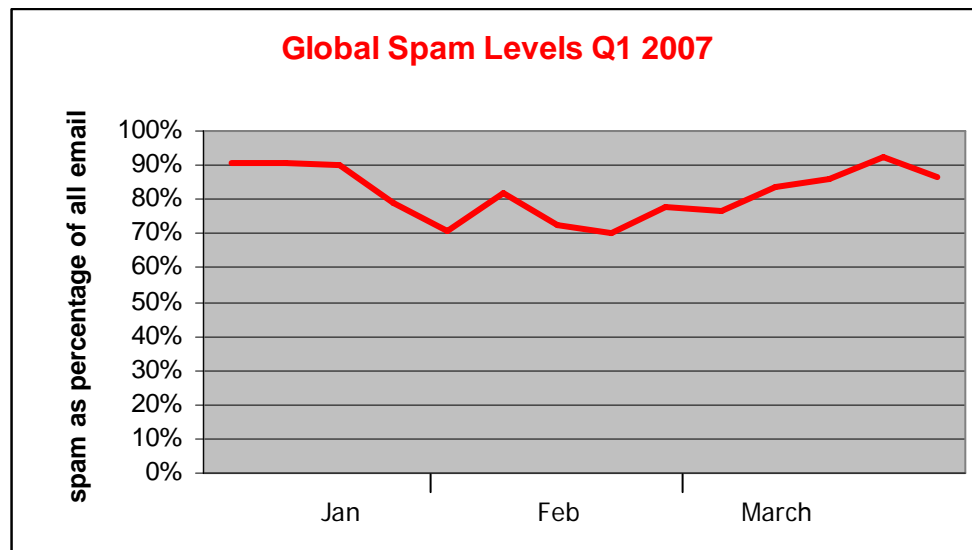




Q1 2007 Spam Trends: Botnets Continue Sending Devious Spam

April 18, 2007

Botnets remained the driving force of email threats throughout the first quarter of 2007, and spammers developed new tactics to fool anti-spam engines. Massive networks of zombie PCs powered the unrelenting onslaught of junk email, keeping overall global spam levels high. Intense spam peaks during the holiday season from November to January were followed by a slight drop in global spam levels in February and March. However this is a natural correction to previous peaks and does not indicate a downward trend. By the end of the quarter, spam levels returned to 85-90% of all global email.



Botnets Continue

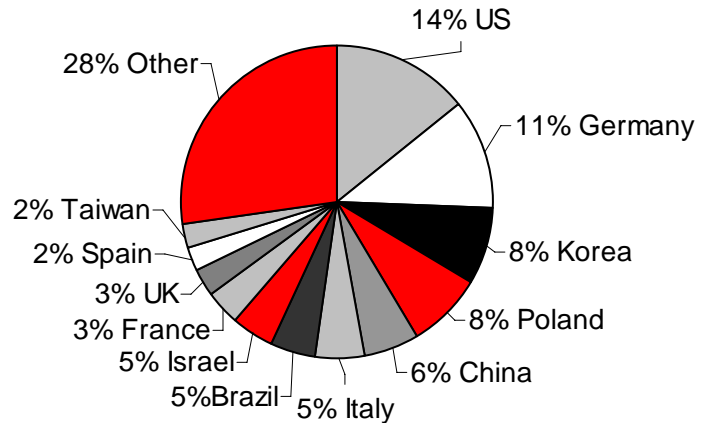
Huge bot networks put the computing power of millions of zombie PCs at the disposal of spammers, who use them to generate randomly-altered image-spam. The wide distribution of zombie PCs affords botmasters the flexibility to alternate the sources of spam attacks dynamically. In fact, the typical zombie computer actively sends spam for brief periods of just a few hours and then lies dormant until reactivated for the next outbreak. Therefore, the ability to dynamically identify zombie-generated traffic the moment the zombie is activated is essential.



