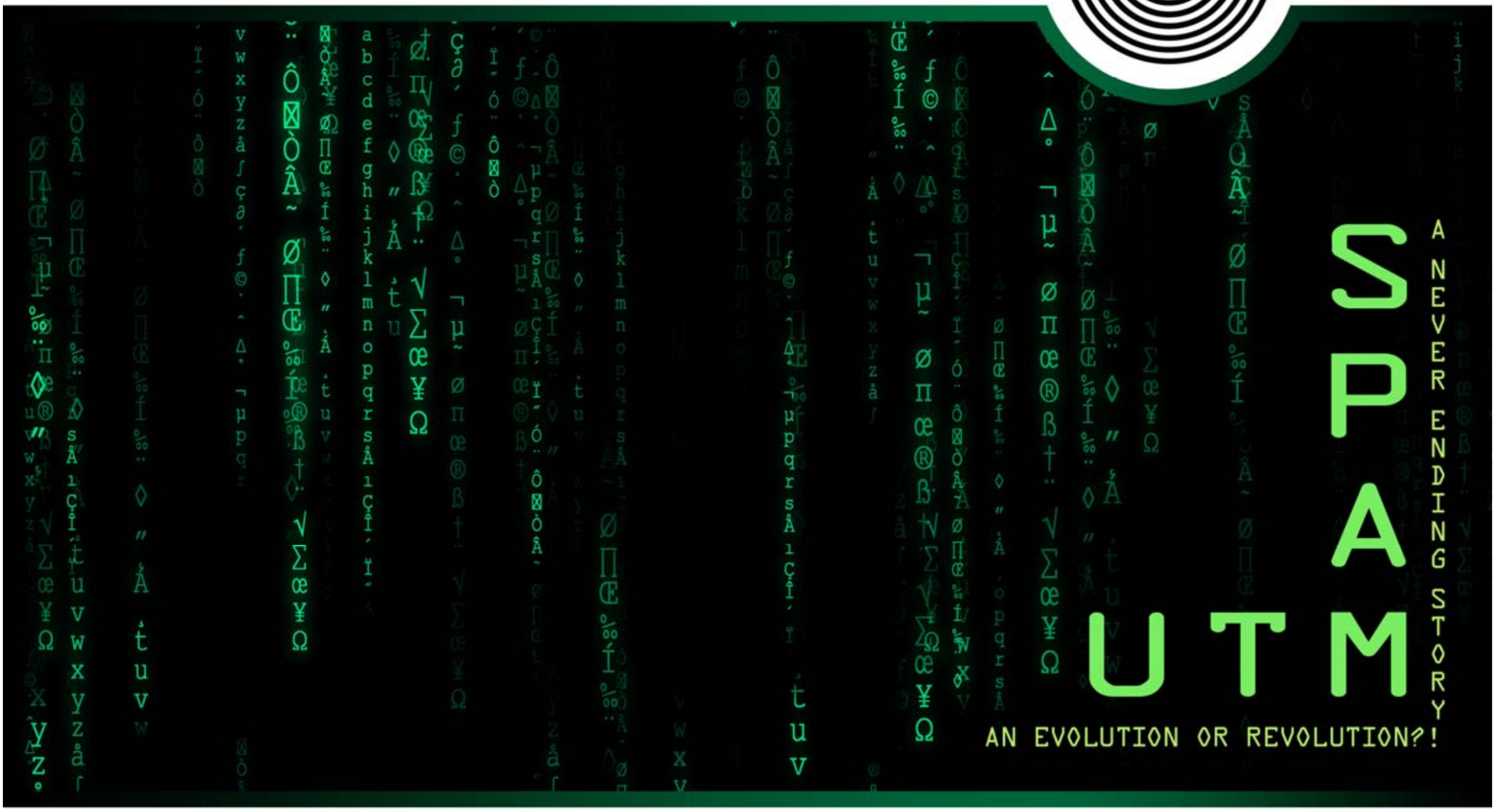
ASIAN ANTI-SPAM GUIDE

MediaBUZZ



SPONSORS

Tumbleweed® now part of Axway

SOPHOS

WatchGuard™

proofpoint™

BoxSentry

OFFICIAL CONSULTING PARTNER

FROST & SULLIVAN

ASIAN ANTI-SPAM GUIDE

MEDIABUZZ PTE LTD

January 2009

Highlights

- *Combating the latest inbound threat: Spam and dark traffic, Pg. 13*
- *Secure Email Policy Best Practices, Pg. 17*
- *The Continuous Hurdle of Spam, Pg. 29*
- *Asian Anti Spam Acts, Pg. 42*

Contents:

ASIAN ANTI-SPAM GUIDE

MEDIABUZZ PTE LTD

January 2009

Highlights

- *Frost & Sullivan: Do not underestimate spam, Pg. 65*
- *Unifying email security is key, Pg. 71*
- *The many threats of network security, Pg. 76*
- *The UTM story, Pg. 82*

Contents:

EMAIL SPAM: A RISING TIDE

IT security and control firm Sophos has recently released its report on the latest trends in spam, and revealed the top twelve spam-relaying countries for the second quarter of 2008. The investigation reveals a disturbing rise in the level of email spam travelling across the internet between April-June 2008, and how some spammers are now using Facebook and mobile phones to spread their messages.

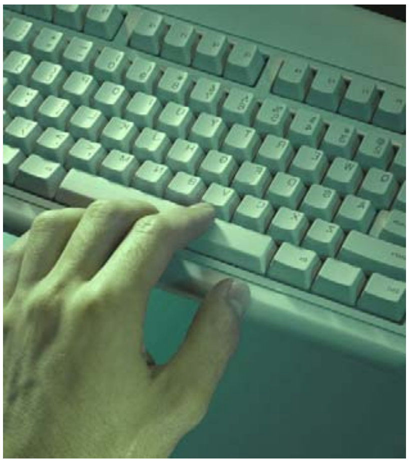
By June 2008, research reveals that the level of spam had risen to 96.5% of all business email. Having risen from a figure of 92.3% in the first three months of the year, corporations are now facing the fact that only one in 28 emails is legitimate.

"If your company is on the internet, it's going to be hard for it to do business unless it has an effective anti-spam defense in place. Otherwise the amount of junk mail will be swamping legitimate correspondence from your customers and suppliers," says Graham Cluley, senior technology consultant for Sophos. "It should be remembered also that some spam is not just a nuisance, but malicious in its intent - trying to get you to click on an attached Trojan horse or lead you to a dangerous website. Organizations need a consolidated anti-spam and anti-malware solution at their gateway, updated around the clock to neutralize the latest internet attacks."

Sophos recommends companies acquaint their users with best practice advice for minimizing best practice advice for minimizing exposure to spam, automatically update their corporate virus protection, and run a consolidated solution at their email and web gateways to defend against viruses and spam.

Spam relayed from hijacked botnet computers

Email spam is almost always sent from innocent third party computers which have been hijacked by hackers. These botnet computers are owned by innocent parties, who are unaware that cybercriminals are using them for financial gain. Typically they are home users who have not been properly protected with up-to-date anti-virus software, firewalls and security patches. It is therefore important that more be done to raise awareness amongst computer users about the importance of keeping their PCs secure.



Spam: Spreading in new ways

Sophos has discovered that spammers are increasingly using networking websites such as Facebook and LinkedIn to send their unwanted links to online stores and bogus lottery and financial scams.

"Spammers are finding themselves increasingly obstructed by corporate anti-spam defenses at the email gateway. In a nutshell - we're stopping the bad guys getting their marketing message in front of their intended audience," says Cluley. "To get around this, we are seeing spammers exploiting networks like Facebook to plant spam messages on other peoples' profiles - these don't just get read by the owner of the profile, but anyone else visiting his or her page."

In May, the LinkedIn business networking system was used by scammers seeking to swindle money from unwary corporate executives. On this occasion, the spammers offered a share of a non-existent US $6.5 million inheritance fund, further highlighting the need for users to be vigilant to unsolicited approaches online.

Sophos experts note that the level of Facebook, Bebo and LinkedIn spam is still dwarfed by email spam, but there is a growing trend for spammers to use other techniques to spread their messages.

Another growing method for spammers to spread their messages is via SMS texts sent to mobile phones. Spamming a lot of people via text message is an effective way of generating a flash-flood denial-of-service attack against the telephone system of an organization you don't like. As mobile operators give away more and more "free texts per month" as part of their calling-plans, and make available SMS web gateways that can be exploited by hackers, we may see more spammers using SMS to clog up phonelines.

