

Astaro OrangePaper

The Hidden Dangers of Spam: How SMBs can confront security risks and restore productivity

Author: Eric Bégoc

Astaro Product
Manager



Date: 2008-11-27

Content	Page
Executive Summary.....	2
A New Generation of Email Risks	2
The Scope and Cost of Spam	5
Efficient Spam Protection	6
Identifying Spam Accurately	7
Boosting Accuracy: Fingerprint and Reputation Based Service.....	8
Managing Spam	10
Astaro's Enterprise Class Spam Protection for the SMB	11
Capabilities for Businesses of Every Size.....	12

Executive Summary

Beyond the well-understood productivity drain that spam inflicts on businesses, threats posed by illicit email circulating through a network are causing many security professionals to rethink protective measures. Staff members sometimes unwittingly unleash security threats by simply clicking on a greeting card link, opening a mail attachment, or previewing a message that contains a malware script. Spam is more than a nuisance—it is often a vehicle for hackers and fraudsters to bridge network defenses and release dangerous payloads inside the network.

Enterprise-scale organizations often protect themselves against illicit email intrusions with elaborate gateways, using expensive and complex screening techniques. Small and mid-sized businesses (SMBs) however, sometimes leave themselves open to risks—largely because they lack the resources to implement countermeasures. Mail gateways scaled to the needs of smaller businesses offer a means to combat spam, mitigate security risks, and restore productivity to companies grappling with an influx of illicit email.

A New Generation of Email Risks

Anyone who has ever returned from vacation to confront an inbox overflowing with hundreds of email messages, most of them spam, knows firsthand the productivity drain this form of communication can present. IT administrators wrestle with this problem daily and as fast as they implement solutions, new challenges arise. Email is indispensable to modern business operations, but to be useful it has to be both safe and convenient. The nuisance of spam is substantial, but enterprising hackers using email to breach the security of the network are more than a nuisance. Emerging security risks are becoming more common as hackers discover innovative ways to use a simple email message to deliver a virus, worm, a malicious script, a phishing link to a fraudulent site, or an attachment that triggers a form of malware.

The scope of the spam challenge is enormous. The Department of Internal Affairs in New Zealand¹, citing recent worldwide estimates, says that each day approximately 120 billion spam messages are generated and distributed. This represents a 100 percent increase over the volume last year. To complicate the situation, spam techniques are shifting to target new vulnerabilities and to

¹ Source: http://www.dia.govt.nz/DIAwebsite.nsf/wpg_URL/Services-Anti-Spam-Index

exploit different file formats, such as image files, Adobe Acrobat files, MP3 files, and other formats.

In Q2 2008 spam levels averaged at 77%

The resourcefulness of attackers using spam reached substantial levels during 2008. The Commtouch Q3 2008 Email Threats Trend Report² noted that spam levels averaged 77 percent of all distributed messages during Q3 and reached as high as 94 percent. Waves of botnet attacks relying on zombie IP addresses and new forms of attachment spam continued to be a problem. The Storm peer-to-peer botnet, seeded by the Storm worm, proved particularly difficult to combat because it can outmaneuver real-time blacklists, skating between an extensive series of networks by using dynamic IP addresses.

Botnets, because of their distributed nature and use of dynamic IP addresses, present a growing challenge to administrators—one which is best met by employing a security solution capable of detecting and deflecting many categories of malicious operations in real time.

Threats associated with eCards during the holidays also proved particularly difficult to identify, masking their content in seasonal greetings. The content often included a link to a site where Trojan software would be downloaded to the unsuspecting card recipient.

Only recently have mail security products evolved to the point that they can successfully defend against the wide range of threat scenarios. In addition, only the most advanced security products are able to counter sophisticated botnets, deceptive phishing attacks, and new attachment techniques for smuggling spam past network boundaries.

