MediaBUZZ's 2nd Anti-Spam Event

SPAM - the never ending story

October 23, 2008

Is spam making a greater comeback now than ever? What does the current spam and email security market look like in the Asia Pacific? Do you know why spam is more than just a nuisance? Are spam filters losing their effectiveness? What more can be done to fight spam? What exactly is 'false positives'? Is anti-spam legislation an effective enough deterrent? What will next-generation spam look like?

Get answers to these questions and read on how to defend your organization even more and better from spam.

Get insights into anti-spam trends and measures from industry experts like:

- Arun Chandrasekaran, Industry Manager Enterprise/ICT Practice Asia Pacific, Frost & Sullivan
- Donald Teo, Regional Manager (Asia) Tumbleweed (now part of Axway)
- David Chow, Sales & Channel Enablement Manager Asia, Sophos
- David Habben, Regional Manager, Asia, Proofpoint Inc.
- Manish Goel, Chairman of the International Committee for AOTA (Authentication & Online Trust Alliance)
- And more ...

SUPPLEMENT CONTENTS	Page

SPAM - the never ending story

Combating the latest inbound threats: Spam and dark traffic

One threat that is always high on email administrators' radar is spam. There are many anti-spam solutions on the market today, but the target is constantly moving: spammers get more clever and creative to get their junk mail to look real, and anti-spam vendors must constantly update their techniques to remain effective. It's a game of "spy vs. spy": spammers are constantly learning how to get around specific anti-spam techniques, and the best vendors are always coming up with new technologies to increase the percentage of spam caught.

For instance, some anti-spam vendors rely on identity analysis or reputation analysis to block spam coming from certain IP addresses. To get around this, spammers have now implemented zombie attacks or botnets (robot networks), planting spyware or Trojans on unsuspecting machines, which then work as slaves to remote machines, which then carry out a spam campaign. Instead of one machine sending out tens of thousands of emails from a single IP address, zombie attacks can have a thousand slave PCs—and a thousand different IP addresses—sending out ten to twenty emails each. Effective email security requires vendors to constantly add adaptive techniques to their anti-spam systems, assuring organizations that even new threats like zombie attacks won't get through their systems—and email security professionals don't get those angry calls or emails about unwanted messages.

Today's enterprises expect spam filters to catch at least 95% of spam; the best spam filters catch upwards of 99% of unwanted emails. Even more importantly, however, spam filters should rarely catch a valid, wanted email and throw it out. These "false positives" have caused many arguments between companies when an expected email has been filtered out and never delivered. Experts recommend that the false positive rate be as close to 0% as possible, since false positives can cost organizations dearly.

Spam is not the only threat to email servers. While spam is unwanted and often annoying, a bigger threat to networks today is malicious and invalid email traffic, referred to as Dark Traffic, which can actually damage an email system or a network. Dark Traffic includes viruses, worms, and Trojan horses that are sometimes attached to otherwise valid-looking emails. The directory harvest attack (dHA) is often a precursor to spam, when a corporate email server is bombarded with thousands—or even millions—of random name combinations in order to determine valid email addresses. Email denial of service (doS) attacks, malformed SMTP packets, and invalid recipient addresses are other types of dark Traffic. As mentioned above, spam and dark Traffic can have a huge effect on bandwidth, often representing 70-90% of all inbound email traffic. Stopping spam and dark Traffic is essential to scaling email infrastructure accurately and keeping network performance up.

The evolution of Anti-Spam Technologies

Spammers and hackers are constantly shifting strategies and tactics to get around spam filters. As new tactics evolve, anti-spam vendors must layer their new technology on top of the old. The following are the four major types of anti-spam technologies:

- Content filtering. Early solutions relied primarily on word lists, email signatures, and lexical analysis. For instance, "Viagra" is a word that's often tagged by content filters. To adapt, spammers started spelling it with "1"s instead of "I"s, and added spaces. Later, they began to include HTML graphics instead of putting in text. Recently, spammers began to put their content in embedded PDFs; some email security vendors can filter the content of PDFs as well.
- Behavioral analysis. This type of anti-spam technology used Bayesian analysis, statistical analysis and heuristics in order to predict spam. The onus for this type of technology often fell

continues on Page 3

SPAM - the never ending story

From Page 3 — Combating the latest inbound threat: Spam and dark traffic

on administrators, who had to do extensive tuning and trial and error before getting satisfactory results. Bayesian filters also increased the likelihood of false positives.

- Identity analysis. This looks at the identity of known spammers (often referred to as "reputation analysis.") This is a promising technology, but may require email authentication to become more widespread. Also, zombie attacks can get around this type of defense.
- Pattern detection. By analyzing patterns of traffic, as much as 80% of traffic can be thrown out as invalid. This reduces the load on email servers and downstream email filters. This type of detection also does not add to the rate of false positives.

All these technologies can layer on top of one another to create an effective anti-spam filter. However, organizations need to implement a secure messaging solution that takes the encryption burden of the end users and intelligently does the right thing.

Policy-driven control and content filtering

Security policy is increasing in both use and importance in today's business environment. Government regulations, as well as the high amount of responsibility and enormous workload given to IT professionals, make it much more efficient to implement a policy-driven framework for security.

The first generation of email solutions simply dealt with email coming into an organization. Most anti-spam products rely on content filtering, but its importance is expanding. It's no longer enough just to look at the text in a message. Inbound threats can be hidden in message text, headers, HTML graphics, and various types of attachments.

However, email traffic encompasses outbound emails as well. To deal with regulations and security concerns, organizations' security policies have begun to address outbound issues. Email systems make it so easy to send messages that employees can send proprietary information, customer information, or accounting information to anyone, at any time—and send it unencrypted.

This could expose organizations to many risks, whether or not the employee is sending the email legitimately or not. For instance, if an accounting employee needs to send private accounting information or customer data to an auditor, those emails could be violating government regulations if they're not protected properly.

How can organizations be sure that employees are complying with government regulations, or that a disgruntled employee isn't sending intellectual property or a customer contact list to a competitor? There could be serious implications if the wrong information gets in the wrong hands due to an unprotected email system.

It's becoming increasingly clear that inbound and outbound email security techniques are linked, especially in content filtering. Identifying keywords, file types, HTML graphics, attachments, headers, and junk traffic are essential for both sides of the email perimeter. Today's email security solutions often leverage the same inbound content filtering technology for outbound email. Rules can be created that flag proprietary data, social security numbers, or other personally identifiable information. Certain recipients, such as auditing firms, can also have their emails flagged.

The next generation of email security solutions must make policy management and content filtering as robust as possible to adequately address all customer concerns. For instance, some vendors don't scan some types of attachments, like PDFs, that can be at high risk for confidential information; other vendors only deal with inbound emails, and have lightweight or hard-to-manage solutions for outbound traffic. Therefore, it's becoming essential to apply similar security technology used for inbound email traffic to outgoing emails.

Best practices for securing outbound messages

Email encryption protocols such as TLS, PGP, or S/MIME have existed for some time, but the process of deploying encryption has developed a well-earned reputation for being difficult, complex, and prone to failure.

continues on Page 4

SPAM - the never ending story

From Page 3 — Combating the latest inbound threat: Spam and dark traffic

However, the need to encrypt sensitive information can't be ignored. Organizations need to implement a secure messaging solution that takes the encryption burden off the end user and intelligently does the right thing to keep messages secure and organizations in compliance.
In other words, it needs to analyze who it's from, what it contains, and where it's going, and take appropriate steps automatically.

