A background image showing a laptop on a desk with a speedometer overlay, suggesting speed and technology.

The Spam Scramble

A Trend Micro White Paper



➔ Ever-Growing Spam Volumes Demand a New Approach to Email Security

August 2010

Learn about new antispam best practices and the hybrid solution with the power of two

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

I. INTRODUCTION

Spam continues to plague enterprises. Rising volumes and more targeted phishing attacks threaten enterprise security, especially those with antiquated antispam and anti-malware solutions. The changing nature of spam and Internet borne malware coupled with the increasing volumes have created an urgent need for a new set of best practices and next-generation security solutions that go beyond the scope of traditional email security.

The rise in spam volume is not only costly in network resources such as bandwidth, CPU processing, and IT help desk time, the drain on end user productivity in organizations is staggering. In fact, Ferris Research estimated that in 2009, spam cost enterprises \$110 billion in reduced productivity worldwide.

In addition to the growing volume and nuisance of unwanted mail, spam has become more dangerous. Enterprises are becoming targets of spear phishing and other targeted attacks. Plus the majority of spam email now contains links to malicious websites where malware is waiting to infect unsuspecting users. And since email with bad links doesn't necessarily contain the malicious code itself, these threats can slip past conventional signature-based email security.

According to TrendLabs, in 2010, 90-97% all email traffic directed towards enterprises is 'spam'. In addition, Trend Micro has seen the volume of spam more than double in the past year—with about 200 billion spam emails sent per day.

II. SPAMMERS—WHO ARE THEY AND WHY DO THEY PERSIST?

The senders of the spam are often part of a criminal gang that uses email to lure victims and ultimately steal enterprise or customer data—credit cards, bank account numbers, or confidential information they can either use themselves or sell on the black market for illegal profit. These gangs treat cybercrime as a serious and lucrative business venture and work diligently to expand their criminal networks—with little risk of capture.

Organizations such as the Russian Mafia, the Chinese Triads and other criminal organizations have quickly adapted to the “digital underground,” where it's very difficult to trace the true sources of spam messages. Messages can be sent from nearly anywhere in the world with no physical presence required.

In addition, spam is actually not illegal in all countries. In some regions, spam is viewed as a legal form of advertisement. This presents a significant problem for law enforcement agencies—since emails cross multiple borders, each with different enforcement agencies and incongruent policies on cybercrime, making prosecution nearly impossible.

Often these criminal organizations use stolen credit card credentials to pay for web hosting. For example, they will pay for a month of web hosting with

A sample of spam industry “goods for sale” by Russian Underground (source: TrendLabs, 2010)

- *Post 1: 1 million custom emails of your choice for \$100*
- *Post 2: \$20 per day to rent spam botnet*
- *Post 3: 1000 valid emails for \$7. Has \$50K validated Yahoo emails available.*
- *Post 4: \$50 per day, 100 emails per minute*
- *Post 5: Bundle of 100 bots, total of 1012 mails/min. Max of 8k bots for hire. \$650 dollars to rent for a week, customer can try for free.*

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

stolen credit card numbers or take out a free trial, using stolen credit card numbers as deposit. These websites are used as fraudulent storefronts, and of course victims are lured to these sites by deceptive spam emails.

Industry estimates on the global revenue from organized cybercrime vary, with criminal organizations earning millions of dollars annually. Legitimate enterprises that become victims of cybercrime pay the highest price. Ponemon Institute, "... found that the median annualized cost of cybercrime of the 45 organizations in our study is \$3.8 million per year, but can range from \$1 million to \$52 million per year per company."

III. SPAMMING TECHNIQUES

Spammers today utilize a myriad of methods to propagate their spam messages in an effort to generate income.

- **Botnets:** networks of "zombie" malware-infected PCs send email on behalf of the spammer, without the knowledge of their legitimate owners. Botnets are controlled by a botmaster, who sells a spamming service to those who wish to send spam.
- **Free email services:** public Webmail (for example, Yahoo! Mail) is misused to send spam.
- **Open proxies:** compromised or misconfigured servers can be used to redirect spam. Known in spammer slang as "peas," open proxies are also sold as a service to spammers in a similar way as botnets.
- **Stolen netblocks:** Spammers set up in business as an ISP, typically by taking over portions of Internet address space

Mega-D is the name of one of the most widespread spam botnets today, though not as prolific as it once was. A single Mega-D spam bot was able to generate around 2,553,940 spam messages in a span of 24 hours, an average of 1,764 spam messages per minute.

MORE ABOUT THE BOTNET THREAT

Spammers are increasingly using "bots", or host computers, which have been compromised through malware to send spam without the knowledge of their owners.

Often these spam bots will be part of a larger "botnet," which may consist of many millions of compromised machines controlled by a "bot herder".