² Source: http://www.commtouch.com/documents/Commtouch_Q208_Email_Trends.pdf

Fateful Fred – Experiences In Spam

Within the first month of taking a position at Digby and March Financial Services, Fred Baldwin managed to jeopardize the security and privacy of the corporate network with careless email activities. Tasked with compiling a report about the current job priorities of members of his workgroup, Fred had a question about the report for his supervisor, who happened to be vacationing in Barbados. To the astonishment of his supervisor, Fred sent him an interim version of the report, which included network usernames and passwords, by unencrypted email. His supervisor promptly admonished Fred about the privacy risks of email messages.

Depressed by this mistake, Fred was browsing through his personal email folder and came across a message with the subject line reading "A Friend Has Sent You a Mystic Greeting Card." The message in the card didn't identify a sender, but provided a link, which Fred quickly clicked on, since he was curious about who might have sent the card. Instead of a card, the link opened up a Web page that appeared to display Russian characters, but in a couple moments his screen went blank, and he wasn't able to reboot his computer. Within a couple hours, no one in his workgroup had an operating computer, and the IT administrator was walking from cubicle to cubicle trying to learn what had happened.

Fred explained how he had followed the greeting card link and what had happened. Fortunately, the worm that was downloaded and released into the network from this link was detected by a neighboring employee, who happened to be running an up-to-date virus package. The administrator quickly took measures to purge the network of the worm, but several hours were lost while the network was shut down to prevent further spread of the worm.

Cautioned against following links or opening questionable email, Fred slipped up again a few days later, though in this case he didn't even open the message in question. He was scanning the messages in his inbox and came across one with a subject line reading "Make More Money Than You Ever Dreamed Possible." Curious, he opened up the preview pane of his mail program to scan the HTML-formatted message, which unfortunately triggered a malicious Java routine embedded in the HTML—something that Fred had not protected against in his email options. The routine quickly gathered the contents of his address book and sent out 233 messages, each containing a hidden botnet script, which would likely be opened when the message recipients recognized his name.

"I didn't realize email could cause a problem if the message wasn't opened," Fred confessed to the visibly angry IT administrator (who had received one of the botnet payloads).

The Scope and Cost of Spam

Ignoring spam can be expensive

Companies pay a steep cost if they choose to ignore targeted email attacks and spam—both from a productivity perspective and a security standpoint. Any way you analyze the problem, the costs clearly indicate the need for selecting and deploying a means to keep illicit email outside the organization's network.

According to a report on the rising costs of spam compiled by Nucleus Research³, as far back as 2004 the average cost of spam per year per employee equaled 1,934 USD. The report further cited the average lost productivity annually for each employee as 3.1 percent and the average number of spam messages received reaching 7,500 (more than double the previous year).

Calculating the Impact of Spam

To more precisely calculate the impact of spam and determine the return on investment (ROI) of a particular anti-spam solution, Commtouch provides a dynamic online tool, the Spam Cost Calculator (<http://www.commtouch.com/site/Resources/calculator.asp>), that lets users enter applicable values for their company and receive immediate feedback on the costs of spam in their environment. Storage costs, productivity costs, and annual enterprise costs are factored into the results. For example, for a company of 250 employees with an average annual salary of 50,000 USD, with each employee receiving 60 email messages a day, averaging 40 percent spam, the following costs apply:

Direct lost productivity costs to enterprise: 72,385 USD

Overall cost of responding to spam: 43,870 USD

Overall annual storage cost to enterprise: 21,025 USD

Total annual cost to the organization: 137,280 USD

The tool also includes an ROI calculator. Users enter the cost of a particular anti-spam solution and the interest rate that applies. The calculator returns the number of days before the investment pays for itself by reducing the costs associated with lost productivity and storage requirements.

³ Source: <http://nucleusresearch.com/news/press-releases/2nd-annual-spam-report-cost-of-spam-more-than-doubled-in-past-year-to-1934-annually-per-employee/>

Efficient Spam Protection

*New spam techniques
require an efficient
security approach*

The many and varied techniques employed by fraud artists, particularly with the rise in merged and hybrid attacks that use email, web sites, and malware to deceive the victim, demonstrate the need for a comprehensive approach to security. Solutions that rely on software installed at the end point, such as virus protection or spam filters, must be maintained across the entire universe of an organization's computers and must depend on end users not disabling or circumventing them.

