



2006 Spam Trends Report: Year of the Zombies

December 27, 2006

The Commtouch year-end roundup of spam trends for 2006 is based on real-time analysis of more than two billion messages per week from all over the globe. Commtouch has named 2006 "The Year of the Zombies" since even though zombies (aka bots) existed previously, during this past year spammers were able to organize them into massive botnets to harness virtually unlimited computing power; this enables them to generate infinite versions of image spam, and launch massive distributed attacks that have proven more and more difficult for traditional anti-spam engines to block. Zombies, along with other innovations have contributed to a 30% increase in spam in the last year.

Zombies Know No Borders

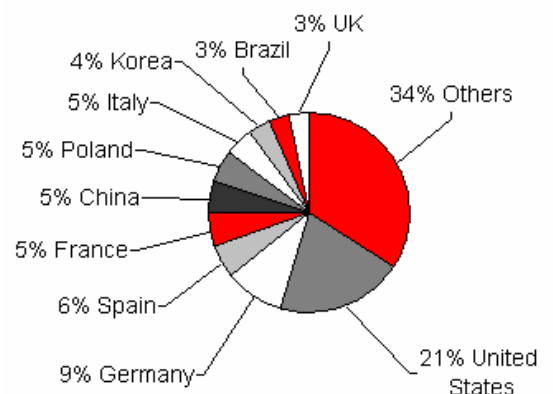
Spammers invested this year in building huge globally distributed botnets, some containing as many as 200,000 compromised zombie computers. Zombies have sprung up in every corner of the globe as they seek out weakly protected computers with fast Internet connections, primarily home broadband users. Commtouch Labs has identified that the largest single number of zombies exists in the United States (21% of all zombies globally), with Germany coming in a far second place (9% of all zombies globally). Many countries have a small amount of zombies, less than 3%, of the world's zombies. However, these countries together account for over 30% of all zombies at any given time, showing just how distributed botnets have become.

Botnets work by taking over large numbers of PCs and using them as bots to launch massive, short-wave attacks. Since the distributed attack is made from millions of otherwise innocent computers, no specific IP address can be identified as the culprit and blocked. Zombies are usually activated for brief outbreaks lasting an average of 2-3 hours, and then they are deactivated by their controllers until they launch their next attack. Zombie fighters are making a concerted effort to bring down botnets but are having little success due to their sophistication and maneuverability.

2006 Spam Highlights

- Zombie activity accounts for 85% of the spam circulating the Internet
- Zombie Botnets pumped spam levels up 30% since last year
- Zombie botnets can send up to 1 billion spam messages in few hours
- Global spam range: 45%-98% of Internet messages
- Spam bandwidth has bloated to 1.7 billion MB per day
- Image spam accounts for 35% of messages and 70% of bandwidth taken by spam
- Ebay and Paypal remain top targets for fraud, together 50% of all phishing attempts

Global Distribution of Zombie IPs





Commtouch Labs has calculated that there are between six and eight million zombie IPs active at any given day. However, zombie machines come in and out of circulation constantly. Approximately half a million new IP addresses are identified as infected by zombies each day.

2006 Zombie Facts	
Number of Zombie IP addresses active at any one time	6 – 8 million
Number of new zombies per day (new bots, dynamically changed IP addresses)	500,000
Length of average zombie-driven spam or malware outbreak	2 – 3 hours
Number of zombies used per outbreak	10,000 – 200,000
Number of email messages a typical botnet sends	160 million messages in just 2 hours
Number of email messages a group of botnets can send, when working in concert	1 billion messages in just a few hours

Source: Commtouch Labs

More Spam or Just Less Detection?

With the help of massive zombie armies the overall global spam rate reached 87% of email sent over the Internet at the end of 2006, up 30% from this time last year (note: this does not count email sent within an organization's Intranet). Internet spam rates vary quite dramatically based on a few key parameters. High quantities of legitimate email messages in the business sector keeps spam percentages lower than in the consumer sector. However, business email increasingly became the target of spam in 2006, registering a 50% increase.

The global average doesn't tell the whole story. The fact is the levels of spam hurled at networks vary dramatically according to network type.

Spam levels as low as 45-65% are enjoyed by small to medium sized enterprises (SME), mainly due to their small size and relatively low visibility. The fewer email users a company has, the less useful it is to spammers, and it may simply not be worth the effort to spammers to launch a Directory Harvest Attack. Secondly, SMEs are generally less well-known to the public and this allows them to stay beneath the radar and avoid becoming a target. Malicious email distributors seem to skip over SMEs in favor of larger enterprises.

Global Spam Rates			
	Global	Consumer	Business
2005	67%	80%	52%
2006	87%	93%	78%
Year-over-year increase	30%	16%	50%

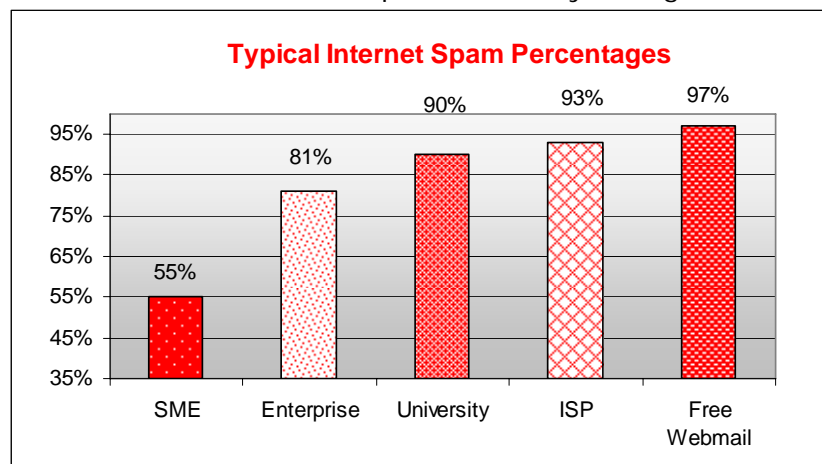
Source: Commtouch Labs



The biggest losers in the war against spam are free email providers that average 95-98% spam. As opposed to SMEs, free email providers are highly visible and have massive numbers of users. Most providers are well known or can be easily identified. All that the spammer must do is write a simple program to generate random user IDs, couple them with the domain names and begin mass distributing malicious emails. Many users open free webmail accounts specifically for the purpose of collecting junk mail, further driving up the spam levels for this type of account.