Trend Labs has noticed large outbreaks of spam originating out of botnets within legitimate MTAs of major Internet Service Providers. A compromised machine within an Internet Service Provider (ISP) can send spam directly or the bot can initiate a session with the ISP's legitimate mail server. Trend Micro continues to work with ISP's to trace and clean the offending IP addresses from their networks.

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

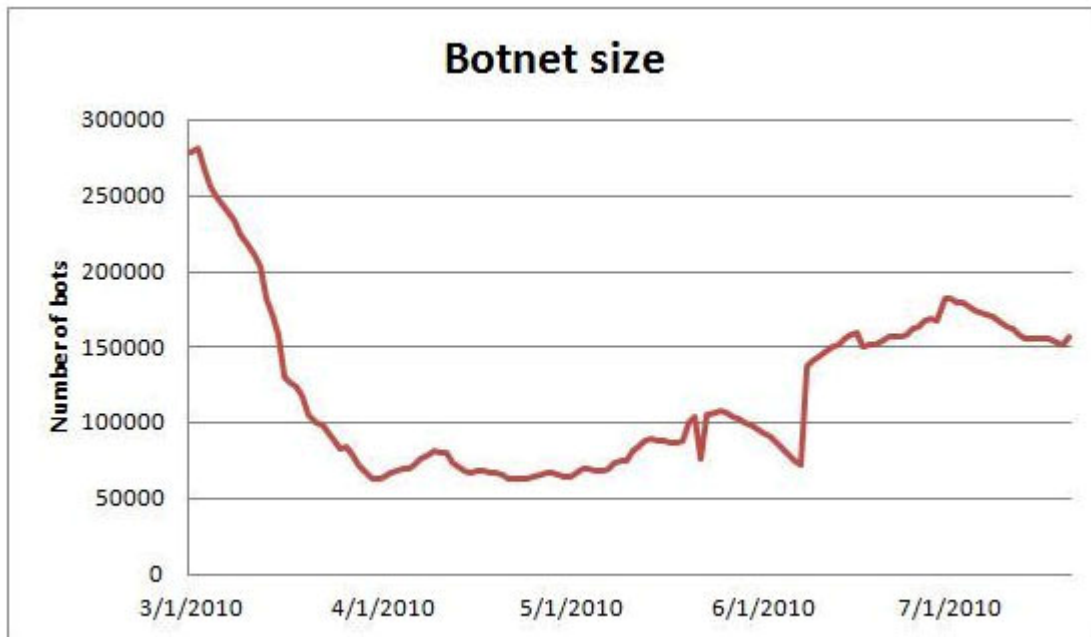


Figure 1. Botnet size

Figure 1 shows the size of a particular botnet between March 2010 and the end of July 2010. As shown, the botnet's size has fluctuated over time; it currently comprises around 150,000 bots. This is not a huge botnet but it still generates multimillion dollars in annual revenue.

Often the services of the botnet are rented out to third parties for illegal activities such as performing a Denial of Service (DDOS) attack, where the target system is flooded with data in order to slow it down or stop it from responding entirely. DDOS services are for sale for about \$70 per day, a small price to cripple a company.

IV. INCREASED SPAM = RISING COST OF SECURITY

The increased volume of bot-generated spam has required enterprises to provide additional resources to process mail, additional bandwidth to receive the emails, additional storage at their final destination, and investigate new strategies for removing the bad mail from their valid business mail.

While antispam technologies are continually improved to tackle the problem, the spammers understand that they too need to evolve their spam. Most commercial spam filters are updated frequently to allow them to detect the latest spam methods, and therefore do a good job detecting spam on a daily basis. In general, an up-to-date antispam engine will typically catch most spam, but its effectiveness will drop in a matter of hours or days if not updated.

Best practice tip:

Set antispam and antivirus filtering policies for outbound email in addition to inbound email. This way, a spam generating computer will be quickly identified within your corporate network.

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

While email administrators strive to preserve the usefulness of their email systems by reducing spam, at the same time, they also need to ensure that legitimate email continues to flow and does not get blocked mistakenly as spam. These “false positives” are possibly more critical to the continuity of a business than allowing a small amount of spam to pass through. More importantly, antispam vendors need to keep refining their detection techniques to take into account the latest spam threats. At the same time, security vendors need to continually work to minimize false detections to ensure that the spam/not spam balance remains acceptable to the user.

V. SPAM CONTROL - SECURITY FEATURES AND BEST PRACTICES

Now that we've discussed the challenges of today's threat landscape, let's take a closer look at the technologies used by modern antispam solutions.

EMAIL AND WEB REPUTATION SERVICES

Central to the fight against the high volume of spam are reputation services. Email reputation service analyzes the history of an email server in order to assign a reputation rating. Typically email reputation is available as a centralized cloud service, queried on demand, allowing an email administrator to create policies to block or delay the messages based on the reputation rating of the sender—usually a known or suspected spammer. Email reputation services can save a considerable amount of resources by rejecting up to 85 percent of all incoming email.