Email continues to be a favorite tool of spammers and still presents a danger to computer users. It is common for cybercriminals to spam out links to compromised websites, often using a subject line and message to tempt computer users into clicking through the promise of a breaking news story or a lewd topic.

The Pushdo Trojan dominated the chart of most widespread

continues on Page 5

From Page 4 — Email Spam: A Rising Tide

malware spreading via email, accounting for 31 per cent of all reports. Pushdo has been spammed out during the year with a variety of disguises.

Some for example, have claimed to contain nude photographs of Hollywood stars Nicole Kidman and Angelina Jolie.

On the bright side, attacks via email file attachments, however, have reduced in 2008. Only one in every 2,500 emails examined in the first six months of 2008 was found to contain a malicious attachment, compared to one in 332 in the same period of 2007.

Phishing still going strong

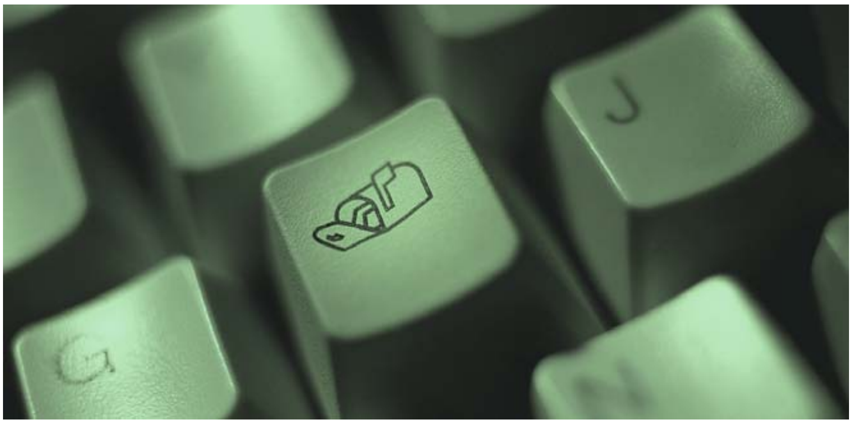
Sophos continues to see widespread phishing email campaigns targeting the users of online financial

institutions, and popular auction and payment websites. In recent months social networking websites like Facebook have also caught the interest of phishers.

It is important to remember that phishing campaigns are not specific to any one operating system, and can affect any internet user regardless of whether they use Microsoft Windows, Mac OS X or a brand of UNIX. Because they exploit trust and human nature rather than software they are likely to continue to be a problem for the foreseeable future.

Spear-phishing on the rise

'Spear-phishing', which involves messages that have been personalized to a specific domain or organization, has become more common in recent months. These emails will appear to come from a trusted source, such as a member of IT staff at the same company as the recipient, and ask for personal information or username and password confirmation. Those who reply to these messages will inadvertently be supplying information that the phisher can use



for malicious purposes, such as identity fraud. Spear-phishers generate the victims' addresses by using special software or using lists of employees found on the networks of social media sites such as Facebook or LinkedIn.

To guard against this risk, all organizations should ensure employees are fully educated about the dangers of posting too much information on these sites, and of accepting unsolicited friend requests

“Businesses need to bite the bullet and take better care of securing their computers, networks and websites. They not only risk having their networks broken into, but are also putting their customers in peril by passing on infections,” adds Cluley. “On the other hand, office works also must realize that it’s not just the business fat cats who need to worry about this. Visiting an infected website from your work PC, or sharing too much personal or corporate information on sites like Facebook, could lead to you being the criminal’s route into your company.”

China as a host of Spam

There is a growing trend for spammers to host their content and websites on Chinese web servers. This has caused problems for some security companies because it is harder to get visibility on Chinese domain name information than it is for other countries. There are also language and cultural issues which have conspired to make it more difficult to get some offending websites taken down promptly.

From the criminals’ point of view the use of Chinese domain names is attractive, as they do not have to change their domain so regularly and may be able to operate for a longer period of time.

Backscatter spam

A noticeable spam trend during the first half of 2008 was the growth in the number of non-delivery report (NDR) messages generated by mail systems that accept spam messages during an SMTP session. If there is a delivery error (for instance, “mailbox full” or “user doesn’t exist”), the system attempts to send a bounce message back to the supposed original sender. The bounce message is directed to the email address found in the envelope sender information (the Return-Path header) in the original message. Because this address has been forged in most spam messages, the bounce message is delivered to a mailbox of a sender who did not send the original spam message.

This is known as “backscatter spam”. Specific addresses or domains that are favorites of spammers can be the target of hundreds, or even thousands, of backscatter spam messages every day.

continues on Page 6

From Page 5 — Email Spam: A Rising Tide

Mobile phone spam

Another growing method for spammers to spread their messages is via SMS texts sent to mobile phones.

According to the Internet Society of China, 353.8 billion spam messages were sent to the country's mobile phone owners in the last year. As a consequence, China's 574 million mobile phone users, receive on average over 600 spam messages each year. Of the 438,668 spam complaints received in June 2008, 39.17 percent were regarding fraudulent texts and 36.28 percent were commercial adverts.

The problem is not confined to China - Dublin and Texas have also recently seen spam attacks.

Spamming a lot of people via text message is an effective way of generating a flash-flood denial-of-service attack against the telephone system of an organization. As mobile operators give away more and more "free texts per month" as part of their calling-plans, and make available SMS web gateways that can be exploited by hackers, we may see more spammers using SMS to clog up phone lines.

Cybercriminals getting more creative

The company has also noted from research of the first six months of 2008 that cybercriminals are increasingly using creative new techniques in their attempt to make money out of internet users.

Most attacks are now designed to try and out-fox traditional security systems such as email-scanning.

Web Infection rates surging

The first half of 2008 has seen an explosion in threats spread via the web, the preferred vector of attack for financially-motivated cybercriminals. On average, Sophos says it detects 16,173 malicious webpages every day - or one every five seconds. This is three times faster than the rate seen during 2007.

Over 90 per cent of the webpages that are spreading Trojan horses and spyware are legitimate websites (some belonging to household brands and Fortune 500 companies) that have been hacked through SQL injection.

SQL injection attacks exploit security vulnerabilities and insert malicious code into the database running a website. Companies whose websites have been struck by such an attack often clean-up their database, only to be infected again a few hours later. Users who visit the affected websites risk having their computer taken over by hackers, and their personal banking information stolen by identity thieves.

In addition, Sophos has identified that the number one host for malware on the web is Blogger (Blogspot.com), which allows computer users to make their own websites easily at no charge. Hackers both set up malicious blogs on the service, and inject dangerous web links and content into innocent blogs in the form of comments. Blogspot.com accounts for 2 per cent of all of the world's malware hosted on the web.

Business websites attacked

Thousands of webpages belonging to Fortune 500 companies, government agencies and schools have been infected, putting visiting surfers at risk of infection and identity theft. High profile entertainment websites such as those belonging to Sony PlayStation and Euro 2008 ticket sales companies are amongst the many to have suffered from the problem.

Unfortunately, there is still a common belief that spam is not a threat but with virtually all of it unwanted, and

a dangerous proportion linking to infected websites, organizations should be secure their email and web

gateways just as fastidiously as their desktops and laptops. Email spam after all these years is still continuing to plague users.◊

By Shanti Anne Morais

A Glance at the first 6 months of 2008

- **Total number of different malware threats in existence – over 11 million**
- **Biggest malware threat – SQL injection attack against websites**
- **New web infections – 1 new infected web page discovered every 5 seconds**
- **Spam-related webpages – 1 new page discovered every 20 seconds**
- **Top malware-hosting country – US with 38%**
- **Top spam-relaying continent – Asia with 35%**
- **Email with infected attachments – 1 in 2500**
- **Spam in business email – 97%**
- **New types of spam – Mobile, Facebook and backscatter spam**
- **Top host for malware – Blogger (Blogspot.com)**

WHAT EVERYONE SHOULD KNOW ABOUT SPAM AND PRIVACY

Email users need to know more about e-mail, spam and privacy to keep up with the global electronic communication environment. So we present some spam-related issues that could affect Asian email users and e-marketers and provide information about dangers surrounding spam and how to move toward permission-based marketing.

What is Spam?

There is no official, legal, definition of spam that everyone on the Internet has agreed on. However, generally it can be one of three things:

Spam posts

These are messages posted to email discussion groups, chat rooms or bulletin boards that are "off topic" or distinctly promotional in a non-promotional setting. If you belong to a discussion group to discuss the aerospace industry and someone posts a message marketing an aerospace trade show, that could be spam depending on the rules of the list. Most lists publish rules for new joiners so they will know exactly what's considered spam before they post.