A more efficient approach is the security gateway, which can be equipped to detect and eliminate a wide range of incoming threats—from attachments containing worms, key loggers, or malware to messages associated with phishing sites or known botnet operations. The gateway provides a direct and defensible centralized point from which an organization can implement a range of security measures—filtering and removing harmful email and burdensome spam before it ever reaches the target recipient. Only with gateways sitting on the perimeter of a corporate network it is possible to reject spam messages during connection time, efficiently preventing transfer of unsolicited and potentially harmful data to the local network.

Besides the careful choice of the best way to fight spam and malware, methods have to be found that cope with emails which are not rejected at connection times. For example, messages that can't 100% accurately be detected as spam need to be quarantined. To keep quarantining efficient and allow a swift overview and access to quarantined messages, attention has to be turned on quarantine management concepts and especially how end-users can be provided with means to self serviced spam management.

Identifying Spam Accurately

Numerous approaches exist for identifying spam and illicit mail senders. Given the variety of formats and approaches used by spam practitioners and fraudsters, an organization using a wide variety of detection techniques can more accurately identify and filter out messages that are likely to be spam. The methods for countering spam fit into two general categories: traditional techniques (that rely primarily on lists and source identification) and next-generation techniques (that use analytics and pattern recognition to rapidly detect and isolate suspicious messages).

The most common traditional techniques for countering spam include:

- **Advanced Greylisting**

This technique causes each incoming message to be met with a defer command by the gateway, causing a valid mail server to queue the message for re-delivery within a few minutes. When the message is seen again, the sending mail-server is added to the greylisting whitelist. This technique is effective because spammers typically do not deal with the backscatter from their spam blasts, so the spamming software will not try again later like a legitimate mail server does.

- **Bounce Address Tag Validation (BATV)**

BATV provides a definitive solution against a spam technique where spammers send messages to end users as legitimate "bounce" mail. This method can be defeated by embedding a code in outgoing messages. If the signature is not present in a bounced message, it can be determined that the message was never sent out in the first place and is not legitimate.

- **Sender Policy Framework (SPF) record checking**

SPF functionality allows to match sender domains and mail servers with officially published mail server information by adopting companies.

- **Reverse-DNS (RDNS) checking/HELO command in SMTP**

Of significant impact is this check which greatly reduces spam at a very low resource cost. This feature does basic checks on a host's "identity" by evaluating its IPv4 address and HELO string via DNS and syntactic checks, since official and valid mail servers adhere to certain rules and formats. When activated, this feature rejects SMTP RCPT commands if the calling hosts are not abiding by official formats, which is very common amongst spammers.

- **Other techniques**

In addition to the technologies listed above, long-standing, effective techniques that have been successful at fighting spam, such as Realtime Black Lists (RBLs), manually configured whitelists, recipient verification or sender address/domain/IP/network blacklisting complete the list of traditional techniques.

These techniques provide useful baseline spam recognition and can contribute to minimizing the spam on the network and illicit messages reaching users' inboxes. As these techniques don't rely on analyzing the actual content of an email message but on header information only, they can drop connections even before the messages are fully transmitted. Not only does this reduce network bandwidth but also it reduces valuable processor resources of the gateway itself.

However, not all spam messages can be blocked through above techniques as for some type of spam the message content has to be considered in the analysis. Common content recognition approaches based on word lists or self-learning engines (Bayes) are not the most efficient solution here as well, as they are usually hard to maintain and require significant gateway resources for detailed analysis of the whole message content.