In addition, advanced antispam engines will employ web reputation by extracting embedded URL's in emails and comparing them to an in-the-cloud list of known websites that have a poor reputation, as they are known to harbor malware or be used by known spammers. This approach is especially effective against phishing mails where the URL in the message will take the user to an infected site, in some cases, a clone of a valid site, with the intent to steal the victim's login or financial details.

VALID RECIPIENT CHECKING, RATE LIMITING, AND DIRECTORY HARVESTING

The list of email addresses that spammers use to peddle their wares are typically compilations of addresses bought and sold on the underground market. These lists are compiled from many sources—taken from compromised systems, such as poorly protected (or unethical) ecommerce stores and web servers requiring registration, or directly from the address books of end users that have been infected with a bot.

Best practice tip:

Enterprises should use a high-quality email reputation service as a first line of defense. This will reduce the number of email servers required to further process the remaining email traffic.

Best practice tip:

Web reputation is a very powerful tool within an antispam engine, providing excellent defenses against both phishing emails and links to malware -infected sites. When choosing an antispam technology this should be one of the key criteria.

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

Another method of obtaining recipient email address lists is done through brute force. Leveraging the immense processing power of the botnets within their command, the spammers will simply guess at common email addresses, using large dictionaries of common forenames, surnames and address syntaxes, e.g.:

- John.smith@trendmicro.com
- John_smith@trendmicro.com
- James.smith@trendmicro.com
- James_smith@trendmicro.com

Once an organization is under attack, the corporate email server will reject messages for unknown recipients. Each of these rejections is logged as an invalid email address and the next combination is attempted. This technique is known as a directory harvest attack, as the spammer will attempt to guess every email address within the corporate address book. Once harvested, the directory information will be used to build new spam lists, or if the company is well known, resold on the black market to allow targeted attacks to be carried out against that organization.

The main defense against this kind of attack is a combination of a valid recipient list, combined with intelligence about the connections into email security software. Great care needs to be taken to ensure that by rejecting messages to unknown recipients, you don't expose the valid addresses during a directory harvest attack. This is done either by accepting and silently dropping messages to invalid recipients or by monitoring the mail flow into each domain, and then applying intelligent rate limiting.

HEURISTIC ANTI SPAM ANALYSIS

Another weapon in the battle against spam is the heuristic-based antispam engine. During heuristic analysis, the spam message is processed by a series of many hundreds or thousands of rules, dependant on the complexity of the antispam engine in use. These rules look for the occurrences of key words, patterns, and characteristics within the message that would be indicative of spam. Such rules may look for key words often used in spam, such as Viagra, the proximity of words in relation to other words, such as looking for "discount" close to "medication," attempts to obfuscate or hide words—instead of using "Viagra," character replacement would be used to create a word that looks similar to the human eye, such as "v1ágrá." Other common rules search for items such as whitespace or lightly colored text in between characters such as "vabicdaefghirjka". Another key rule is the analysis of any URLs located within the message.

Best practice tip:

Many email content security solutions have options to automatically update the list of valid recipients, by integrating with corporate LDAP. Enabling this functionality means that the list of valid recipients will be automatically updated in a timely fashion without additional steps for the administrator.

Best practice tip:

If your email security solution has options to enable directory harvest protection and rate limiting, you should enable these. However, you should monitor the email flows carefully as in some cases this may cause valid emails to be delayed. Your security vendor should be able to provide details on how to test and configure these features if necessary

Best practice tip:

The heuristic antispam engine should be set at the default level, and set to tag spam messages rather than delete them. The sensitivity can gradually be raised over a period of time to balance the catch rate versus the false positive rate. More advanced solutions offer the option to take different actions based on the probability of spam. For example, the email administrator could create a rule to delete messages that are highly likely to be spam, and quarantine or tag messages that are less certain.

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

For each of these rules executed against the message, a score is given, with a total score provided after processing all of the rules. If the total score for the message exceeds the thresholds set, then the message is considered spam and treated accordingly. The setting of the thresholds for heuristic antispam engines is one of the most problematic areas of email security—if the heuristic engine is too “aggressive,” then the spam catch rate will be very high, but so will the false positive rate. If it’s too low, then there will be minimal false positives, but a high volume of undetected spam. A ‘one size fits all’ approach to spam sensitivity rarely fits all customers due to the wildly different types of legitimate email traffic—nearly all heuristic engines require a degree of tuning to their environment to be most effective.

ADAPTIVE TECHNOLOGIES

Another layer of protection essential to today’s threat landscape is responsive and adaptive technologies, both locally and through community intelligence.