Experts strongly recommend the following features for an effective outbound security solution:

1. Strong content filtering
2. Flexible and intuitive policy controls
   - Effective solutions should take policy actions and route mail based on policy
   - Policies should be granular: identity of sender, identity of recipient, matching keywords, attachments, etc.
   - Multiple options should be available: blocking, encrypting, adding a disclaimer, etc.
   - Easy to implement: should be an intuitive GuI instead of a Unix command line
   - out-of-the-box lexicons for common government regulations (such as HIPAA, GLBA)
3. Multiple outbound delivery methods
4. Universality
   - Any recipient should be able to receive an email that's been properly secured
   - Recipients should additionally be able to securely respond to the email

Integration and consolidated management

If not addressed properly, the security and architectural challenges discussed above can cost companies hundreds of thousands of dollars in unnecessary infrastructure costs and lost productivity, as well as the consequences of noncompliance or compromised confidential information. Disparate solutions have been available to address some of these challenges in the past, but increasingly, email administrators are looking for consolidation and simplified management.

Point solutions are not the answer

Many companies have deployed point solutions that just take care of a single email problem. Anti-spam and anti-virus solutions that check email can be deployed at the user level or as an email plug-in. But this type of approach is rarely part of an overall security strategy, and often leads to gaps or overlaps in email security. Additionally, most of these one-off solutions have different management interfaces, which can lead to high administrative cost and effort.

As email security threats evolve, point solutions are often not worth this extra layer of management, since they only deal with a single email threat, and often only using a single method for defense. Spam, in particular, has evolved past what many point solutions can handle, making the products essentially ineffective.

Enterprises now expect email security solutions to deal with many different security threats, including all the types of dark Traffic that can eat up so much bandwidth. In addition, the defending solution should be multi-layered, using different approaches and technologies to protect against evolving threats. If this type of solution is implemented, organizations can be confident that they will be quickly protected against new types of dark Traffic as they emerge.

Leverage and simplify

Email management can be difficult with many different products. Not only can inbound and outbound security leverage the same technologies, but administrators also want to use the same management console to simplify their work and increase effectiveness.

Gateway filters leverage inbound and outbound email security with ease of management. This provides administrators with the highest level of control, can perform both inbound and outbound security tasks (depending on the solution), protects against all types of dark Traffic, and saves the most bandwidth.

Although they have architectural advantages, not all gateway email solutions are easy to manage.
Some gateway vendors simply partner with third parties for parts of their solution. This isn't a problem if the integration is done well and customer

continues on Page 5

SPAM - the never ending story

From Page 4 — Combating the latest inbound threat: Spam and dark traffic

support is seamless to the organization, but that's not always the case.
Some providers offer more features as part of their core offering, and these solutions tend to have integrated functionality, more streamlined support, and more complete management consoles.

Any email security solution should offer consolidation of services and multiple functions, as well as a single, centralized management tool and centralized reporting. This makes every administrator's job easier.

The demands of today's enterprises are driven by new government regulations and changing business requirements. Organizations can choose from a new generation of email security solutions that meet the requirements to pass the "administrator invisibility test" much better than first-generation solutions.
In order to meet these requirements, complete email security solutions should provide:

- Seamless integration of multiple security functions
- No need for fine tuning or adjusting of spam and virus filters – these should be handled by outside experts
- Intuitive and effective policy controls
- Deep inspection of all content and attachments
- Integrated outbound secure delivery
- Centralized control over inbound and outbound security

Email revolutionized the way organizations conduct business, and the next-generation email security solutions continue to build on those advantages. While choosing the right email solution may not change the way businesses communicate, it will deliver dramatic savings—not just in the areas of budget and infrastructure, but also in the time and resources of IT professionals and their organizations.◊

Condensed from a whitepaper by Tumbleweed, now part of Axway

Click here to return to the contents page

SPAM - the never ending story

Know what to do when spam is in your Inbox

Generally speaking, most of us can spot spam in our Inbox. However, what you do when you do spot spam can affect how much more follows it.

Here is what to do if you spy spam in your Inbox:

Don't open it.
In particular, don't open attachments that you are not expecting. Viruses often spread by hijacking the email list of affected computers. So just because you recognize the sender doesn't mean the email, or its attachment, are legitimate.

Remember the phrase "I see you".
Pixel tracking is a once legit method now used to verify and track active email accounts. It involves embedding an image from a Web server into messages. If your email reader supports HTML messages, then upon opening one with an image, your IP address is recorded on the sender's web server access logs. Since the image filename is possibly tailored for you, they'll also know your email account is active. Fortunately, some email clients automatically suppress images unless you turn them on for a given message. If you do want to take a look at a picture sent in a questionable email, try to view messages while you are offline, or turn off the receipt of HTML messages.

Don't purchase anything from spam emails.
Never buy anything from link in a spam email. If you do, you can assume your details will be passed around to others.

Return to sender: ignore false no-delivers.
Beware of spam with a subject line suggesting your email was undeliverable. Simply ignore them.

Groupthink.
Beware of spam implying you are subscribed to some newsgroup. You'll usually get 3-10 messages simultaneously with similar subject lines and content, but supposedly from different people... extremely sly.

Paved with good (and bad) intentions.
In addition to spam sent illegally, there are a surprising number of spam emails sent by legal and legitimate organizations.

This includes:

- **Government Approved**
  Although most governments have started to clean up their acts, there is little doubt that there are still some forms of government sponsored spam still being propagated. Do note thought that governments and subversive organizations might bury legit messages within apparent spam.
- **Testing, testing, spam, two, three**
  Email security firms may release innocuous spam as part of experiments to see how people respond. This spam does no real harm, but it can still be annoying.
- **In the name of education**
  Computer Science students have been known to imitate spammers in order to get material for their theses. Again, this student sent spam is innocuous, but it still clogs up your email account.◊

Click here to return to the contents page

SPAM - the never ending story

Frost & Sullivan: Do not underestimate spam

Spam is definitely a problem that enterprises will do well to take heed of, mainly due to firstly, the embedded threats which may come via spam mails these days, be it viruses or spyware and secondly, the amount of valuable bandwidth it takes up which affects the overall speed and efficiency of a corporate WAN setup. A third reason why spam is much more than a nuisance says Arun Chandrasekaran, industry analyst, Frost & Sullivan, is due to the loss of employee productivity in dealing with spam.

"The evolution of spam from mere nuisance emails to the spam of today carries with it a greater capability and propensity for different types and forms of threats to be embedded within. Indeed, the common mistakes made by businesses/users these days is to underestimate the level of threat posed by spam towards their corporate networks, in particular, the possibility of spam acting as a vehicle for malicious threats to intrude into their company's network. In addition, spam may also create an indirect adverse effect on employee productivity by choking up the company's bandwidth pipes, thus resulting in system lag and affecting various business processes," he elaborates.

Commenting on why spam is and will continue to be a never-ending story Chandrasekaran continues, "With the email emerging as the key business communication tool in the IT era, it is definitely attracting a fair amount of attention from spammers looking to infiltrate corporate networks via the email gateway, as well as becoming a convenient way through which organizations can spread their marketing messages. As a key enabler of connectivity in an increasingly globalized world, the email medium is likely to continue being manipulated by parties looking to leverage on its widespread usage and popularity. With the cost of sending Spam being almost zero, it is never going to vanish soon."

In addition, spam is more dastardly than many people realize.

In fact, according to Chandrasekaran, there has been a shift in the nature of spam, with threats becoming harder to detect these days, as they move from text and html-based platforms to PDF spams and spoofed NDR messages. Increasingly, the definition of spam is moving towards a contents-based classification, whereby threats could come from an innocuous-looking email which becomes otherwise once the receiver opens up the email. As for what lies ahead, "The near future is likely to witness greater convergence between email and web-based threats, with spammers looking to hide their true intentions behind the façade of a legitimate looking web address sent via an email," shares Chandrasekaran.

