access, the amount of spam actually sent from any particular country is closely related to the size of its PC using population and the availability of broadband Internet access. Of course, the botnet rate is also influenced by the level of computer security. If Trojan malware doesn't penetrate defenses, a PC will not become a zombie.

Global Spam Rates Stable

Overall global spam levels remained at 85-90% during the second quarter of 2007. Though the average level over time is stable, considerable fluctuation is seen from day to day. This is evidence of the rapid-burst distribution method used to evade human-based filters that are subject to delays in classifying new spam outbreaks. By the time honeypots or human spam reporting systems recognize a new spam message, the outbreak is liable to be over. Spam levels did dip slightly in April and May, but returned to Q1 levels by the end of the second quarter.



Source: Commtouch Detection Center

Most Popular Spam Topics

Pharmaceutical spam soared during Q2, with 45% of all spam touting Viagra, Cialis and other medicines, up from just 12% last quarter. The same subjects continue to be popular for spam sent in Q2 as in previous quarters. Sexual enhancement products and stock 'pump-and-dump' scams remain popular, according to the Commtouch Detection Center.

Subjects of Spam Email	
Pharmaceuticals 45%	Replicas 7%
Stock Pump and Dump 18%	Gambling 6%
Sexual Enhancers 10%	Software 3%
Finance 8%	Other 3%

Source: Commtouch Detection Center

Image Spam Wanes

Image spam, or the technique of embedding or attaching GIF or BMP images to spam messages, now accounts for less than 15% of global spam email messages, a drop from 30% in the first quarter. Technical advancements have most likely caused the use of this technique to recede. The anti-spam industry has had ample time to improve its ability to defend against this tactic, and therefore spammers have moved on to newer, more effective (at least for now) techniques.

Conclusion: Email Threats Converge, Complete Security Solutions Become Essential

Huge botnets are now being used to flood the Internet with spam, but also to distribute email-borne malware. Commtouch research shows over 60% correlation between IPs launching both spam and malware attacks. The current reality requires complete email defense that protects against spam, email-borne malware and blocks SMTP sessions with malicious IPs. Commtouch Anti-Spam, Zero-Hour Virus Outbreak Detection and Reputation Services deliver complete email defense.

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 Reputation Service dynamically blocks spam at the network perimeter based on the reputation of the sender.

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