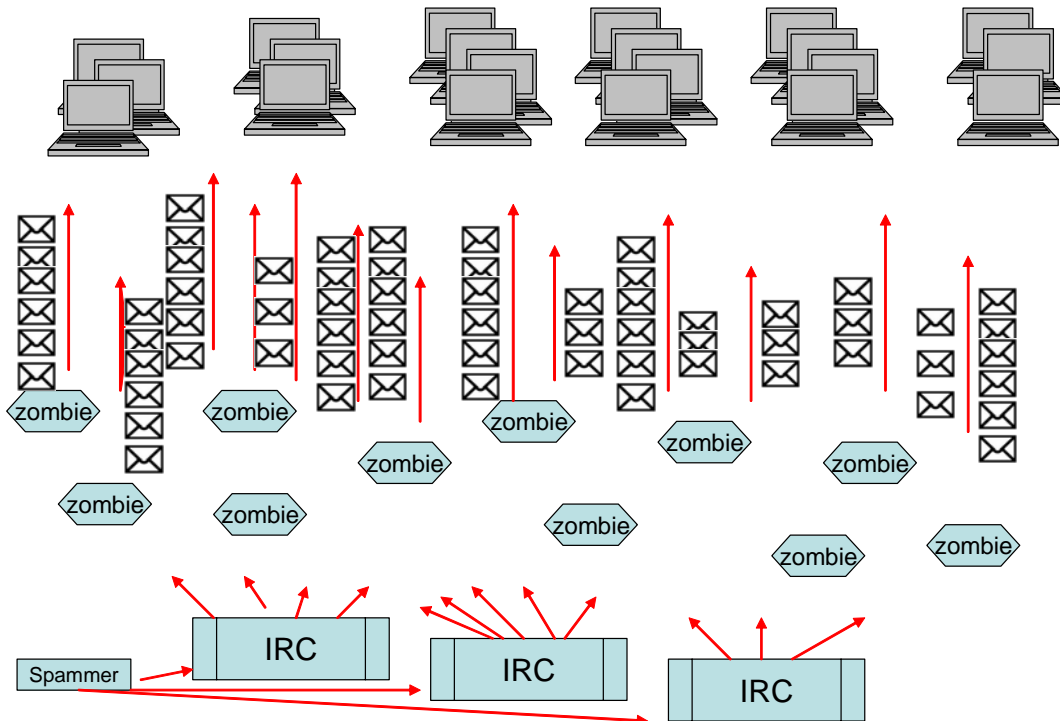
The chart on the right shows the global distribution of active zombie IPs for a randomly sampled 24-hour period during the quarter. The amount of spam each individual zombie can send is dictated by the speed of its Internet connection. As broadband access becomes more widely deployed, more zombie computers are capable of sending large quantities of spam.

The spammers continuously capture additional zombie computers by distributing malicious Trojans that give the spammer control of ordinary PCs. Widely distributed botnets are capable of sending massive amounts of malicious email in very short periods of time, making it difficult for static technologies to identify and block any particular sender IP.

Global Distribution of Zombie IPs



Botnets Distribute Massive Amounts of Spam





Most Popular Spam Subjects

The same subjects remained popular for spam sent in Q1 as in previous quarters. Sexual enhancement products and stock ‘pump-and-dump’ scams are still the most popular, according to the Commtouch Detection Center.

Subjects of Spam Email	
Sexual Enhancers 53.6%	Pornography 2.6%
Stock Pump and Dump 19%	Software 1.4%
Other Pharmaceuticals 12%	Electronics 1%
Finance 3.8%	Other 6.4%

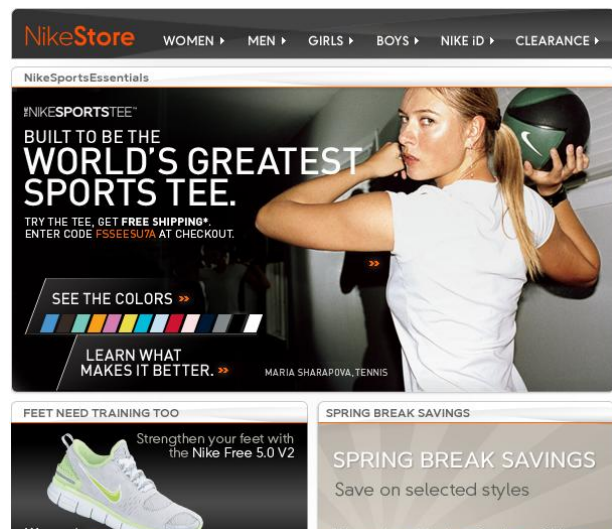
Latest Spam Trick: Hijacking Newsletters

Spammers unveiled a new email tactic in the first months of the new year – hijacked newsletter spam. Hijacked newsletter spam aims to evade anti-spam filters by disguising itself as a legitimate form of mass distributed message – email newsletters. In this scheme spammers essentially commandeer a popular legitimate email newsletter and insert their spam image at the beginning of the message. This trick works by cloaking the spam image in a legitimate email newsletter to sneak past anti-spam solutions and into users’ inboxes.

How Hijacked Newsletter Spam Works

Popular Newsletters: Perfect Victims

Hijacked newsletter spam takes over popular, legitimate email newsletters from well-known companies. In the first quarter of 2007, a spammer copied the code of a consumer newsletter from sporting good giant Nike, altered the message and used it to distribute spam. The stolen email newsletter references a series of images, all dynamically loaded from a legitimate Nike server.