ISPs come in close behind free email providers because they also host very large numbers of email accounts, many of whom use the ISP domain for their email. Institutes of higher education are also prime targets not only due to size and visibility, but for cultural and demographic reasons as well. Freedom of speech is a very strong cultural value at most

universities. They may be more reluctant to implement strong anti-spam solutions since this could be seen as censorship. The student population is also prized by spammers because they are considered more susceptible to the myriad of financial exploits, many of which allure victims with offers of too-good-to-be-true student financing.



Source: Commtouch Labs

Spam Innovation Floods Inboxes

The figures listed above refer to the proportion of all email sent globally across the Internet that is spam, not the amount ends up in users' inboxes. The actual amount of spam in users' inboxes varies depending on what type of anti-spam solution they are using. Inboxes and networks were flooded in 2006 as spam blocking rates of many anti-spam engines crashed under the pressure of innovative new spam techniques. Approaches such as IP blacklisting and content filtering and exposed their Achilles' heel as spammers developed new techniques using images, randomization and maximized distribution via botnets.

Dynamic Zombie Botnets Overcome Blacklisting

The use of botnets has reduced IP blacklisting to only a small part of the fight against spam, since the IP addresses of spam senders are constantly changing. The vast majority of IP addresses sending spam are zombies (accounting for 85% of all spam sent). In some cases, IP address range owners may not realize their servers have been hijacked by one or more zombies, and that they are unknowingly sending a combination of spam and good mail. In such a case, blacklisting the IP address range prevents users from receiving the legitimate mail this organization sends. The appropriate response is to rate limit or 'tar pit' the incoming mail based on the reputation of the sender. This has the effect of slowing down the rate at which mail is received from this sender, allowing the legitimate email messages to be received without overwhelming the network with illegitimate mail.



Image-Based Spam Overwhelms Text-Oriented Anti-Spam Technologies

Image-based spam flowered throughout 2006, employing new camouflage techniques every few weeks, in order to befuddle anti-spam engines. What started as basic text captured in a GIF image to bypass basic dictionary-based content filters, morphed into new (and sometimes nearly unreadable) formats. These approaches allow spammers to launch massive automated attacks wherein no two emails are exactly alike.

2006 Innovations in Image Spam

Random pixels in the background of the image (they appear to be 'dirt' in the background)

Changes to border color, background color, font color

Broken puzzle pieces with multiple images coming together to appear as a single image of text

Animated GIF images

Use of other image formats besides GIF and JPG, e.g. PNG

Addition of random text sampled from legitimate web sites

"Snowflake" patterns spread throughout the image

Wavy fonts, random line breaks and connected letters

Patchwork colors in background

Multicolor characters with pixel-level randomization

Source: Commtouch Labs



Image-spam Causes 70% of Bandwidth Bulge

The amount of image-based spam grew substantially in 2006, reaching 35% of all spam at its peak distribution time, compared to less than 10% of all spam this time last year. Image spam is particularly costly not only because it is often able to evade detection by traditional anti-spam technologies, but the large file size places an unbearable burden on bandwidth and storage resources.

Massive image spam attacks helped bring spam bandwidth bloat to 1700 terabytes of bandwidth per day (1,700,000,000 MB) in 2006.

2006 Image Based Spam Bandwidth Bloat		
Number of email messages sent per day, globally	Estimated	160 billion
Number of these email messages that are spam	87% x 160 billion	140 billion
Breakdown of image spam vs. text spam	35% image based spam 65% text based spam	48 billion image based spam messages 92 billion text spam messages
Daily image spam volume	48 billion x 25K (average size of image spam message)	1200 terabytes (or 1,200,000,000 MB or 1.2×10^9 MB)
Daily text spam volume	92 billion x 5.5K (average size of text spam message)	500 terabytes (or 500,000,000 MB or 5×10^8 MB)
Daily spam volume (total)	1200 + 500	1700 terabytes (or 1,700,000,000 MB or 1.7×10^9 MB)
Percentage of total spam volume used by image-based spam	$1200 / (1200 + 500) \%$	70%

Source: Commtouch Labs

Image-spam is 35% of spam messages, but creates 70% of the volume of spam messages. This huge increase in volume has prompted the industry demand for on-session blocking solutions that can stop spam at the network perimeter before it wreaks havoc of costly network resources.



Conclusion:

Increased Sophistication of Spam Attacks Requires Real-Time Zombie Detection

The number of spam attacks is increasing, though perhaps not at the alarming rate some anti-spam vendors have been suggesting. The real cause for concern is that for now it seems the industry is losing the innovation race against spam and email-borne malware. The heat is on anti-spam technology vendors to regain control.

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. IP Reputation Services dynamically block 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 more than 50 OEM partners, who integrate it into managed services, security appliances, software gateways and client software applications. For more information about enhancing your security offerings with Commtouch technology, see www.commtouch.com or write nospam@commtouch.com.