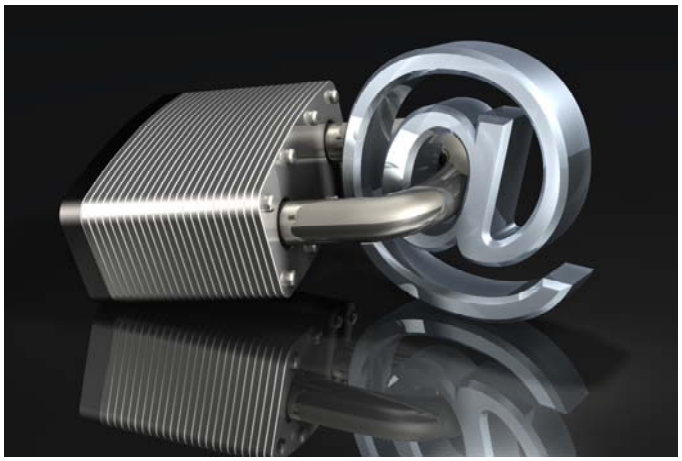
The Asia Pacific has of course, not been spared from the onslaught of spam. Although the cultural and language diversity inherent in the region has meant that the English language spam has not yet impacted countries where English is not the first language, such as Japan and China, nonetheless, in recent years, there has been a rising penetration of non-English spam in the region, with many countries emerging as spam relaying stations in the process as well. Also, the proliferation of botnets in Asia and it being used as a vehicle for spam has seen dramatic increase in spam originating out of Asia.

One key driver for the rise of spam in the region is the lack of compliance in the area of content security, with many governments in the region still exhibiting a relatively immature mindset towards the perils of email security breaches. Moreover, many emerging markets in the region, such as Vietnam were late in fully embracing the IT revolution, thus resulting in a delayed reaction to the notion of email security and spam. However, with IT integration in businesses rapidly ramping up, compliance concerning email security is expected to expand accordingly, as governments and enterprises look to protect their IT assets amidst an increasingly sophisticated threat landscape.

continues on Page 8

SPAM - the never ending story

From Page 7— Frost & Sullivan: Do not underestimate spam



Chandrasekaran believes that legislation definitely helps in contributing to the war against spam. “However, introducing compliance without a fitting enforcement strategy will also lead to nowhere. Nonetheless, the first step for governments across APAC is to introduce compliance concerning email security, so as to increase public awareness towards the problem of spam and drive greater adoption of the relevant solutions,” he says.

A key characteristic of spam is its ability to evolve fast and keep up with the current times. Commenting on the latest spam trends as well email protection systems, Chandrasekaran observes, “We definitely see a drive beyond spam in the past year, as more enterprises begin to take a closer look at outbound email filtering in addition to the traditional inbound email perspective regarding spam emails. In fact, with data leakage prevention (DLP) becoming a buzzword in the IT sector these days, it is no surprise to see enterprises looking to ensure that sensitive data and information are not being leaked out into the public domain via the email channels. As such, we do expect outbound email filtering/email DLP to play an important role in driving up email security in the near future, particularly due to Compliance.”

One common thread that was touched on a lot during MediaBUZZ’s Anti-Spam seminar on October 23, 2008, was ‘false positives’. The term false positive first arose from the world of diagnostic tests.

An anti-spam product is like a pregnancy test - it eventually comes down to a yes or a no. False positives refer to legitimate email that is incorrectly labeled as spam by anti-malware software/email filters. Explaining why false positives are creating such a stir lately, Chandrasekaran notes, “With email becoming a critical piece in business communications these days, it is no wonder why false positives are taking centre stage as enterprises start realizing the costs of losing legitimate emails, which may actually translate into a more direct adverse impact on the business as compared to filtering out illegitimate spam emails. Although spam has become synonymous with email security nowadays, vendors are likely to shift their focus to ensuring legitimate emails get delivered successfully as enterprises increasingly turn their attention towards that.”

As to whether the war against spam will ever be won, Chandrasekaran has this to say, “Obviously we have to believe that the war against spam can be won, if not, security professionals like us will be out of a job!”

On a serious note though, he advices that we have to start looking ahead to the future and remember that email integrity is no longer just about spam emails. After all, the problems brought about by email gateways to corporate networks are becoming more sophisticated and have a more direct impact on businesses nowadays. It would be a mistake if everybody was to remain fixated on the issue of spam without looking at the broader issues that have emerged pertaining to email integrity in recent times. “In fact, the war should not be waged against spam alone, but the issue of email integrity as a whole. It should be a concerted effort that needs effective legislation, law enforcement as well as co-operation between the various entities – governments, service providers, vendors and businesses,” he concludes emphatically.◊

By Shanti Anne Morais

Click here to return to the contents page

SPAM - the never ending story

Packing even more of a punch in email security

In September 2008 Axway Inc. and Tumbleweed Communications successfully merged to become one of the leading global providers of multi-enterprise collaboration, secure content delivery, and application integration solutions.

A messaging security provider, Tumbleweed Communications was the Platinum sponsor of MediaBUZZ's event "Spam-a never ending story". Mr. Donald Teo, Regional Manager (Asia), Tumbleweed (now part of Axway) presented on "The Erosion of Spam Filter Effectiveness" and allowed Asian e-marketing an interview afterwards. I was very interested in finding out more on Tumbleweed's expectations regarding the joint ventures in Asia and wanted to get more insights into the challenges his company is facing right now and how he sees the merger's impact in the Asia Pacific region.

The company serves now more than 10,000 customers globally, has around $275MM annual revenue and 1,700 employees. It has a global presence, with key offices in Scottsdale, Arizona (HQ of Axway), Redwood City, California (HQ of Tumbleweed), Paris and Singapore and a 24x7 Global Support with centres based in US, Europe and India.

Both companies have merged to solidify their collective strengths for customers in a variety of categories.

Axway gains a client base strong in several key categories, including an entry into the US Federal Government market. Tumbleweed in turn gains increased global presence, improved R&D expenditures and a technology stack that grows beyond secure gateway and email security.

Axway customers also come away as winners, gaining the addition of Tumbleweed's policy-based secure email delivery and identity validation capabilities while Tumbleweed customers gain Axway's Synchrony functionality, including DMZ security, end-to-end managed file transfer, global process visibility, business-to-business integration, application Integration, and trading partner management, all built on a service-oriented architecture.

In addition, Axway will now integrate Tumbleweed's managed file transfer (MFT), email security and identity validation products into their multi-enterprise collaboration product portfolio with a three-phase integration strategy that is designed to offer immediate and long-term value for customers of both companies.

Phase 1 involves field integration of complementary products that provide immediately two integrated solutions:

***SecureTransport Plus Business Activity Monitoring*:**

Tumbleweed customers can now supplement their SecureTransport deployments with Synchrony Sentinel, a powerful, easy-to-use event collection, management and presentation platform, for end-to-end visibility into both B2Bi and MFT. Synchrony Sentinel improves customer experience, reduces operating costs and brings a true enterprise view to cross-platform and application file movement for both business and IT. Sentinel enables portal-based customer self-service, executive dashboards, better visibility for customer service representatives and proactive alerting and event management.

continues on Page 10

SPAM - the never ending story

From Page 9 — Packing even more of a punch in email security

Sentinel bridges the gaps in requirements for visibility for both technical and business teams.

***SecureTransport Plus Enterprise MFT*:**

Tumbleweed customers can deploy Synchrony Sentinel and Synchrony Transfer to add business activity monitoring (BAM) and internal file transfer across multiple platforms and applications, including mainframes, AS/400 and major enterprise resource planning (ERP) solutions. Files represent 80% of the data in an organization, yet enterprise service bus (ESB) and SOA strategies today fall short of providing critical services for file-based applications. By capturing, correlating and acting on events from SecureTransport, Synchrony Transfer, and business applications, Sentinel provides complete event-based management of all of the business processes SecureTransport supports today.

Axway will soon launch Phase 2, integrating core Tumbleweed products into Axway's service-oriented Synchrony™ Framework. In the longer term, Axway will initiate Phase 3 to merge any functionally similar products into a single, best-in-class solution.