Needle in a Haystack

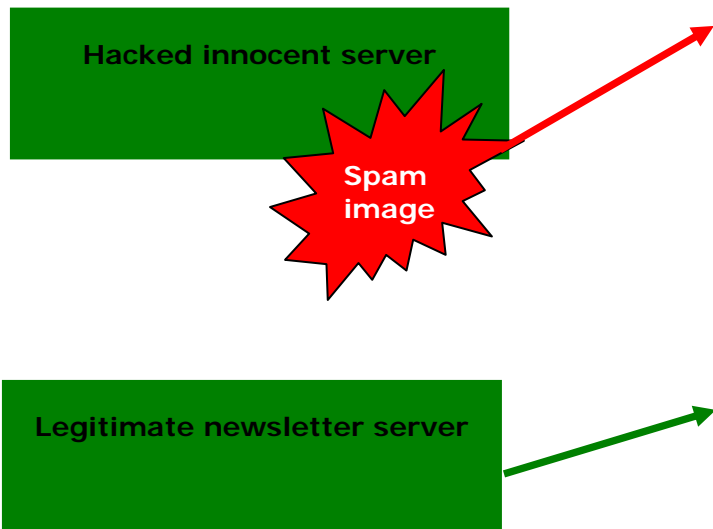
The spammer then inserts a spam image that is hosted on another server. The spam hosting server may either be an illicit website managed by the spammer or an innocent server the spammer has hacked and used to host the spam image. The highlighted line of image source code `` points to the spam image that has been posted on an innocent website.

```
MIME-Version: 1.0
Content-Type: text/html
Date: Fri, 16 Mar 2007 06:53:34 -0700 (PDT)
X-CTASD-RPTID: str=0001.0A090205.45FAA166.0040,ss=1,fgs=0
X-CTASD-IP: 89.178.224.75
X-CTASD-sender:

<a href="javascript:alert('http://1.email-nike.com/r/043rn8260f8v00skkx');"></a></td>
</tr>
<table border=0 cellpadding=0 cellspacing=0 width=600>
<tr>
<td><a href="javascript:alert('http://1.email-nike.com/r/043rn8260f8v00skkx');"></a></td>
<td><a href="javascript:alert('http://1.email-nike.com/r/043rn8260f8v00skkx');"></a></td>
<td><a href="javascript:alert('http://1.email-nike.com/r/043rn8260f8v00skkx');"></a></td>
</tr>
<tr>
<td><a href="javascript:alert('http://1.email-nike.com/r/043rn8260f8v00skkx');"><img src="http://c.email1-
```

All Images Rendered

When the spam message is opened, all the images -- legitimate and illicit -- are loaded from their respective servers and appear together in the email message. The spam image may serve as a link to a website hocking pharmaceutical knock-offs or other wares. In the example a stock pump-and-dump image was displayed.





How Hijacked Newsletter Spam Evades Filters

The new hijacked newsletter spam was designed to bypass many types of anti-spam techniques.

Anti-spam technologies that rely on content filtering are bypassed by this type of spam since the content looks like a legitimate newsletter. Bayesian filters that weigh different aspects of a message to determine if it is spam can be fooled because the legitimate newsletter content could outweigh the disguised spam image link.

Spam filters based-on Optical Character Recognition (OCR) and other image-analysis algorithms are oblivious this latest type of image-spam. OCR-based and image-analysis technologies are only capable of scanning images embedded within the message itself. Hosting the spam image on a web server renders these techniques useless.

URL blockers are also fooled by hijacked newsletter spam. The spammers often crack legitimate websites and upload the spam image without the site owner's knowledge; this allows the message to evade anti-spam solutions based on blocking of suspicious URLs. If the email message only contains a link to a legitimate web server, URL blocking anti-spam solutions will not recognize it as spam.

Conclusion: Botnet-Powered Email Threats Require Network-Based Security

Hijacked newsletter spam is only the most recent spammer development. The innovation race continues as spammers aggressively search for new ways to evade traditional anti-spam solutions, including URL blockers and OCR technologies.

Commtouch's Recurrent Pattern Detection (RPD) technology delivers extremely high spam detection rates and protects against spam attacks in real-time as they are mass-distributed over the Internet. The unique content-agnostic technology detects and blocks spam in any language and is highly effective against image-based spam. Commtouch Reputation Service dynamically blocks spam at the network perimeter based on the reputation of the sender.

Commtouch anti-spam, Zero Hour Virus Protection and IP Reputation technology has been selected by scores of OEM partners, who integrate it into managed services, security appliances, software gateways 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