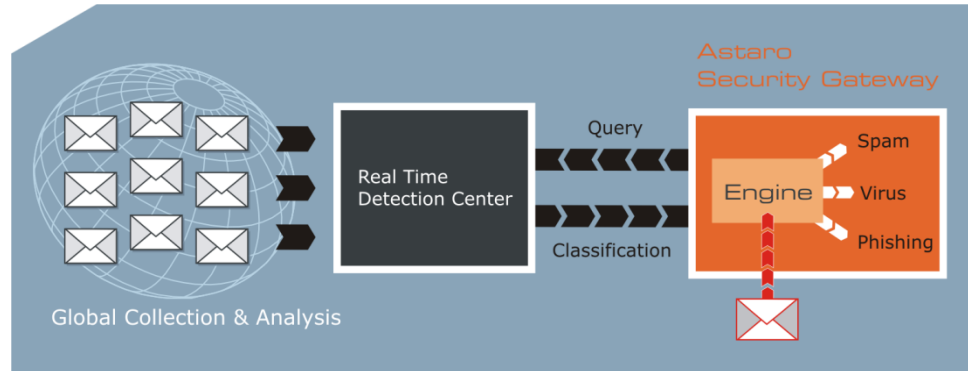
Boosting Accuracy: Fingerprint and Reputation Based Service

*Centralized spam
outbreak detection
in real time*

Next-generation techniques are rapidly gaining favor among IT administrators who want to eliminate these kinds of spam. One approach is to use strategically located collectors at major ISPs and thousands of deployed scanning devices to gather global information via billions of messages. By using this patent-pending Recurrent Pattern Detection (RPD™) technology, this information is then analyzed in real-time to rapidly identify spam outbreaks and spammer trends, generate spam fingerprints, identify sources of spam and create a centralized reputation database of email senders around the world.

Using these fingerprinting methods, this unique content-agnostic technology detects and blocks spam in any language and is highly effective against various types of attachment spam (including images or PDFs), as well as blended spam/malware threats. This advanced spam engine allows for much higher message throughput than scanning individual each message for content and working with a resulting points system.

Another advantage is that by using this new spam detection techniques, solutions generate far fewer “false positives” where for email messages addressed to single individual recipients, the false-positive rate can even drop to zero.



Spam Classification with Recurrent Pattern Detection

A technique for identifying and blocking phishing attempts should also be an integral part of any effective anti-spam solution. Phishing involves sending messages that appear to be from legitimate institutions, but are actually from masquerading fraudsters trying to obtain sensitive personal data, such as social security numbers, bank account numbers, and other confidential information. As is the case for countering spam, countering phishing attempts, generally requires multiple means of identification, including detecting suspicious phishing servers, correlating patterns of phishing content, and scanning message content to detect signatures associated with phishing attacks.

Managing Spam

Even if today's anti-spam techniques are evolving and getting even better, no solution or product exists that can be 100% accurate on spam detection. This makes spam management an important part of any solution that addresses the challenge of spam on the company network.

The choice of management techniques can have a substantial effect on productivity—both at the administrative level and at the end user level. The optimal approach for spam management should have these characteristics:

- Flexibility to adapt to various work environments without onerous restrictions
- A design architecture that minimizes spam traffic on the network and reduces storage requirements allocated for unwanted messages
- A management approach that requires minimum time from email users and administrators to deal with sorting and deleting suspected spam messages

One common technique that is used for spam management in anti-spam applications is to simply flag an email message that appears to be spam and then pass it along to the user's inbox. This approach does not help reduce network traffic, since messages are distributed in the same manner as legitimate email, nor does the approach help reduce storage requirements. Similarly, anti-spam solutions that quarantine spam on the user's local storage still circulate volumes of spam across the network.

Centralization alone is not enough

A centralized, gateway approach to spam management does a much better job of keeping spam off the network and consolidating it in a single area, generally a quarantine database, where it can be further screened and examined. Some anti-spam solutions require that the administrator bear the burden of inspecting the contents of the quarantine area and determining the disposition of the messages. A far better option is to offer the user a portal to the quarantine area so that they can individually inspect messages and release messages that are wrongly filtered (false positives).