So, Axway provides end-to-end visibility, analytics, and internal file transfer capabilities to customers of Tumbleweed's MFT solution, SecureTransport™ and a bigger customer base that enables Tumbleweed to provide a total solution not only on e-mail security but also on product services. Donald Teo revealed that after the merger, Tumbleweed will keep the directive as a subsidiary under Axway.

"We still run our own marketing campaigns. We also still work with the respective partners to push our e-mail security product", he told us.

As for the key technical challenges for an e-mail security company, Teo considers the continuous attempt to foresee what a hacker is trying to do next. "They can change a subject of an e-mail into something that is common and that can therefore bypass the computer or they can break up an e-mail into picture files or different picture partitions to go through" Teo explains.

That's the reason why his company is constantly updating their solutions and continuously tries to understand the mind of hackers.

It's what they call a pro-active approach to prevent suspects from coming into the system.

Tumbleweed has its own lab that consists of about 40-50 engineers, based in Sofia, Bulgaria for developing countermeasures. Their qualified team there analyzes every day spam that is coming to a computer all over the world and on top of that, they work with the third party provider Commtouch, which is specialized in anti-spam and anti-virus technology.

With Commtouch, the company has a honey pot at hand that is placed all over world, Teo said. And that's the reason why they don't plan to set-up a lab in Asia any time soon. They are located in Hong Kong and Singapore and think that is sufficient to understand the trends in the market.

Commtouch has its own technology and they were one of the first in the market that had what's called "real spam detection". So besides using own techniques to define spam, Tumbleweed is constantly in touch with Commtouch to leverage on their real time detection.

In Asia, he sees the trend that most of spam and its ensuing scams are coming from China, pointing out to the recent stock scam that was trying to bring down the market. He continues to explain that it is sometimes very difficult to differentiate real investors from scam, which actually looks often very legitimate and real so that people tend to believe it and start buying shares. And exactly that happened to one listed company in Hong Kong that created immense up-roar.

continues on Page 11

SPAM - the never ending story

From Page 10 — Packing even more of a punch in email security

Of course, some of the stock scams which are circulated also come from US, using computers in China which are not as secure compared to the one in US as barely any regulation or spam law is in place. But Teo also pointed out here that businesses shouldn't only concentrate on spam that is coming into the organization but also focus on what goes on in the company itself.

When asked to characterize the unique value propositions of Tumbleweed and how his company differentiates itself from other players in their industry he said: "Initially, we said we have the best spam capture and less false positives, but actually that's what all other vendors now say as well.

So I say that we definitely have a better user interface than the rest of the competitors. And in addition, we allow our users to individually control and manage their spam, which means they decide whether an e-mail should be classified as spam or not."

For organizations looking for a proven, easily deployed solution to stop junk email, and protect against viruses and worms, Tumbleweed's MailGate AntiSpam can therefore be the right choice.

It incorporates both proactive as well as reactive anti-spam technology, delivering up to 98% capture rates with extremely low false positives.

MailGate AntiSpam combines three technologies, Dynamic Anti-spam (DAS™), Intent Based Filtering (IBF), and Recurrent Pattern Detection Technology (RPD™) to virtually eliminate spam without losing good messages. The proactive IBF technology applies artificial intelligence to identify evolving spam techniques. Tumbleweed's Message Protection Lab™ identifies and analyzes spam and phishing attacks, publishing regular filter updates to the MailGate appliance via the optional DAS update service. RPD identifies spam outbreaks on the Internet through the real-time analysis of large volumes of email. A simple web interface lets users access quarantined messages and filtering options. Its high performance, fast installation, and low maintenance provide one of the lowest Total Costs of Ownership (TCO) of any solution on the market.

Teo explained: "From a single interface it is possible to see the volume of the e-mails coming in, how many e-mails are classified as spam, what are the connections that are blocked by DHA and DOS, and best of all, users can individually do white-listing and blacklisting which means their own spam classification, regarding content, subject line, special keywords etc."

In the beginning, Tumbleweed's focus was mainly on the enterprises whose concern was always on cost-savings and productivity of their IT. But while the enterprises kept their capability to run and buy the product in-house instead of outsourcing, SMBs did in general outsource their services to so-called ISPs or hosting services and became dependant. Today, Teo sees this trend morphing. Considering the downturn, he expects that many enterprises will outsource their IT needs to service providers, too. Therefore Tumbleweed has aligned its strategy with this trend and now looks at hosting providers or even ISPs to be able to provide a better anti-spam solution to them. Tumbleweed's Regional Manager is convinced that "outsourcing is the way to go". "Still there has to be a lot of concentration on awareness and data leak protection", he added and pointing out that not "all users around the world are well educated and therefore not all computers are protected". According to him, there is not a lot that vendors or technology providers can do, saying: "we can only protect in terms of spam that is coming into the network but we can't protect the users' PCs itself and play therefore only a part in terms of education or user awareness."

Due to the fact that everybody has more or less got more accustomed to spam in the course of time, Teo sees more a focus on the prevention of information leaking out of the company and expects that by-and-by, the market will see a consolidation from anti-spam to data leakage. ◊

By Daniela La Marca

Click here to return to the contents page

SPAM - the never ending story

Spam's not going away and more security with control needed

Did you know that according to Sophos, 95% of all email is spam and virtually all spam is sent from compromised computers? Moreover, one in every 416 email messages between July and September this year contained a dangerous attachment, designed to infect the recipient's computer – a staggering eight-fold rise compared to the previous quarter where the figure stood at only one in every 3,333 emails. According to the company, much of this increase can be attributed to several large-scale malware attacks made by spammers during the period. The worst single attack was the Agent-HNY Trojan horse which was spammed out disguised as the Penguin PanicApple iPhone arcade game.

Other major incidents included the EncPk-CZ Trojan which pretended to be a Microsoft security patch, and the Invo-Zip malware, which masqueraded as a notice of a failed parcel delivery from firms such as Fedex and UPS. Windows users opening any of these attachments exposed their PCs to the risk of infection and potentially put their identity and finances at risk. A point to note, the most widespread attacks seen by Sophos are not designed to run on Unix and Mac OS X.

In addition, Sophos finds a spam-related webpage every 3 seconds, which adds up to almost 24,000 a day. Spam, says the company, is a continuing problem, and spammers keep coming up with new, innovative ways to get users to click on their emails. This keeps both vendors and users constantly on their toes. Also, despite being around for years, spam poses significant challenges. In fact, one of the biggest hurdles when it comes to spam is the fact that it is constantly changing, says David Chow, sales & channel enablement manager, Asia, Sophos. "Spam keeps up with the times and vendors and users have to work hard to keep a few steps ahead of them." He also adds that spammers will always find new, innovative ways to send out junk email, and there will also always be a new subject.

Asia is not spared at all in the spam war. More and more Asian countries are also appearing on Sophos' list of spam-relaying countries (for example, China inclusive of Hong Kong, South Korea, Thailand, Philippines, Taiwan, Vietnam, Australia, Japan, Malaysia and Singapore). Reasons for this include the rising popularity and proliferation of the Internet, more bandwidth and also the fact that many of these countries have weaker security know-how and experience. Unsecured computers are a playground for spammers, and a haven for botnets and hackers alike.

Asian companies are also at great risk to spam simply because their security compliance is currently very week, states Chow. He adds that this however, will change over the next few years as most of them invest more on their security infrastructure.

Chow notes that the war against spam will continue to escalate. With spam being more malicious now than ever, it's no wonder than that Sophos' advanced its pro-active botnet defenses with Sender Genotype. A next-generation reputation filtering technology designed to eliminate botnet spam at the IP-connection level and unlike traditional reputation filters, which rely on prior knowledge of the sender, Sender Genotype effectively identifies aberrant behavior from IP addresses,

continues on Page 13

SPAM - the never ending story

From Page 12 — Spam's not going away and more security with control needed

which have not yet established a reputation and immediately blocks them from connecting to Sophos customers' mail systems.