"Junk" email

This would be a broadcast email message sent to multiple recipients who did not request it, and who aren't even in the right target audience for it. For an example, an offer for Viagra sent to millions of people regardless of their age, sex or health. This kind of spam is easy to spot because it's so obvious.

Non-permission marketing

This is an email message which is (or appears to be) a broadcast sent to multiple recipients who did not request it -- even though they may be in the right target audience to potentially appreciate such a message.

This is the hardest kind of spam to understand; and it's the type that is most pervasive in the B2B marketing world today.

Anyone who sends a message to a list of customers or targeted prospects, each one of whom did not proactively give permission ahead of time to receive that particular type of message, could be guilty of sending spam.

Is this spam as "bad" as the first two types? That depends on the law in the state or country the recipient is in, your organization's stated privacy policy, and how annoying the message might be in terms of promotional content and/or frequency.

Unfortunately when it comes to the annoyance factor, spam is in the eye of the beholder. Which means a message you think is perfectly acceptable might intensely annoy some recipients.

In the end, THE SENDER'S OPINION DOESN'T MATTER. All that matters is the opinion of the recipient.

If somebody thinks you spammed him or her, you probably did.

The Legal Outlook

(Please Note: We at MediaBUZZ Pte Ltd are not lawyers, nor did a lawyer review the information below prior to publication. It's merely intended to serve as a starting point for discussion between you and your legal counsel.)

Thanks mostly to the growth of annoying junk emailers, citizens around the world are contacting their governments asking them to stop spam. Although you may not be a junk emailer, the laws being discussed and enacted could affect your organization, simply because their wording can be fairly broad. So, you may not think of yourself as a spammer, and still get in legal trouble someday.

UNITED STATES

Every year more bills are introduced into the House and Senate in relation to email. These are moving forward without much opposition (after all, who wants to take the side of a nasty spammer?) Currently six, including a wireless spam bill, are under discussion.

Most require that all email messages include an opt-out option (i.e. a way to get your name off the list) and that list owners are to be held accountable for swift unsubscribe processes. In the B2B space, proposed laws look a lot like current fax marketing legislation -- you can email anyone with whom you have a "current business relationship."

15 states, including California, already have spam laws on the books. In general these laws will only affect business marketers if they have an office in that state, and are knowingly sending unsolicited email messages to recipients in that state with whom they have no prior relationship.

CANADA

Canadians are way ahead of the United States in terms of email regulation. New Canadian regulations took effect January 1,

continues on Page 8

From Page 7 — What everyone should know about spam and privacy

2001 that currently apply to every company doing business with organizations that are regulated by the Canadian government, such as banks, airlines, trucking companies, telecommunications firms, etc.

These regulations are on an evolving schedule -- by 2004 the laws will affect everyone doing business in Canada regardless of their relationship with the government.

Non-Canadian organizations with Canadian subsidiaries and/or offices located in Canada should learn more about this regulation immediately. We also recommend that others track this area carefully because the evolving Canadian situation could be used as a predictive forecast for American legislation.

EUROPE

The European Commission set a fairly strict anti-spam directive more than a year ago. In general European lawmakers are in favor of opt-in lists where the recipients have proactively asked to be on the list. They are not in favor of opt-out lists, where recipients have been placed on the list without their permission and they must opt-out (or unsubscribe) to get off the list.

Many American businesses currently email their customers and prospects on an opt-out basis. So, European laws could definitely affect some legitimate American companies who do not think of themselves as spammers.

You cannot be prosecuted or fined if you do not have a European office. However, if you do have ties to Europe, watch out! Three different expert sources have told us that as of July 1 2001, the European Commission are specifically seeking American violators they can make a very public example of.

One source said, "A lot of people think the Europeans are just rattling their sabers. They're not. They're serious about this."

ISPs, Corporate Mail Managers & Black Holes

Even if you are in full compliance with the law in every country on earth, you can still get in trouble as a spammer.

Why? Because Internet Service Providers (ISPs), such as SingTel, StarHUB, or Pacific Internet that provide the means for companies and individuals to go online, have to power to stop anyone they think is a spammer from using their systems. Quite simply, if an ISP decides you are a spammer, they can stop any email from your server from going through their system.

If ISPs are so powerful, then why is there so much spam today? Simply because it's very easy to open an email account. Many junk emailers open email accounts under false names, use them once, and then fold up shop and move to the next account within a few hours. By the time the ISPs move to stop them, they are long gone.

However if you are a legitimate business, chances are you're sending out email using your own company name. So, if an ISP decides to stop you from emailing their members, it's a lot harder for you to get around it. You can't just switch company names!

Aside from ISPs, the other people who can block your email are corporate mail managers and the individual recipients. Most medium-large organizations have someone in charge of their email system. If that mail manager receives a few complaints from folks in the office about a potential spammer, he or she is likely to block all email from that sender in the future. Most individuals can also easily block email these days with just a few keystrokes by using the "mail block" or "block sender" feature in their email program.

In none of these cases -- the ISPs, corporate mail managers and individuals -- are the people involved generally consulting with lawyers before they block your email. It's not about the law. They see something they think is spam and they stop it. End of discussion.

So even if your email is completely legal, it can still be blocked if the recipients think it's spam. It's all a question of perception. We asked several experts on both the ISP and corporate mail manager side to describe the measures they take to decide if something is spam or not. Generally their answer boiled down to the number of complaints they received and who they received them from. If the CEO complains about being spammed, you can bet the mail manager is going to block that emailer!

Most experts also told us to bear in mind that ISPs and managers are busy these days. They don't have a lot of time to closely examine each case of suspected spam. So a couple of complaints can be enough for many of them to take action.

ISPs and many major corporate and governmental mail managers are well-connected.

continues on Page 9

From Page 8 — What everyone should know about spam and privacy

Thanks to email discussion groups and bulletin boards, they often pass the word when they spot a suspected spammer. So, if you've been blocked by one organization, you can find yourself quickly blocked by others.

The most famous blocking list is called the "Black Hole." Aside from the obvious junk emailers, some pretty big company names have appeared on this list at one time or another, reportedly including Microsoft and Real Networks.

Protecting Your Brand

"Why can't I just test it?" We hear this question all the time. A marketer (usually from a direct mail background) says, "Well sure, spam isn't a great thing. But there's no law against it, and I probably won't end up in the Black Hole because I'm not running a scam or selling sexual material. So, why can't I just test sending a broadcast email to a non-permission list to see if it works for me?"

Our answer is - you can. But be forewarned, you may be risking something more than a few legal fines and IT problems. You may be risking your brand.

Even if you don't get think spam is a big deal, plenty of other people do. In fact, plenty of your customers and best prospects do. Studies have shown that about 40% of recipients really, really hate anything they perceive as spam, and an additional 30% just dislike it.

So, your non-permission campaign may get orders. In fact if the list is a highly targeted one, and your offer is strong, you may make a profit ... initially. But at what cost?

Even if some of the people on the list respond positively, up to 70% of people on that list may have been annoyed by your message. Some may even be annoyed enough to swear to never do business with you again.

Some may tell their ISP or corporate mail manager to block all email from you in future. Some may decide just to delete all emails from you in future without opening them.

This is a particular problem for B2B marketers because your sales prospect pool is probably fairly limited. You don't have tens of millions of potential customers. You may not even have tens of thousands. If you are operating in a tightly targeted pool, you shouldn't further limit your prospects by sending something they might perceive as spam.

Conversely, if your company is a big famous brand name, and you are caught spamming, it could turn into an online PR crisis as users email each other and post the news on public boards and chat rooms.

How can you know up-front if your customers and/or prospects will perceive your email as spam? The easiest and best way to know is to ask them.

If you are currently sending regular emails to a list of people who have opted-in to get email from you, you should consider sending a survey as well. Lots of surveying software on the market now makes this remarkably quick, inexpensive and easy.

If you are currently sending emails to a list of people who have not specifically asked to get that type of email from you, you should begin investigating permission-based marketing immediately.

Gathering Permission

If you are new to permission marketing, your first step should be to get a copy of Seth Godin's book, "Permission Marketing: Turning Strangers Into Friends and Friends Into Customers." This best-seller, published in 1999, is still the basis of most strategies and tactics behind successful email marketing today.

Here are some of the basics every marketer should know: THE THREE TYPES OF PERMISSION - All permission is not alike.

1. Opt-Out:

In this situation the list owner informs people that they are on the list -- and the only way they can get off the list is to take action by unsubscribing, cancelling or "opting out." Basically you're saying, "You're already on my list and if you don't want to be on my list then you'll have to tell me. Otherwise I'm going to keep emailing you."