Statistical analysis, machine learning, and adaptive technologies can be used at an organization’s gateway by tracking traffic patterns, hashing email messages, pulling out information in embedded URL links, looking for content typical of spam and other behaviors which would indicate a spam attack. These patterns and signatures can be used to stop a targeted spam or phishing attack in its tracks—right at the targeted enterprise gateway. The pattern files can then be shared with all enterprises through a cloud-based repository of information. And with a global system of correlated threat data, all customers are better protected from spam outbreaks compared to an email security appliance sitting alone at the network edge. In particular, enterprises benefit from much needed zero day protection against emerging threats.

CLOUD SERVICE FOR ANTISPAM

To counter the need for dedicated on-premise hardware and support, many customers are looking to cloud-based antispam solutions to avoid these resource costs, routing their email messages through a third party for scanning before they are delivered into their infrastructure. Cloud-based services are designed to be on-demand and elastic in order to provide flexibility in both, cost and scalability, as well as having a centralized team of mail security experts to ensure that the solution employs the latest antispam techniques to maximize detection rates. Enterprises can, and should, leverage the cloud to provide a first line of defense for spam filtering.

Best practice tip:

For any antispam solution to be effective, it should be granular enough to allow different policies and sensitivities to be applied to different domains or groups of domains as they are likely to have differing requirements.

Best practice tip:

A gateway email security solution should leverage machine learning for phishing and spam outbreak prevention. Gateway email security should be part of a larger threat intelligence community, so that there is global threat intelligence sharing.

Best practice tip:

Using a cloud service to block a high proportion of emails before they reach the customer’s network, drastically reduces resource utilization in both the customer’s email servers and internet connection. This service should be backed by an aggressive Service Level Agreement (SLA).

THE SPAM SCRAMBLE

EVER-GROWING SPAM VOLUMES DEMAND A NEW APPROACH TO EMAIL SECURITY

VI. THE INDUSTRY'S FIRST HYBRID EMAIL SECURITY: INTERSCAN MESSAGING SECURITY VIRTUAL APPLIANCE

Trend Micro has developed the industry's first integrated hybrid SaaS email security solution designed to provide the benefits of both a cloud-based solution (to remove a high percentage of messages within the cloud), and an on-premise VMware Ready virtual appliance (to give an enterprise the fine level of policy enforcement that they require and the privacy they prefer). With this hybrid solution, enterprises can minimize outlay on expensive dedicated appliances and also leverage the latest virtualization technologies.

LAYERED SECURITY MANAGED FROM A SINGLE CONSOLE

These components are linked transparently, one in the cloud to remove a large percentage of unwanted inbound emails, and another on the enterprise premises, for more granular policies and policy/privacy enforcement of outbound email. This greatly simplifies the configuration process for the enterprise since both cloud and on-premises components are managed from a single console. In addition, the solution queries its local message tracking logs, and searches the cloud component of the solution for the equivalent logs. A single set of results are shown, combining both local and cloud results into a single log.

FIRST LINE OF DEFENSE: EMAIL REPUTATION AND WEB REPUTATION

InterScan Messaging Security Virtual Appliance employs email reputation, web reputation, traffic shaping, and heuristics—to weed out unwanted content before it hits the network edge. These technologies leverage unique cloud-client architecture, powered by the Trend Micro™ Smart Protection Network™, a global network of threat intelligence sensors. Email reputation policies stop mail sent by known spammers—blocking up to 85 percent of all email. Meanwhile, web reputation blocks emails with links to infected or malicious websites. Email, web, and file reputation threat data is correlated by the Smart Protection Network in the cloud to stop threats as soon as they emerge. As the volume of threats increases to thousands per hour, the need for comprehensive, immediate and correlated threat intelligence is critical to protecting your enterprise.

PRIVACY AND CONTROL WITH ON-PREMISE SECURITY

Emails flagged for further inspection are quarantined on premise; no email is stored in the cloud—none. Inbound email security layers including DHA protection, machine learning, and granular content filtering controls are also available on premise. In addition, outbound content inspection, spam and virus filtering, and encryption secure outbound content and provide early detection of bot activity.

THE HYBRID SOLUTION ALIGNED WITH ALL OF TODAY'S ANTISPAM BEST PRACTICES

The hybrid email security approach within InterScan Messaging Security Virtual Appliance removes many of the obstacles for enterprises that desire the benefits of both an in-the-cloud solution and an on-premise solution. And the benefits are significant, including lower management overhead and better alignment with antispam best practices as discussed within this document. The results set a new standard in terms of greatly reducing the volumes of spam received by the enterprise—without interfering with business critical emails.

© 2010 Trend Micro, Incorporated. All rights reserved. Trend Micro, InterScan, Trend Micro Smart Protection Network, and the t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. WP03_Spam_100824US