Based on data collected in 2008, SophosLabs estimates that botnets generate nearly 90% of all spam worldwide. This issue is compounded by the fact that spam bots appear online for mere minutes at a time to send targeted messages, often using dynamically assigned IP addresses and low traffic volume to bypass traditional reputation filtering. Sophos Sender Genotype overcomes this inherent weakness by monitoring connection requests and rejecting those showing evidence of botnet connections. Even a new or unknown sender IP (e.g. a newly recruited bot) that has never before sent a message can be blocked using Sophos' breakthrough technology.

Sender Genotype is a free, seamless upgrade option for existing and prospective customers of Sophos Email Appliances and PureMessage for UNIX.

In addition to the development of Sender Genotype to counter the ever-increasing volumes of spam, Sophos also recently delivered eXtensible Lists (SXL) to its Email Security and Control solutions portfolio.

SXL is an online look-up system that dramatically accelerates the distribution of anti-spam intelligence, moving away from traditional scheduled updates to a real-time system that provides quicker response to new and emerging spam campaigns.

"At Sophos we are committed to constantly updating and improving our technology and developing new technology in the war against spam. Our philosophy is simple – it's based on security with control.

We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our future security and control direction focuses on integrating information control and security compliance into our existing infrastructure," Chow emphasizes.◊

By Shanti Anne Morais

SPAM - the never ending story

The Not So Secret Cost of Spam

It's definitely no secret, spam is adversely costing businesses lots of money.

Here's a quick look at how:

Anti Spam and Anti-Virus Technology

With the amount of malicious mail around, these two should always go hand in hand. Most companies not only spend thousands of dollars on anti-spam software and hardware solutions, but they also drop cash on employees and consultants to plan, deploy and maintain the technologies.

Wasted Storage

Quarantined spam (where junk messages are placed in a directory for review and confirmation by recipients) requires additional storage capacities. For many, the whole idea of quarantining spam is so they can take a look at it at a later time, and maybe find email messages that may be valuable to them. However, most users don't ever tend to review their quarantined spam. Remember, even spam that sits in your 'delete' box takes up valuable storage space which cost money.

Dip in Productivity

Spam simply wastes your employees' time. Remember the old adage, 'Time is precious'? Well, according to a study by Nucleus Research, the average employee spends 16 seconds reviewing and deleting each spam message. Deleting messages is turning out to be the most expensive spam strategy. The same study reveals that the average employee at companies that delete spam messages loses an average of 7.3 minutes per week looking for lost legitimate messages.

ISP Costs

It would be naive to believe that ISPs aren't passing along junk email's tremendous costs to their customers.

In an October 2007 report, anti-spam software vendor Symantec Corp. estimated that 70 percent of all email was spam. The traffic burden created by junk email forces ISPs to add extra network and server capacities. In addition, they also install their own anti-spam solutions. All these are costs.

The Intangible Cost

Spam has an often unseen, broader economic impact as well, affecting many companies and even nations that are least able to bear the burden. Consider Nigeria, for example. Nucleus Research noted that while fraud and corruption have been rampant in Nigeria for some time, the country may be forever kept in the digital darkness because of the volume of deceptive email sent by local spammers. The research firm noted that most spam filters block any mail with "Nigeria" in the title or text, effectively keeping anyone communicating with, from, to or about Nigeria from doing it via email.

It might be interesting for you to check out just how much spam is costing your business.

For an idea, try http://www.cmsconnect.com/Marketing/spamcalc.htm ◊

By Shanti Anne Morais

Click here to return to the contents page

SPAM - the never ending story

Unifying Email Security is Imperative

A strong advocate and believer of unified security, Proofpoint's Gerry Tucker, regional director, Proofpoint, gave us his take and perspective on spam especially in the Asia Pacific region.

Photo: Gerry Tucker

Do you think spam is a huge problem (and not just a nuisance as many people tend to think)? Why?

Today's spam poses a number of significant threats to organizations for a number of reasons over and above the "nuisance" value. Firstly, today's spam is complex in nature and is very often the carrier or open-door to additional threats. It can deliver a payload via the message directly or via the action taken by the recipient that can result in a breach of security to not only that individual but also the organization as a whole. With the development of techniques such as backscatter we are also now seeing spam effectively becoming a Denial of Service Attack. These are just some of the ways in which spam continues to pose an increasing threat to individuals and organizations.

Why do you think spam is still a problem after all these years?

The fundamental reason why spam is still a problem is that the spammers continue to invest in new technology and techniques. The main reason for this is because it is highly profitable for the spammers. In the same way that the spammers continue to innovate, vendors must continue to invest in their solutions to keep them up to date and ensure they are delivering maximum effectiveness to their customers.

What do you think is the biggest problem/ challenge posed by spam today?

There are a number of problems posed by spam today: One is its growing volume; second is the growing complexity including techniques such as social engineering and the third is the dynamic and targeted nature of these attacks. In some cases, we have seen an individual user receive over 100,000 messages within a matter of hours. Organizations need to ensure that they have solutions in place which can dynamically adapt to these threats in a rapid fashion without adding to their administration and maintenance overheads.

What are the top spam threats of 2008? Has this changed in any way from the spam threats of 2007? Do you think these threats will change in any way in 2009/2010? What significant problems does spam pose for businesses in particular?

As mentioned above there are a number of areas of concern for businesses:

- increased volume placing an excessive strain on infrastructure
- lost productivity
- loss of confidential information as a result of accessing spam
- becoming part of a botnet themselves which can result in a virtual network outage of their outbound email

continues on Page 16

SPAM - the never ending story

From Page 15 — Unifying Email Security is Imperative

What are the common mistakes that businesses/users make when it comes to spam? What do you think they should be most aware of when it comes to spam? What can they do to better protect themselves?

One of the most common mistakes is to assume that what worked yesterday will work today. This is very often not the case. Users need to constantly review their infrastructure and security solutions to ensure they have the highest level of protection with the lowest total cost of ownership. Look for solutions that can demonstrate an effective solution and are dynamic in nature.

Does the spam problem differ in any way in the Asia Pacific as compared to other regions in the world?

Spam in Asia Pacific still lags behind other parts of the world but we are rapidly catching up.
In addition to this, Asia Pacific is increasingly becoming a source of spam either as part of botnets or as local spam gangs seek to get in on the "business opportunity". We are now also seeing spam that is specific to the region and indeed also to certain countries and languages.

Where do you think Asia stands when it comes to spam and also where do you think we stand when it comes to the war against spam? Why do you think so many countries in Asia are 'spam-relaying countries'? Do you think this is going to change in any way in the near future? How?

Although Asia makes up only around 16% of global spam volume, this is increasing exponentially with India and China leading the way. Internet penetration in Asia is around 15%, compared to a 75% penetration rate in North America. Over the next few years, Asia will be one of the biggest growth areas for internet connectivity. However this will pose a monumental challenge. As most of these users are relatively inexperienced and with limited understanding of security, they pose a risk for the rest of the community as they become "relays" for spam and other malware.

We need to work harder to educate individuals and organizations as to best practices in combating spam and other threats. The solutions that offer help with spam and malware also need to understand that Asian spam is different from other spam, with spam being less focused on financial services, and more heavily represented in health and pharmaceutical product schemes.

In Proofpoint's presentation at our Anti-Spam Forum, your presenter, David Habben, noted that many users are sending out spam themselves. Can you elaborate on this? Is this a new development, and how can it be prevented?

This phenomenon is generally part of botnet activity. In many cases the individuals or organizations are not aware of this activity until they get blacklisted by which time it is too late. In today's work, it is necessary to consider not just the inbound threat but also those posed by emails originating from within the organizations' network. This type of threat can be potentially more damaging than inbound threats.