Some opt-out lists are created when there are pre-checked boxes on registration or order forms online. If visitors have to take action by unchecking the box, then that is considered opting-out.

In general opt-out lists perform less well for marketing campaigns than opt-in lists because

continues on Page 10

From Page 9 — What everyone should know about spam and privacy

people haven't proactively asked to receive the information. In a growing number of recipient's minds opt-out lists are spam. So, if you plan to go in this direction, it's worth thinking twice first.

As one businessperson told us, "I get antagonized when a company assumes I want to be on their list. If you just ask me first, I might happily agree to be on it. But if you tell me I'm already on it and I have to do some work to get off, you've antagonized me from the start. Opt-out is not a very customer-friendly way to proceed."

2. Opt-In:

Unlike opt-out, people on opt-in lists have actively requested to be added to the list. They are hand-raisers. They have not only given you their email address, they have also given you explicit permission to email them a certain type of message with a certain type of frequency.

Here's the biggest point of confusion -- if someone has given you their email address, perhaps on a business card or on a form they filled out as a site visitor, they are NOT an opt-in. The only way someone can be an opt-in is if they know what they are opting-in for - a newsletter, a regular sales message, a third party ad message ... whatever. It's got to be spelled out.

That's why if you are collecting email names (and which company these days isn't?) you need to also collect specific permission. You need to ask people at the point of collection what sorts of things you can do with their name in the future -- such as send them a newsletter. If you don't ask anything, if you just gather an email address at the point of sale without questions, then in strict terms the only way you can use that email address is to communicate with that customer about that particular sale -- sending shipping information and/or a receipt by email. You can't add them to your newsletter list and say it's "opt-in" because they didn't.

3. Double Opt-In:

Have you ever been tempted to put someone else's email address into a registration form? Or have you ever signed up a friend or colleague for an email newsletter? Double opt-in is designed to prevent this from happening.

If a list is a double opt-in list, a message is automatically sent to the person who's been signed up, asking if he or she really wants to be added to the list. Unless he or she actively replies positively, his or her name is wiped from the list very shortly thereafter and they never get another message.

Some purists believe the only way you can be safe and sure that your list is really opt-in is to make it double opt-in. This is probably a good idea if you plan to rent your list (most lists on the rental market are double opt-in) or if highly secure or confidential information will be sent to the names on the list.

Otherwise, most marketers can simply use the singular opt-in -- but be prepared for some complaints from people who will angrily email you saying, "Hey I never signed up for this!" Every singular opt-in emailer in the world gets these complaints at least occasionally. So you need a procedure in place to deal with them.

TOP 4 WAYS TO GATHER PERMISSION

The number one question we're asked by readers is, "Am I allowed to send someone just one unsolicited email in order to ask for permission to add them to my list?" In other words, is it ok to spam someone once, so you can avoid spam in the future? Given the legal, ISP and branding concerns we've outlined above, the answer is probably not.

So how do you gather permission? By using all the media -- both online and offline -- that you already use to interact with your marketplace successfully, such as:

1) Direct Mail: Many companies have gathered opt-ins by using postal postcards, snap-packs or other direct mail packages to ask people on their postal list to opt-in to their email list. Usually they direct recipients to a Web address where they can sign up. You might also want to add a phone number.

2) Broadcast Email: Be very sure the email list you use is either an opt-in list (or double-opt-in to be safest.) Your best bet is to ask to see the form that people opted-in on. If a list owner can't show you that, then don't rent the list. Also, if a list owner offers to sell you the list -- so the list is in your hands and goes out under your company name -- then it is assuredly NOT an opt-in list.

On occasion if you have a very strong, beloved brand name, and you have an email list of customers who have bought from you recently, you may be able to get away with sending a broadcast email to those customers once to ask them to opt-in. This may not be legally safe in Europe or Canada, and unless you are careful, it can hurt your brand in the USA.

So proceed with caution.

continues on Page 11

From Page 10 — What everyone should know about spam and privacy

3) Email Newsletter Ads: Many marketers have had great success gathering qualified prospect opt-ins by advertising in email newsletters because newsletter lists are often more targeted than broadcast email lists. You won't have much space - - sometimes less than 50 words -- so focus your copy on a single strong offer. White papers, free newsletters, sweepstakes and other free offers work well.

4) Your Communications Materials: Your opt-in offer should be on almost every communication your company makes. This includes, every page of your Web site (consider making it part of your navigation bar), business cards, employee email signatures, space advertising in magazines, print materials, order forms, customer service inbound calls, etc. Remember a few years ago when you had to add your URL to everything? Now you have to do the same with your opt-in offer.

HOW LONG DOES PERMISSION LAST?

Not as long as you think. People have short memories. In fact one research report showed that just under 5% of opt-ins will completely forget they signed up for your list within 30 days. The general rule of thumb is any name you haven't emailed in six months to a year has probably forgotten they ever gave you permission. So if you email them, they may think you're a spammer.

This means you should take two steps:

1. Have a plan of action for the opt-in names you collect. With their permission you might want to email them some sort of useful information at least every 4-6 weeks. Quarterly mailings are probably too far apart.

2. Always add a section to your messages that tells people how you got their email address, and how they can get off the list easily (and without cost.)

CREATING AN EFFECTIVE PRIVACY POLICY

Every organization collecting email addresses must have a privacy policy. While it's not the law in most countries yet, it's simply good business. As a marketer, you'll be pleased to hear that company after company has reported that when they include a link to their privacy policy when asking for an opt-in (or sale) it increases response rates.

In some senses privacy policies are the 100% money-back guarantees of the 21st century. Having a good strong one can help raise your sales, although customers may rarely use it.

WHO SHOULD MANAGE YOUR PRIVACY POLICY

At least one person in your organization should be in charge of creating, maintaining and managing your privacy policy. If you don't already have a Chief Privacy Officer, someone in your legal, marketing or IT departments may take charge. Whoever it is should be very good at cross-departmental communication.

Your Privacy Manager will need to coordinate with every department that collects, touches or uses customer or prospect data in some way. This includes sales, accounting, marketing, customer service ... you name it!

Some companies have found that whoever headed up Y2K compliance is a good person to tap for this role as well.

You may want to start the process by hiring the services of a privacy consultant. Although there are plenty of them in Europe and Canada, there are still only a handful in the United States.

American readers have recommended the following:

Your policy should simply state exactly how your organization plans to use any and all data collected from your Web site. Our biggest warning -- be careful not to make your privacy policy too broad sweeping. If you say something like "We'll never give your data to a third party" watch out, because if you ever use an outside email fulfillment provider to send messages, they could easily be construed as a third part

How often should you update a policy? As often as things change in the way your organization handles data. Experts recommend your policy manager check with all departments for changes at least every six months. In fast-moving organizations, quarterly might be your best bet.

And yes, expect changes. Saying "This policy will never ever change until the end of time" is a sure way to invite trouble. ◊

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.

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."◊

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 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.

continues on Page 14

From Page 13 — Combating the latest inbound threat: Spam and dark traffic

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. 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

continues on Page 15

From Page 14 — Combating the latest inbound threat: Spam and dark traffic

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 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

PROOFPOINT SURVEY VIEWED SPAM AS AN INCREASING THREAT IN ASIA

Spam is a growing problem for 91% of Asian organizations, with many saying they have lost business, suffered security or privacy breaches or had customers or clients lose confidence in them as a result, according to a recent survey from Proofpoint, Inc.

“Email is failing in its role as the primary business communication tool within many organizations,” says Gerry Tucker, regional director for Proofpoint in APAC. “While organizations have solutions to counter issues like spam and other inbound threats, their approach is generally piecemeal and becoming increasingly ineffective as these issues worsen.”

The recent second Proofpoint Securing assets For Enterprise (SaFE) Survey of email security issues in Asian enterprises completed by 100 IT managers and executives in Singapore, Malaysia and Thailand, found out that:

- Although spam was a major concern for organizations, with 47.1% of the respondents stating that this was their top concern. 51.5% of respondents stated that data loss was an even bigger concern for their organizations
- When it comes to data loss. 84.1% of Asian enterprises stated email as their top security risk, followed by webmail (8.7%), from a messaging security perspective. Blogs and message boards (2.9%) are also a growing concern as is instant messaging at 1.4%.
- 27.5% of organizations in the region have been negatively affected by loss of private data, with 46.6% of organizations saying they have disciplined an employee for violating email policies.
- Respondents also reported that their current anti-spam solutions stop less than 95% of spam. 24.6% said that their anti-spam solution is less than 90% effective; 50.7% stated that it is 90-95% effective and 17.4% that it is 95-99% effective. Only 2.9% of respondents said their anti-spam solution is more than 99% effective.