Keeping users apprised of the current status of suspected spam messages sent to them is another means of simplifying the management tasks. This can be done by generating periodic reports to email users so they remain informed about the status of messages that have been quarantined. Users can then use the portal at their convenience to inspect the messages.

Combining multiple techniques for identifying spam, including both traditional and new methods together with a centralized architecture effectively keeps spam off the network and gives users and administrators streamlined methods for screening and disposing of spam.

Astaro's Enterprise Class Spam Protection for the SMB

With a strong understanding of the unique requirements of the SMB, Astaro offers integrated all-in-one solutions to address email, web, and network security challenges. These solutions, packaged in easily deployable frameworks—including hardware appliances, virtual appliances, and software appliances—can be quickly implemented by IT groups. IT groups realize the solution benefits immediately, without lengthy training sessions, complex ongoing maintenance tasks, extended installation scenarios, or difficult integration into the company infrastructure. Astaro Mail Gateway offers this flexibility and ease of use while targeting a wide range of productivity and security issues, with features that offer multi-layer spam recognition, malware protection with dual virus scanning, built-in email encryption (S/MIME and OpenPGP) and Remote Exchange Access (SSL VPN).

“Our aim with AMG is to offer the established and award-winning email defenses of our unified threat management (UTM) solutions in a dedicated email security appliance,” said Astaro co-founder and CSO, Gert Hansen. The Astaro Mail Gateway fits effectively into the full line of products developed by Astaro to deliver cost-effective, unified threat management capabilities to businesses ranging in size from small- to enterprise-class. By using an appliance approach Astaro can provide security solutions that can be quickly deployed and easily administered through centralized controls. Astaro Mail Gateway can also fit into an environment containing other Astaro solutions, including Astaro Web Gateway and Astaro Security Gateway. All of these gateway products can be centrally administered using the central management appliance, Astaro Command Center, providing a comprehensive and easily managed security solution for customers.

The spam recognition Astaro Mail Gateway provides, is based on multiple techniques including Advanced Greylisting, BATV, SPF, RBL, whitelists, recipient verification as well as Recurrent Pattern Detection. While the spam rate the gateway will recognize is unmatched, it still comes with a broad range of options to manage spam. Besides basic options as flagging spam and sending out

multiple spam user reports daily, Astaro Mail Gateway also provides end user self-service portal which is available in 15 languages.

Capabilities for Businesses of Every Size

Email is central to the operation of every modern business today, but to be able to enjoy its benefits and guard against security threats, all email communication must be examined for spam and malware, and subject to the most advanced forms of security protection available.

A mail gateway provides a practical and effective means to accomplish this, and the Astaro Mail Gateway brings many of the sophisticated protections and spam management mechanisms that enterprises use to small to mid-sized businesses that may be lacking any type of centralized security or privacy measures. With the added benefit of built-in, transparent encryption, the Astaro Mail Gateway helps fulfill many of the regulatory mandates in force in different geographies around the world.

Relying on end users in an organization to do the right thing is a dangerous proposition. Far too many computer users fall prey to deceptive web links embedded in messages, appeals from phishing sites, tempting attachments that are poisoned by malicious scripts, and similar threats. By setting up a centralized mail gateway, these kinds of risks can be substantially reduced. Astaro Mail Gateway copes effectively with spam, includes strong security protections, and installs easily as a hardware appliance or virtual appliance. Mail security is too important to be overlooked—whether an organization has 10,000 employees or 100.

Contact



www.astaro.com

Europe, Middle East, Africa

Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germany
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

The Americas

Astaro Corporation
3 New England Executive
Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia Pacific Region

Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Japan
T: +81 3 4360 8350
apac@astaro.com

This document may not be copied or distributed by any means, electronically or mechanically, in whole or in part, for any reason, without the express written permission of Astaro AG.

© 2008 Astaro AG. All rights reserved. Astaro Security Gateway, Astaro Command Center and WebAdmin are trademarks of Astaro AG. All further trademarks are the property of their respective owners. No guarantee is given for the correctness of the information contained in this document.