Why do you think current spam detection is not what it should be?

Many solutions have simply failed to keep up. They are based on older techniques and technologies which have failed to evolve. The net result of this is that end-users have to develop and maintain their spam solutions rather than the vendor providing an effective solution. At the end of the day it is the vendor's responsibility to deliver an effective security solution.

What are the benefits of using a SaaS Spam filter? Do you think more and more businesses will turn to SaaS in this space? Why?

There are several benefits to a SaaS spam solution. The most immediate is the reduction load on the organization's infrastructure as bad traffic is stopped in the cloud. In theory, this should reduce the levels of administration but this will only work if the SaaS solution is effective.

continues on Page 17

SPAM - the never ending story

From Page 16 — Unifying Email Security is Imperative

If it is not, then it could well have the effect of increasing administration due to false positives/negatives. As with any SaaS solution, one of the keys to success is to ensure that you have the best SLA in the industry, such as that offered by Proofpoint. It then becomes the vendor's responsibility to ensure they meet these rather then the end-user.

What do you define as unified email security?

Today, email security covers four key areas

- Inbound
- Data Loss Prevention (DLP)
- Encryption
- Email Archiving

These four elements need to be combined with a clear and implemented security solution which can then be used to provide reports and audit information to the organization.

There was a lot of talk about 'false positives' during our Anti-Spam forum. What's your take on false positives and where does Proofpoint stand here?

One of the trade-offs with older technologies is effectiveness versus false positives. Due to the unique nature of the Proofpoint technology we have been able to demonstrate consistently the highest levels of effectiveness with the lowest levels of false positives irrespective of the deployment models, be that on premise or in the cloud.

Do you think the war against spam can ever be won?

I am not sure the war can ever be won until we can educate people not to purchase or access spam. However, we can definitely win the battles and make it harder for the bad guys to generate revenue. At the end of the day, if the economics don't stand up the spammers will stop. So if everyone was to use Proofpoint, we might well put ourselves out of the spam business at some point. Fortunately for our business, email security is broader than just spam.

Do you think anti-spam legislation helps in the war against spam? What do you think needs to be improved or looked at when it comes to the current anti-spam law in Singapore? Overall, where do you think Asia stands when it comes to anti-spam legislation?

Unfortunately national anti-spam legislation in places like Singapore, Australia and Thailand has not had any significant impact on the spammers. This is mainly to do with the fact that most spam does not originate in the country where it is finally viewed and so the legislation is to a large degree ineffectual. A global approach needs to be adopted but it is unclear if that can actually be achieved.

How do you think spam is going to evolve in the future?

Spam will continue to evolve using new techniques and also new media. We are already seeing IM and SMS spam, as VoIP networks continue to grow it is possible that they too may be targets for the spammers with a whole new generation of voice spam. One thing is certain vendors such as Proofpoint need to continue to invest and develop their technology to ensure that our customers do not suffer from this continued growth.

What do you think makes Proofpoint stand out from its competitors in this area?

There are a number of areas that makes Proofpoint stand out from the crowd. Firstly, there is the breadth of the solution covering all aspects of email security as described above. Secondly, there is the unique nature of the technology that is in use in our solutions which aimed at achieving effective security policy with minimum business impact. The final element is the ease of deployment with a choice of hardware, virtual (VMWare) or in the cloud models available. In addition to this, as Proofpoint focuses solely on messaging security we have been able to continuously innovate to deal with the evolving threats in the world today and into the future. ◊

By Shanti Anne Morais

Click here to return to the contents page

SPAM - the never ending story

Email Reputation and Authentication are Crucial in the War against Spam

It's never been more crucial for users to realize that spam is much more than a nuisance. A study by Ferris Research reveals that the global cost of spam has doubled between 2005 and 2007, and is now over US$100 billion per annum worldwide. Having morphed over the last few years, a lot of spam nowadays is malicious and part of cyber-criminals' targeted attacks. What's worse, the manner/technique of spam attacks is constantly changing. Due to the evolution of email spam, filtering companies responded by combining anti-virus and spam filtering into their solution offerings.

Manish Goel, CEO of BoxSentry and Chair of the International committee for AOTA (Authentication & Online Trust Alliance) notes that all anti-spam tools/spam filters, no matter how good they are, suffer from false positives – "it's just very difficult to prevent." At the same time, users have very high expectations. "Users have to realize three very important things: Firstly, spam is always evolving. Secondly, spam filters are not magic wands and finally, spam is never going to vanish into thin air," he emphasizes.

According to Goel, false positives are a bigger problem than spam. It's easy to understand why as they, like spam, are much more than an inconvenience. Legitimate messages that never reach their intended recipients (i.e. false positives) can easily lead to confusion, frustration, anger, wasted time, double work, hurt feelings, missed deadlines and, most importantly, incomplete business transactions. "False positives can be even more catastrophic and costly to a business than spam," observes Goel. However, having said this, he is also quick to point out that spam; especially malicious spam should be blocked at all cost.

Most anti-spam vendors typically promise accuracy rates in excess of 99 percent. Yet ,with companies' financial well-being increasingly tied to their email service, any spam filter that is less than 100 percent effective poses a serious risk. It's not all bleak though; the good news is as Goel points out, false positives have been making their presence heard and felt, and the whole security industry in itself is recognizing the fact that they are a pivotal issue that needs to be addressed.

BoxSentry itself is a leading voice in this arena and has redefined the agenda for email security by effectively creating a new category of email security solutions zooming in on protecting legitimate email. "We are very focused on anti false-positives, that is, the philosophy of being innocent until proven guilty. This is why a key focal point of ours is protecting legitimate emails at all costs. In fact, we have taken a contrarian approach with our ground-breaking flagship solution, RealMail, which has been developed to ensure an exceptionally low rate of false positives whilst still effectively protecting against email security threats such as spam," he explains further.

RealMail in fact, is a full email security suite that provides complete and multi-tier email protection, says Goel.

The company also partners with other leading security companies like CommTouch Software which provides email fingerprinting (i.e. real time email pattern detection) to ensure RealMail stays in the forefront of email security. In addition, they also partner with a leading anti-virus provider, which cannot be named at this point of time.

continues on Page19

SPAM - the never ending story

From Page 18 — Email Reputation and Authentication are Crucial in the War against Spam

RealMail can also be deployed as an Appliance or as a Managed Service. Indeed, RealMail, shares Goel, was envisaged as a SaaS solution from day one. "The future is Managed Services," states Goel emphatically. "For any organization, email security is non-strategic. It therefore makes more sense to have a shared infrastructure in place, one that provides complete real-time protection that is at the same time, extremely cost effective," he continues. Contrary to the perception that SaaS is only well-received by SMBs, RealMail's customers go across the board, from SMBs to even large ISPs and companies. "We are continuously improving our technology, including new partnerships and also integrating new components into our technology and strategy," Goel adds.

Sharing his observation of the email security market, he notes that the email filtering marketplace is seeing a level of consolidation. He also says that users are getting more aware of the issue of false positives and its consequential damages.

Commenting on the effectiveness of legislation in the war against spam, Goel believes that anti-spam legislation is necessary but not sufficient. "Anti-spam legislation is an important component of making a strong stand and statement that spam is not to be and cannot be tolerated. However, will legislation solve the problem of spam? The answer here is a definite no. The main reason for this is because the majority of spam originates offshore, plus spammers make money from it. However, as mentioned, anti-spam law states that as a jurisdiction, the country that imposes and implements it does not tolerate spam. This is a very important statement to make," he remarks.

He also observes that any anti-spam legislation that needs to be introduced should be well-balanced between protecting the consumers while not hindering businesses.