Commenting on the results of the survey, Tucker notes, “Our latest survey highlights how Asian email users are gradually losing confidence in email and the negative effect this has on most organizations. While negative impacts on staff productivity are most common, significant numbers of respondents report more serious impacts such as losing business or loss of customer confidence.”

He adds that the most common issue for email users was not that they receive too much spam, but that they were uncertain they were receiving all genuine emails sent to them.

“The survey shows just how dysfunctional email has become at many organizations when the solution -- blocking suspicious emails -- has become a more common problem than the issue it is meant to fix,” elaborates Tucker.

”As spam volumes have risen, we are seeing organizations turning up the settings on their anti-spam solutions and more genuine emails are being blocked as a result.”

“The survey also shows exactly how ineffective organizations’ anti-spam solutions have become. Best practice recommends that solutions should be 99% plus effective, something only. Best practice recommends that solutions should be 99% plus effective, something only 3% of organization currently achieve,” he continues.

An interesting point to note, this survey mirrors the results recently conducted by Proofpoint Australia, which showed that 72.5% of Australian organizations see spam as an increasing threat.◊

SECURE EMAIL POLICY BEST PRACTICES

Many organizations have corporate email policies in order to accomplish a variety of objectives. These policies can help businesses gain competitive advantages when dealing with customers via email, as well as give the organization a way to improve productivity, reduce misunderstandings, and increase accountability.

But now that the instant communication of email is expected from most organizations, some very real security concerns are arising. Many organizations have deployed email systems with the sole purpose of enabling communication. Often, little regard is given to the problems that can arise by email communications falling into the wrong hands. In fact, the security risks have become so public—reports of credit card numbers, social security numbers, pension accounts, and private health information being stolen—that legislators have passed several regulations in the last decade.

Of course, whether or not your company is subject to government regulations, there are many business reasons to protect against intellectual property leaks. If confidential data is sent to the wrong person, or is sent unencrypted, it can irrevocably damage your business—even if you're not subject to government regulations.

The paper policies that sales, customer service, and human resources departments put in place often don't address all the issues—and don't come close to meeting the demands of complying to those regulations. Some organizations take a "see no evil" approach, particularly when they already have an email policy in place: they see no evidence of noncompliance, so they assume (or pretend) that they meet the demands of regulations.

In today's security environment, compliance must be demonstrated. Although companies can ignore a security hole like email policy, an attacker can still exploit it, and an email inadvertently sent to the wrong person can still be a public relations nightmare. In order to be effective, therefore, organizations must implement email policy enforcement. There are many ways to enforce policies and put systems into place that support compliance, but no clear-cut strategy is laid out in any of the new laws.

There are two ways organizations can choose to comply with regulations. The first is simply to make sure the organization can pass an audit by meeting the minimum requirements (sometimes these are referred to as "checkbox" solutions). However, some organizations go beyond the "letter of the law" and actually address the security issues that your customers are worried about.

It is in this spirit that an email policy should be formulated. Can you make it easy for your employees to safely send information via email to the necessary people, both inside and outside the organization? Can you create and implement processes to protect the necessary information? Today's enterprises expect spam filters to catch at least 95% of spam; the best spam filters catch upwards of 99% of unwanted emails.

Approaching security policies effectively

Identifying problem areas is a critical first step. Organizations sometimes underestimate the amount of time that it will take to create policy and implement a solution.

Another challenge is that organizations simply address needs that are uncovered by an internal analysis.

However, internal analysis can often overlook critical issues. This is an area where many companies are willing to "see no evil," believing they will somehow not be responsible for fixing problems if they don't know the problems exist. This is an attitude that hackers, identity thieves, and attackers love; but obviously this attitude is the wrong approach for the concerns of regulators, consumers, and customers. An external audit, although it can be expensive, will often reveal every area that regulations aim to address—and will certainly demonstrate due diligence to your customers.

Perhaps the most important aspect of policy enforcement and compliance is that it is ongoing. It is clear that protecting private information and intellectual property be a business objective for organizations of all sizes. Because of that, it is inadequate to allow policy enforcement and compliance to be a one-time (or even annual) "project." It must be integrated into the business process. Each regulatory requirement should be mapped to a policy or a standard in the organization, and technology and automation should be leveraged to support implementation.

There is no "one size fits all" policy; it must be written to address your organization's unique needs. How is email being used to support your business functions?

continues on Page 18

From Page 17 — Secure Email Policy Best Practices

What kind of regulated content is going out in your email, and to whom? Answering these questions will make it clear what needs to be addressed in the email security policy.

Training vs. technology: which is best for policy and compliance?

Choosing the right kind of technology is very important. Much like the physical security of an office building, employees should be aware of the security features and know how to operate the security functionality in order to get where they need to go. It is perfectly reasonable (and usually expected) that employees will need to be trained how to operate a card reader, an electronic door key, or the alarm system. However, it is not reasonable to require users to rewire the alarm system every day in order to get in and out.

Essentially, an effective email security system should provide employees with a reasonable expectation of security. This means it should have a degree of automation and be part of the organizational infrastructure but not be an "undue burden," much like the organization's telephone system or the physical security system.

Choosing and implementing a system

Older email security models tended to block all suspicious content; however, that has proved impractical and inadequate.

Some companies have chosen reporting only. This can be a good first step in assessing an analyzing an organization's needs, but if the requirement is to protect private information, guard against intellectual property leaks, or comply with legislation, simple reporting cannot meet this need.

The first step to adequate and effective email policy implementation is an analysis of your email use.

Some questions that can be helpful to determine email security needs are:

- How is email being used to support your business objectives? A re there emails that are going out on a regular, ongoing basis, or is it ad hoc?
- What kind of information is your company sending across email? Is there financial data, health care data, or company confidential information being sent?
- Who are the senders and recipients? Internal employees may have different security requirements than business partners and customers.

Answering these questions will determine if you require stringent email security measures as part a standard process, if is more effective to look for rogue data and emails, or if there are other needs.

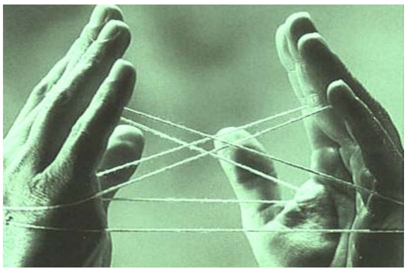
Email encryption types

Setting up email security as a standard process (for instance, for accountants who send reports with private information to auditing firms) requires different solutions than companies who need to simply look for possible leaks. Email encryption solutions protect the content of the email from prying eyes, but each solution is appropriate for a different scenario.

- Gateway-to-gateway and gateway-to-desktop encryption is most appropriate for business-to-business communications. If your organization and your auditing firm have set up a direct network-to-network connection using TLS or S/MIME, some systems can automatically send the email using the specified encryption method, and a system on the recipient's end can automatically decrypt it. Some systems support S/MIME gateway-to-desktop encryption, which means the decryption can be done by the email client (Microsoft Outlook and Lotus Notes both have S/MIME decryption capability). This requires coordination between the two companies, or at least prior coordination between the sender and recipient. If recipients have their own digital certificates set up to authenticate email (most often using PGP and S/MIME), gateway-to-desktop encryption is also supported. Be aware that some companies may not allow encrypted mail to pass through gateways, as it would be an easy way for company secrets or malware to be transmitted.
- Desktop-to-desktop encryption is most appropriate for employee-to-employee or consumer-to-consumer communication. If an organization has senders with recipients who are well-versed in a user encryption method like PGP, an email system can be set up to require (and automatically apply) PGP encryption between certain users if the file fits the policy.
- Universal secure delivery is most appropriate for business-to-consumer communications (and in some other cases as well). Some email security systems have an

continues on Page 19

From Page 18 — Secure Email Policy Best Practices



option to encrypt the message and post it on a secure Web site. It then requires authentication by the recipient to view. This assures that messages can stay secure without requiring recipients to have technical knowledge of encryption to view private documents. See more information on universal secure delivery below.

The basics of intelligent content filtering

Once companies analyze their email usage and decide on encryption technologies to implement, the next step is to choose an email security solution that supports their needs.

Today, the best practice for effective email policy enforcement and true compliance is to implement an intelligent content filtering solution.

Intelligent content filtering is currently the only type of approach that can adequately address all four of the above parts of the integrated business process, and is therefore the only type of approach that can support the necessary business objectives.

Inbound accuracy

Although outbound email is what most organizations will focus on to meet compliance, inbound traffic can also be a concern. Unwanted email that contains malware can undermine the best security policy. Outbound email security solutions also include inbound solutions as well.

It's important to note that not all inbound solutions are created equal. Many spam filters have high rates of "false positives"—real messages that are perceived as spam and therefore thrown away. One false positive can be more damaging to an organization than a hundred unfiltered spam messages. Be sure to choose a solution that has a low rate of false positives.

Content and outbound accuracy

Most of the outbound email traffic organizations have does not need encryption.

However, as organizations become increasingly dependent on email, it's nearly inevitable that social security numbers, individually identifiable information, customer data, proprietary data, or trade secret will make its way through email.

The security problem is that the majority of this type of email is legitimate. That is, this information must be sent and received in order for tasks to be accomplished. (To complicate matters, sometimes this information must be sent and received in order to achieve compliance with other pieces of legislation!)

Therefore, solutions must have maximum flexibility. Analyzing the content of outgoing email for personally identifiable information and proprietary data is essential. But simply blocking flagged emails won't suffice; there must be options for secure email delivery that are easy for senders and recipients.

Part of this flexibility is the ability to limit false positives for outbound messages. Although false positives are generally thought of as applying only to inbound email, outbound messages that are flagged erroneously can create a burden for email administrators. Although false positives are more difficult to limit on outbound emails, some solutions implement tunable policy controls exist to significantly reduce the number of false positives on outbound content.

In addition to looking for specific information—social security numbers and so forth—solutions must also look for patterns that show potential information leaks. If a health care organization can flag an email that contains words like "patient" and "eligible," the risk of revealing private information can be greatly reduced.

Moreover, systems vary on the kind of attachments they can process.

Some systems, for example, can't process PDF files. This requires that PDF files cannot be sent or received with the assurance that the information is safe. Be sure that the system you choose can adequate address all the types of attachments your users commonly send.

Some email security solutions have preconfigured content inspection policies for specific regulations. Additionally, these solutions often have pre-configurations available to identify and flag credit card and social security numbers.

The following are types of content that can be filtered, and what today's email security solutions can do with that content:

Message filtering

The content of the email itself is scanned. This includes:

- Message header
- Message subject
- Body of message

Attachment scanning

Attachments can be a big factor for threats, and can also eat up bandwidth. Some email solutions can only scan certain attachment types. Be sure that the email solution you choose supports all the attachment types that concern your company.

continues on Page 20

From Page 19 — Secure Email Policy Best Practices

The best solutions can scan hundreds of different file types, and support rules for attachments above a certain size. To adequately preserve bandwidth, a rule can be created to either block large attachments, or route them to a different delivery method (universal secure delivery, or even an FTP server). To adequately protect against attacks, the solution should be able to scan for the true type of file, not just the extension letters (changing the extension letters is a common attacking technique).

File types include:

- ZIP files
- PDF files
- Other compression types (RAR , StuffIt, and more)
- Graphics files (JPEG, GIF, PNG, and more)
- Video and music files (MP3, A VI, WMV, and more)
- All Microsoft Office files

Encrypted attachments

As encrypted files and password -protected files prevent email security systems from viewing the contents (these files could potentially contain viruses, malware, proprietary information, or noncompliant information), the option to stop encrypted and password-protected documents from coming through the system should be available in any good email security system.

Nested attachments

E mail systems should support the scanning of a compressed file within compressed attachments (a PDF inside of an RAR inside a ZIP file, for instance).

Pattern matching

A s mentioned above, matching on word(s), wildcards, and patterns is an important way to look for potential information leaks.

Lexicons

U sing dictionaries and lists of regular expressions are another way to catch potential information leaks. If your business is regulated by HIPAA, GLBA, or another specific regulation, an email solution should provide extensible dictionaries based on those requirements. It's also important to give "weight" to certain lexicons (weighing "social security number" more than "patient," for example).

Identity

The sender and recipient information is also important. Analyzing the traffic from the legal department to an outside law firm will likely have different rules than the CEO communicating with a potential business partner. For instance, an intelligent content filter can enforce a rule that all email traffic between your organization and its auditing firm must be encrypted.

Currently, identification can be done using methods including user directories, digital signatures, and manual addressing. E mail authentication is still in its infancy, however, and current methods (like public key infrastructure) still face many practical implementation challenges. However, vendors are working on solutions, and effective identification and authentication solutions are expected to be included in future product releases.

Policy enforcement

When a policy requirement is noted, there are many options available. The most flexible security solutions offer more options so that companies can have complete control over their email communications, and map business processes directly to email policy processes.

These options include:

- Reporting and logging. This simply flags the email and notes the violation in an audit file. This is often a first step for organizations that are developing their email policies. It is not meant to be a final step, as it does not meet the requirements for compliance. The best systems allow reporting and logging to be fully customizable, triggered by certain events, and done in real-time. Another use case is when a new policy is written, it can be reported on first to see if the triggers are correct.
- Delivery. Several options are available for the delivery of the actual email communication:
- Quarantine. This places the message in a secure area for review, usually by an email administrator.
- Drop/Delete. If the email is inappropriate or illegal to send, organizations can simply drop or delete the email at the gateway.
- Return to sender. This returns the email to the sender if a policy violation occurs.

continues on Page 21

From Page 20— Secure Email Policy Best Practices

An annotation can be added to the return message explaining the policy violation.

- Defer. Also called "rate-throttling," this is used to conserve bandwidth. F or instance, if one user is receiving (or sending) thousands of emails, the rate of receipt can be "throttled down" to a reasonable number every hour. Another example is that an email large attachment can be deferred until a time when email traffic is low (in the middle of the night, for instance).
- Encrypt. Automated routing for outbound encryption messages is part of a best practice for meeting compliance demands while also addressing usability issues. See the list in the "Email encryption" section above for details and use cases on different outbound encryption methods.
- Annotate. This allows the email to be amended with any text or HTML content the organization desires. Many companies choose to add a legal disclaimer to outside emails, and this automates this process.
- Digital signatures. This adds a digital signature to the email, which is often done for authentication purposes.
- Routing. E mails can be sent to different email domains within an organization, based on senders, recipients, or content. This is especially important in distributed organizations to make sure emails are routed efficiently and accurately.
- Notifications. When an email meets certain requirements, it can trigger an automatic notification to be sent to any email address; for instance, a supervisor, the legal department, or an email administrator.
- Archive. This places a copy of the message in a permanent email archive in the file system.
- Forward. Depending on the policy, an additional recipient can be designated and sent a copy of the email (for instance, the corporate counsel can receive a copy of any email with the words "pending lawsuit"). Also, an alternate relay can be designated to receive the message.
- Modify headers. Tags, notes, and other values can be added to the email headers. This is typically done if an external system is in place for further processing.
- Modify subject. E mails can be in violation of regulations if the subject line contains personally identifiable information. (Subject lines, even in encrypted emails, are sent in the clear.) Health care organizations have set up policies that flag emails if social security numbers or patient identification numbers are in the subject line. If subject lines have personally identifiable information, they can be deleted; if the subject requires conforming to a standard, information can be added to the subject line.
- Strip attachments. If attachments over a certain size are not allowed, the message can be sent without them.
- Tag for further processing. This allows policies to be chained; combinations of factors can be considered and reviewed before action is taken.

Universal secure delivery

One of the most commonly deployed methods of encryption/decryption is using a staging server to act as a secure store for private messages.

Universal secure delivery works like this:

1. A sender creates an email message and hits the send button.
2. The email security system flags the content and/or identity of sender/recipient as requiring encryption.

   Alternately, the sender can mark the item as "secure.")
3. The system automatically encrypts the file and posts it on the staging server.
4. The system automatically sends a message to the recipient with instructions on how to retrieve the message from the secure store.
5. The recipient follows the instructions, authenticates to the secure store using a Web browser, and retrieves the message. Any reply will also be sent via this secure delivery method.

   Universal secure delivery is chosen frequently because it requires very little training for both senders and recipients; it protects all necessary data, meeting not only the letter of the law but the desires of consumers and legislators; and it leverages familiar technology (a Web browser) to perform its tasks.

Tracking and reporting

A complete email system should perform the tracking of emails through the chain of receipt. Senders and administrators can get information such as:

continues on Page 22

From Page 21— Secure Email Policy Best Practices

- Whether or not the intended recipient received the message
- The disposition of the message (for example: Was it quarantined? Was it blocked by a spam filter?)
- The identity of the account that opened the message (for example, the intended recipient, a proxy, or an unintended recipient)

Tracking can be performed based on the recipient's identity, by the message itself, or by attachment. Many of these tracking options are available at the gateway; some options are only available via certain encryption types (e.g., universal secure delivery).