"Once again, at the end of the day, the vast majority of spam comes from overseas. Bearing this in mind, legitimate email senders should not face so much constriction. Legitimate senders are often the unknown victims of spam as their emails get thrown out by the anti-spam filters. This is why education of the email senders is very important. The Direct Marketing Association of Singapore is one Association which is doing a very good job here," Goel says.

As for the Singapore Anti-Spam law, Goel has this to say, "Maybe some things in the legislative act here to be clarified or explained more clearly. However, the law is definitely a step in the right direction. Changing it will not make an impact on the user experience or solve any spam problem. In the meantime, it is important to make users realize that a lot of their legitimate emails may just be disappearing."

Goel also emphasizes the importance of sender authentication which he says should go hand in hand with a false positives' email strategy and solution. "In this way, trusted email lists are built," he continues. "Reputation is also a very important key here as with a good reputation technology system, a list of trusted correspondence is built per organization. RealMail does this using patented technology. In this way, users know that the email they are receiving is from a trusted source. Email senders with a positive reputation and who engage in transparent sending patterns get priority over unknown senders. We see the market shifting in this direction."

He concludes that spam is a problem that will never go away. "Email is a crucial part of communication for all organizations nowadays, however it is broken and a key question for us in the industry is to fix this. This is why our core mission is to do just this and restore business confidence in email communication."◊

By Shanti Anne Morais

Click here to return to the contents page

SPAM - the never ending story

False positives are on the radar, but spam filters should not be disregarded

False positives (legitimate email that gets blocked by spam filters) are a genuine problem. Think of that email that you were waiting for ages for, but which was in your spam folder all along. What about those important emails which never reach you at all? False positives not only cause frazzled nerves and hurt feelings (how many times have you come down hard on someone for not sending you an email, only to discover it fell into your spam box?), but it also costs you time, and maybe even lost deals and money.

Failing to receive critical messages in a timely fashion can do irreparable damage to customer and partner relationships and cause important orders to be missed, so eliminating false positives while maintaining high anti spam accuracy should be of upmost importance to any enterprise anti-spam solution. Anti-spam software is designed to protect your inbox from unwanted messages, but unless your system is properly trained, even the best software misses the mark and flags legitimate messages as spam.

Why do false positives occur?

Various anti spam solutions make use of different methods of detecting and blocking spam. Anti-spam software typically use content filtering or Bayesian Logic, an advanced content filtering method, to score each email, looking for certain tell-tale signs of spammer habits such as frequently used terms like "Viagra", "click here" or even, “Anti-Spam”. Other anti-spam solutions reference blacklists and whitelists to determine whether the sender has shown spammer tendencies in the past. A false positive can occur when a legitimate sender raises enough red flags, either by using too many "spam terms" or sending their messages from an IP address that has been used by spammers in the past.

Here’s how to minimize false positives

Although it might take a person only a moment to process a message and identify it as spam, it is difficult to automate that human process because no single message characteristic consistently identifies spam. In fact, there are hundreds of different message characteristics that may indicate an email is spam, and an effective anti spam solution must be capable of employing multiple spam detection techniques to effectively cover all bases. In addition, the same way one man’s meat may be another man’s poison, what’s one man’s spam might be another person’s heaven.

A comprehensive anti spam approach involves examining both message content and sender history in tandem. By using a reputation system to evaluate senders based on their past behavior, a more accurate picture of their intentions and legitimacy can be discerned, and a solution's false positive rate can be further lowered. Important questions to ask include: Has the sender engaged in spamming, virus distribution or phishing attacks in the past? If not, the likelihood of their message getting past the email gateway just went up, and the chances of a false positive declined accordingly. If they have, an effective reputation system knows and flags the message.

In addition, a good reputation system should work in tandem with an authentication system – that is, every email should be confirmed to be from a trusted source.

Self-Optimization

In order to be most effective, anti spam solutions must learn based on a recipient’s preferences. While most of us prefer not to receive emails containing the term Viagra, some medical organizations might need to receive these emails in order to process patient data. In order to best learn your organizational preferences, anti spam solutions should put filtered emails into a quarantine that allows users to review and make decisions as to whether a particular message is spam.

continues on Page 21

SPAM - the never ending story

From Page 20 — False positives are on the radar, but spam filters should not be disregarded

Making this quarantine available to the end-user lowers the administration costs and increases the accuracy of the anti spam system.

Each time a user makes a decision about whether a particular email is or is not spam, the system becomes more personalized and intelligent about filtering email for that individual in the future. Over time, users find that they rarely need to review their quarantines anymore because the system has learned how to identify messages that are important to that user. An effective, accurate anti spam solution aggregates multiple spam detection technologies, combining the benefits of each individual technique to stop spam while minimizing false positives. It also puts suspected spam into a quarantine that is available to end-users, and learns how to better identify spam in the future.

Why spam filters should not be thrown out...at least not yet

If we lived in a perfect world, there would be no need for spam filters. With the proliferation of spam and its ever-changing face, anti-spam technology is definitely necessary. Running a company email system without spam filters risks forcing employees to waste precious time searching for real business messages embedded in an endless stream of con offers, pornographic ads and just plain gibberish. For many companies, that's almost as unacceptable as losing good email. Fortunately, it's possible to use spam filters while minimizing the risk of losing legitimate email; here are a few steps that your company can take.

Compare products

Remember that all spam filters aren't equal. Some products do a much better job of separating junk from legitimate emails than others. Carefully read the reviews of competing products to see which products and services offer the best filtering success rates.

Customize the filter

Just about all anti-spam applications allow administrators to fine-tune system settings for maximum effectiveness.

Filter adjustment, however, is as much an art as it is a science. It's important to think creatively about words and conditions that may cause the anti-spam app to tag a legitimate message as junk. Filters for a medically oriented company, for instance, should be configured so that the word "breast" would not be blocked when followed by the words "cancer research." Be forewarned though, it takes a lot of work to tune a spam filter for maximum effectiveness.

Enable whitelisting

Whitelists allow all emails from trusted senders to pass through the filter untouched, even if they contravene filter settings. Find an anti-spam application that lets end users build and manage their own whitelists, then show your users how to use this valuable feature.

Protect employee email addresses

Your business will get far less spam if employee addresses aren't scattered all over the Web, where spam robots can scoop them up and relay them to spammers. Make it a company policy to prohibit employees from posting business-domain email addresses to Web boards, social networks and similar sites. Some companies take this practice to the next level by eliminating all employee addresses from enterprise Web sites, funneling viewer inquiries to specific, generic addresses such as "info@ ..." "sales@ ... "and "support@… "

Encourage end users to occasionally check their junk-mail folder

Most anti-spam applications dump tagged messages into a file called the "junk-mail folder," "spam folder" or something similar. Remind employees that if an important, expected email fails to arrive, a quick glance in the junk-mail bin might be a good idea. It is also a good idea to periodically check your spam folders.◊

By Shanti Anne Morais

Click here to return to the contents page

SPAM - the never ending story

Scary Email Issues of 2008

What do Halloween and a sent email have in common? Both can be equally frightening, according to Proofpoint, a provider of unified email security, archiving and data loss prevention solutions. With Halloween lurking around the corner, Proofpoint has identified some of the scariest email issues of 2008.

These blunders, attacks and mishaps have caused sleepless nights and financial peril for consumers, corporate executives, politicians and of course, email and IT administrators.

In no particular order, Proofpoint highlights some of this year's email mishaps below:

Phishing Fiasco

In September, it was reported that cyber-criminals were launching fake sites for charities and asking unsuspecting consumers for donations to help in the hurricane disaster efforts. With any phishing site, people can be tricked and treated into revealing financial information and often discover the fraud after it is too late.

The Proofpoint Attack Response Center reports that "themed" phishing attacks continue with the latest threats preying on consumer concerns around the global financial crisis.