As noted above, reporting is often a first step for organizations that are developing their email policies. Email systems should have complete reporting features, be customizable (by time, by user, by IP address, and much more) and be able to quickly and efficiently create summaries to send to supervisors, administrators, and other interested parties.

Conclusion

Creating an email policy and an atmosphere for proper compliance is of paramount importance. When an organization knows what's at stake—whether it's supporting business objectives or avoiding the consequences of noncompliance—it can more easily gain support for an implementation strategy.

With email security, it's important to have the flexibility and the power to analyze, assess, configure, tune, and audit as needed. E very organization is different, and so every organization's email security policy will focus on different areas. Many solutions are available, but no matter what solution is implemented, configuring it to meet the email policy is essential to meeting compliance.

Choosing a system that is flexible enough to meet your needs, has the power to analyze and process properly, and delivers a seamless user experience can be challenging. But having the right email policy and the right email solution in place are the first steps to help your organization meet those business objectives.◊

Condensed from a
whitepaper by Tumbleweed
(now part of Axway)

MailGate: Award-winning email security

Recent independent testing and reviews have consistently rated MailGate as the most comprehensive and easy-to-manage email security appliance. And that's no surprise. Providing the power and flexibility to effectively defend against network attacks, spam and viruses. MailGate efficiently manages and enforces regulatory compliance and corporate email policies through content filtering and policy controls. Build on a secure Linux platform that installs in minutes. MailGate features intuitive administrative controls and centralized management for multi-appliance deployments.

The MailGate appliance gets the highest ratings for power and performance – 99.1% spam capture rate with NO false positives.

To learn more, visit www.tumbleweed.com or contact us at our enquiry hotline: (65) 6419 5486

SC MAGAZINE RECOMMENDED
RECOMMENDED

WEST COAST LABS CHECK MARK
SEE YOUR SAFEGUARDS AT www.check-mark.com
Anti-Spam PREMIUM
ANTISPAM PREMIUM RATING

VeriTest a service of Lionbridge
NO FALSE POSITIVES

Tumbleweed®
now part of **Axway**

Tumbleweed
APAC Office: 8 Shenton Way, #31-01, Temasek Tower, Singapore 068811
Telephone: (65) 6419 5486
Email: APACSales@tumbleweed.com

ACWdistribution

ACW Distribution (S) Pte Ltd
Tumbleweed Authorized Partner
Corporate Office: 10 Ubi Crescent, #03-56, Ubi TechPark, Lobby C, Singapore 408564
Telephone: (65) 6325 1390
Email: enquiry@acw-distribution.com.sg

"Since deploying Tumbleweed MailGate, we are now offloading 70 percent of our email traffic. It's much easier to manage the email server, has greatly reduced the size of the email store and minimizes the change of corrupting email queues and mailboxes."
- CITIC PACIFIC

FILTERING OUT SPAM AND SCAMS

Spam is no longer simply a time-consuming irritant. It is a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts and could cause a loss of service or degradation in the performance of network resources and email gateways.

Symantec's latest *Internet Security Threat Report Vol. XIII* (an update of Internet threat activity in the Asia-Pacific/Japan region from July to December 2007) found that spam made up 71 percent of all monitored email traffic globally. Out of all these spam emails, 0.16 percent contained malicious code. This means that one out of every 617 spam messages blocked by Symantec Brightmail AntiSpam contained malicious code. Symantec's monthly State of Spam report also found that spam levels have been steadily increasing from an average of 66 percent of all messages in July 2007 to 78 percent in July 2008.

For businesses, the economic impact of spam, spyware, and the like are all too clear. Not only do these threats impact productivity, network bandwidth, hardware resource, and support, they also introduce serious legal liability issues and undermine hard-earned corporate brands and reputations.

In the face of such mixed threats, what are concerned businesses to do? Problems such as spam and spyware threaten to undermine the integrity of a company's information. Corporate information must remain secure, reliable, and available at all times. And because spam and spyware utilize the same vehicle—the Internet—as legitimate business-critical communications, the challenge is to ensure that wanted information exchange continues while unwanted activity is halted.

Keeping spam, spyware, and other threats out of the workplace requires a powerful combination of information security technologies, including antispam, antivirus, firewalls, and policy management.

Today's spam attacks

Spammers today use a number of tactics to evade detection by antispam solutions with only limited filtering abilities. As a result, the most effective antispam solutions such as Symantec Mail Security 8300 Series employ a variety of filtering techniques to stop complex spam attacks in real time—without compromising accuracy. Essential filtering technologies in an antispam solution include:

Reputation Filtering: Reputation filtering examines the quality or reputation of the sending source or mail server of a spam message. This type of filtering can identify Internet protocol addresses that are suspect servers or open proxies used by spammers as well as servers from which no spam is sent.

URL Filters: URL filters, in turn, identify spam URLs in messages and remove characters that conceal a Web site address in a message. This type of filtering is very effective against disguised URLs, extreme randomization, and very short messages.

Heuristics Capabilities: Heuristic capabilities are characterized by programs that are self-learning, or in other words, they get better with experience. Heuristics offer a highly effective defense against new spam by analyzing the header, body, and envelope information of incoming messages and looking for distinct spam characteristics such as the inclusion of excessive exclamation marks or capital letters. While poor heuristics do little more than create an administrative burden by producing countless false positives, the best heuristics can result in near-perfect accuracy.

Signature Technology: Signature technology also plays an important role in filtering out spam. The most advanced signature technology actually strips random HTML from spam and counteracts the variations that spammers often insert, resulting in a potent answer to today's highly randomized, HTML-based spam attacks. Similar signature technology is also used to identify embedded images, executables, zip files, and other message attachments through which spammers entice recipients.

continues on Page 25

From Page 24 — Filtering out Spam and Scams

Foreign Language Identification: Foreign language identification is another essential spam filtering technique, which can identify the 10 to 20 percent of all global spam that is sent in non-English languages.

Mixing It Up

Effective protection against today's complex threat landscape, where spam is blended with malicious threats, requires that businesses employ a combination of information security solutions.

Antivirus technology works to identify viruses, worms, and spyware, which are often distributed through spam. When updated regularly and configured appropriately, antivirus solutions can automatically delete or clean malicious messages, including mass-mailing worms that can result in hundreds of spam messages.

Additionally, firewalls that are configured to allow only authorized outbound traffic can also reduce the threat of spyware and other malicious code that attempts to phone home over the Internet without the user's knowledge or permission or tries to launch fraudulent applications. Firewall rules also can be created to block access to known spyware sources.

Furthermore, corporate information security policies can be updated to ensure that file-sharing and other software is correctly implemented and that appropriate usage policies are in place and being followed. Many of the best Internet firewalls and advanced antivirus applications are circumvented not by experienced hackers, but by careless and/or uninformed employees who have not been trained to recognize and respond to Internet threats. In developing and disseminating a solid, up-to-date information security policy, employees are educated in and reminded of their role in fighting against invading threats. A number of policy management tools are available to streamline this ongoing process, making it easier and less time-consuming to achieve and demonstrate companywide-wide compliance.

Information security technologies provide a sophisticated and effectual deterrent from information security attacks that threaten to undermine the integrity of business-critical information. By utilizing the most innovative and powerful antispam filtering techniques together with antivirus, firewall, and other security technologies, businesses can protect the security and availability of their business information even as new generations of Internet threats emerge.◊

By Eric Hoh,vice president,
Asia South Region and
head of Global Accounts,
Asia Pacific and Japan,
Symantec

THE RESURGENCE OF SPAM

While Bill Gates' 2004 prediction that spam would be eradicated within two years clearly missed the mark, few expected spam's extraordinary resurgence in 2007. Since 2006, spam levels have steadily climbed from 56% of all email hit around 76% of email in the most recent month's report.

While the economy is on the minds of many, it seems it is also on the minds of spammers, who continue to use the economy as a ruse to deliver their messages. Spam levels averaged in at 76.4 percent of all messages in October 2008. This spam level represents a year on year, increase of nearly six percent since October 2007, but a decrease since the 80 percent level in August this year.

Here are some of the very latest top trend trends according to Symantec:

The Holidays are coming: 'Tis the Season for Spam

With the 2008 holiday season approaching, spammers are once again taking a seasonal spam angle and using email to tout such wares as pharmaceutical, product and casino spam.