Preying on Palin's Email

A hacker breached the personal Yahoo! account of vice presidential candidate Sarah Palin and revealed portions of its content on a site called Wikileaks. Security experts note that it can be fairly simple for a determined person to hack into a personal email account, but concerns have been raised about Palin using her personal email for business issues. David C. Kernell, son of Tennessee State Representative Mike Kernell, was indicted earlier this month in the case.

Obama's Unsightly Spam

A malicious spam email spread in September claiming to have a link to a sex video of Obama, but instead included spyware to steal sensitive data from the victim's computer. Current events and sensational news headlines—both real and fictional—remain popular subject lines for phish and spam attacks because of their potential to lure recipients into opening the email or its attachments.

Emails: Dead and Buried

Oracle Corp. failed to unearth CEO, Larry Ellison's emails that were sought as evidence in a class-action lawsuit. According to the US District Judge Susan Illston, Oracle should have figured out a way to comply with the order to produce the information, which was issued in late 2006.

Email Job Elimination

Carat's chief people officer accidently alerted staffers that their jobs could be in peril by sending an office-wide email only meant for senior management. Additionally, the specifics on the talking points of their restructuring were shared.

Unhealthy News Anchor Obsession

A former news anchor, smitten by his female co-anchor was charged with hacking into her email account 537 times in 146 days, often checking on her 10 times a day or more. He logged in from both home and work and passed on some of the information to a Philadelphia newspaper gossip columnist.

Space Encounters

NASA found a computer virus on a laptop aboard the International Space Station, which carries about 50 computers. Email continues to be one of the most common distribution methods for new viruses and other malware, underscoring the need for organizations to deploy anti-virus technology at the email gateway, email server and end-user desktop levels.

Qualcomm's Email Cemetery

Qualcomm got smacked with an $8.5 million penalty because it bungled its own discovery of email relevant to a patent lawsuit with Broadcom. As more courts require thorough discovery searches, mistakes like these will come to the forefront.

continues on Page 23

From Page 22 — Scary Email Issues of 2008

Batting Back Backscatter

Stephen Gielda, president of Paketderm, found his servers were being inundated with a tidal wave of backscatter messages. At one point, he was being hit by 10,000 bounce back messages per second.

Angel-O-Lantern

Countrywide CEO Angelo Mozilo hit reply rather than forward when typing 'disgusting' in response to a customer's email. The media and the investor community noticed Mozilo's response. In fact, one investor on a Web site wrote, "I hope that company gets what they deserve10."

"Given all of the potential risks and costs associated with email, it's no surprise that nearly 15 percent of IT executives that Proofpoint recently surveyed said they would eliminate email in their organizations if that were feasible," notes Sandra Vaughan, senior vice president of marketing and products for Proofpoint. "But email has evolved from a business and personal communication tool to the most mission-critical application for most organizations. From courts of law to the race for the presidency, email security is being taken very seriously. And while email can cause mayhem, there are solutions available that help organizations reduce the substantial risks posed by both inbound and outbound email."◊

Click here to return to the contents page

The Rising Tide of Spam Continues Unabated

IT security and control firm Sophos has released the results of its investigation into the latest spam trends and revealed the top twelve spam-relaying countries for the third quarter of 2008. The figures show an alarming rise in the proportion of spam emails sent with malicious attachments between July-September 2008, as well as an increase in spam attacks using social engineering techniques to snare unsuspecting computer users.

According to the report, one in every 416 email messages between July and September this year, contained a dangerous attachment, designed to infect the recipient's computer - a staggering eight -fold rise compared to the previous quarter where the figure stood at only one in every 3,333 emails.

Sophos has identified that much of this increase can be attributed to several large-scale malware attacks made by spammers during the period. The worst single attack was the Agent-HNY Trojan horse which was spammed out disguised as the Penguin Panic arcade game for Apple iPhones. Other major incidents included the EncPk-CZ Trojan which pretended to be a Microsoft security patch, and the Invo-Zip malware, which masqueraded as a notice of a failed parcel delivery from firms such as UPS.Windows users opening any of these attachments exposed their PCs to the risk of infection and potentially put their identity and finances at risk. The most widespread attacks seen by Sophos are not designed to run on Unix and Mac OS X.

Elaborating on this, Graham Cluley, senior technology consultant at Sophos shares, "For Apple Mac and Unix lovers, these major spam attacks just mean a clogged-up inbox, not an infected operating system. But organized criminals are causing havoc for Windows users in the hunt for cold hard cash. Too many people are clicking without thinking – exposing themselves to hackers who are hell-bent on gaining access to confidential information and raiding bank accounts. The advice is simple: you should never open unsolicited attachments, however tempting they may appear."

Social Engineering continues to outfox users

As well as using malicious email attachments, cybercriminals have continued to embed malicious links and spam out creative and timely attacks designed to prey on users' curiosity. For example, in August, Sophos warned of a widespread wave of spam messages claiming to be breaking news alerts from MSNBC and CNN.

Each email encouraged users to click on a link to read the news story, but instead, took unsuspect-

continues on Page 24

SPAM - the never ending story

From Page 23 — The Rising Tide of Spam Continues Unabated

"When a spam email appears to come from a trusted source, too many users are fooled and end up clicking through to a malicious webpage," observes Cluley. "The naivety shown by many internet users is downright dangerous. In the past, hackers were more like teenage mischief-makers breaking into sheds to see what they could find. Today they're hardened criminals wearing hobnail boots with no qualms about breaking into your home and stealing everything they can get their hands on."

Spammers have proven themselves to be unafraid of trying new methods of distributing their marketing messages and spreading their malware to an undefended public during the last three months. Sophos has seen an escalation in the amount of spam being sent via social networking websites such as Facebook and Twitter, and expects this trend to continue to rise.

Emerging countries surface as spam-relaying offenders

This quarter's report has seen three new entries to the spam hall of shame: Colombia and Thailand have assumed eleventh and twelfth place respectively, while India has shot straight into the chart at number seven.

"Insecure computers, wherever they are in the world, are a spammer's dream - they can be easily hijacked remotely and joined to sprawling networks of botnets designed to create chaos by sending floods of spam and carrying out denial-of-service attacks," elaborates Cluley. "The message needs to be heard loud and clear: if you don't properly defend your PC you are not only putting your data, finances, and identity at risk, you are also endangering other members of the internet."

Sophos identified the top twelve countries responsible for relaying spam across the globe between July-September 2008:

1. United States 18.9%
2. Russia 8.3%
3. Turkey 8.2%
4. China (incl HK) 5.4%
5. Brazil 4.5%
6. South Korea 3.8%
7. India 3.5%
8. Argentina 2.9%
9. Italy 2.8%
10. United Kingdom 2.7%
11. Colombia 2.5%
12. Thailand 2.4%

Other 34.3%

Other countries:

14 Germany 2.27%
15 Spain 2.17%
17 France 1.74%
22 Canada 1.18%
24 Philippines 0.90%
29 Japan 0.65%
31 Netherlands 0.60%
32 Australia 0.56%
40 Indonesia 0.30%
41 Switzerland 0.29%
42 Singapore 0.29%
48 Ireland 0.23%
49 Austria 0.22%
54 South Africa 0.17%
56 Malaysia 0.15%
64 New Zealand 0.11%
67 Belgium 0.10%
95 Luxembourg 0.03%

Whilst the United States retains its position as the top relayer of spam, Russia has increased its contribution to the world spam problem, soaring from 4.4 percent last year, to 8.3 percent during this time period.

Spam relayed by continent, July-September 2008

1. Asia 39.8%
2. Europe 23.9%
3. North America 21.8%
4. South America 13.2%
5. Africa 1.0%
6. Other 0.3%

According to Sophos researchers, there is no sign that recent legal action by the authorities against major spam gangs have had any perceptible impact on the amount of spam in circulation. The company recommends that organizations automatically update their corporate virus protection, and run a consolidated solution at their email and web gateways to defend against viruses and spam.◊

Click here to return to the contents page