Rise in Image Spam Linked to Phishing Scams

The connection between a recent rise in image spam and phishing spam emerged in October 2008. Symantec defines image spam as an unsolicited message containing an image in the body. Image spam reached a peak of 52 percent of all spam in January 2007. In September 2008, image spam averaged 2 percent of all spam, but in October 2008, this increased to 9 percent. A direct correlation can be made between the increase in image spam and the increase in phishing attacks that contain financial institution logos during October.

The file size of image spam messages can put a strain on email infrastructure if not managed properly. Nearly 92 percent of image spam monitored in the last 30 days had an average size of between 5-50Kb. When you consider spam messages in total over the last thirty days, only 16 percent fall into the 5-50Kb with the majority (79 percent) of messages falling into the 2-5Kb range.

Lottery Scam, Sister to 419 Spam still continuing

Lottery scam, closely related to Nigerian or 419 spam, continued in October. Two notable lottery scams were observed by Symantec in October 2008. The FIFA World Cup which opens in South Africa in 2010 was targeted in one scam. This lottery scam message claimed that in conjunction with the South Africa 2010 World Cup organizing committee, a drawing had taken place, and the "lucky" email recipient won a jackpot of $USD 800K. In order to claim the prize, the email recipient is instructed to contact a paying agent and provide them with their personal information.

Also observed this month was a lottery scam message relating to the 2012 Olympic Games in London.

Despite being four years away, the lottery scam email claims that the recipient has won £950k. The recipient is also asked to contact the paying agent to claim their money.

Mumbai terrorist attacks bring out the worst in spammers

India recently suffered a shocking terrorist attack, with hostage situations in Mumbai involving Indian nationals as well as tourists and travelers from all over the world. Updates on the terrorists' activity are still being followed closely.

Sadly, spammers would never want to miss the chance to capitalize on the fast-spreading news of this tragic incident, using related headlines for their fraudulent emails with product advertisements or malicious links/attachments. Symantec has come across spam messages showing news headlines regarding the Mumbai terror, but the content inside is completely unrelated and is advertising pills.

This spam technique of using recent tragic news events has become a staple tactic for spammers. Among others events, spammers targeted the Nargis cyclone in Myanmar and the Sichuan earthquake earlier this year. Email recipients are advised not to click on links found in such spam emails.◊

2008 Q1 SECURITY THREAT LANDSCAPE

Web threats are in now way decreasing, in fact according to Sophos Security Threat report Q1 2008, the web now hosts an unprecedented number of threats and continues to be the preferred way for malware authors to deliver their attacks.

According to Sophos, the company discovers a new infected webpage every 5 seconds. This is an average of more than 15,000 every day, three times more than in 2007. Sophos has also discovered that a new spam-related webpage appears almost every 3 seconds.

Mal/Iframe and Mal/ObJS continue to dominate the chart as they did in 2007, with attackers taking advantage of vulnerabilities

The results of research into which countries contain the most malware-hosting websites reveal some interesting changes when compared to 2007, Sophos reports. The US has experienced unprecedented growth in this area, hosting almost half of all infected websites. The country has almost doubled its contribution to the chart compared to 2007, when it was responsible for hosting less than a quarter of compromised websites.

China, which in 2007 was responsible for hosting more than half of the infected websites on the web, has returned to its 2005 standing, playing host to just a third of infected websites.

Thailand has now made its debut to this top 10 list, accounting for 1 percent of the infected websites found by Sophos in the first quarter of 2007.

Email threats, spam and phishing

In the first quarter of 2008, only 1 in 2500 emails was found to be carrying malware – 40 percent less than in 2007. Rather than incorporating malware into the email in the form of an attachment, cybercriminals are using unsolicited email to provide links to compromised websites.

In addition, Sophos experts have discovered many Pushdo campaigns during the first part of 2008. They note that some of the techniques used have been technically sophisticated in an attempt to avoid detection. These techniques involve changing the type of packers used, in which the malware tried to obfuscate itself.

Spam continues to plague computer users. Sophos research reveals that 92.3% of all email was spam during the first quarter of 2008. The security company also finds a new spam-related webpage on average every 3 seconds – 23,300 each day.

This calculation includes pages registered on "freeweb" sites such as Blogspot, Geocities, etc. Sophos predicts this number will increase so long as its authors are making money from such ruses. By ensuring that spam messages are quarantined and not delivered to the recipient, businesses can save not only time and money, but can also help protect their users from emails linking to infected sites.

In an attempt to defeat sender reputation-based filers, the spammers who relied heavily on botnets are trying to abuse free webmail services such as Hotmail. AOL AIM and Gmail. Experts believe that the rise in webmail spam might be related to spammers having bypassed CAPTCHA techniques – a challenge response test used to determine that the user is human.

According to Sophos, the US has decreased its contribution to the spam problem, relaying only 15% of spam, compared to one fifth in 2007.

continues on Page 28

From Page 27 — 2008 Q1 Security Threat Landscape

Sophos is also monitoring a large number of Chinese domains that are being promoted by spam campaigns. Interestingly, there is a 2008 promotion inviting people to register .CN domains for a mere USD 14 cents.

Such a low cost is attractive to spammers as they can register hundred of new domains and rotate them every few minutes during a spam run in order to bypass spam filers that use URL blocklists.

Phishing still remains a huge problem for banks and other financial institutions. It also poses a problem to large online companies like eBay and PayPal. Sophos measured the number of phishing emails targeting these two organizations in 2007, and found that during the first quarter of 2007, 59 percent of phishing campaigns targeted at least one of them.

However, the first quarter of 2008 has registered a massive decrease in the number of campaigns targeting both eBay and PayPal. PayPal has been the target in slightly over 15 percent of phishing campaigns, while eBay has accounted for jus less than 4 percent of all campaigns. Heightened user awareness may be responsible for phishers looking elsewhere to lure in unsuspecting victims to bogus websites. Computer users need to remember to be vigilant when entering confidential data online and only to do so from a fully protected computer.

Spear phishing activities, which target specific organizations, are also seeing a rise, with educational institutions and webmail services being particularly targeted and vulnerable.

While most users have learned how to recognize most standard phishing attempts, they are more likely to trust – and therefore be conned by – emails that purport to be sent from the company's IT or HR department. Sophos advised businesses to exercise extra vigilance in this area.

Data leakage

Stories about organizations from businesses to government agencies losing sensitive data still dominate the press, and Sophos expects this trend to continue in 2008.

Questions remain as to how hackers manage to plant malware even in companies that are PCI compliant. This brings attention to the crucial point that achieving compliance must not lead to complacency. While no security system is perfect, it is worth remembering that the more effort required to steal a company's data, the less attractive a target it becomes.

More Mac malware and vulnerabilities

Although still tiny when compared to the Windows malware problem, Mac users are not unscathed when it comes to malware attacks. During the first quarter of this year, Sophos discovered a new Trojan designed to scare users into purchasing bogus security software, poisoned web adverts that would lead to either a Mac or Windows infection, and vulnerabilities that affected Mac users just as easily as Windows lovers.

With Apple Macintosh's market share on the rise, it seems likely that hackers will increase their attempts to outfox a user population which has often, incorrectly, believed itself to be immune from many internet security threats.

The Future

While the idea of protecting your data has been revamped and re-introduced to the market by many in the security industry, it is not a new concept. Security issues over the last 15 years have revolved around protecting information – from the macro viruses of the early 90s that tampered with and deleted information to today's large-scale data thefts.

Just as technological advancements help legitimate marketers and sales teams to focus their efforts on specific markets quickly, efficiently and cost-effectively, they have also made life easier for hackers. For both the good and the bad guys, improved technology has led to improved return on investment.

This is not the time for companies to bury their heads in the sand and hope no one notices any gaping security holes in their network. Today, attacks are sophisticated, well-funded and at large. Putting in place an up-to-date security policy that defends your web and email gateway, proactively protects your endpoint computers and mobile devices, and educates your users on appropriate and acceptable online behavior can make an organization a very unattractive target indeed.◊

Condensed from Sophos Security Threat Report Q1 08

THE CONTINUOUS HURDLE OF SPAM

The birth of the internet communication has brought us much convenience and ironically hindrance. The well known spam problem which came about in the early 1990s proves to be a continuous one.

No one in the past would have thought it was possible and easy to get PC and network users to install viruses, worms, application-downloading Trojan horses and other forms of malware on their computers. Today, it is estimated that 10 to 25 percent of all PCs in the world are part of botnets and the number is a constant flux. Albeit increasingly hidden, spam has become a significant topic of discussion and revenue generator of the internet world today.

Just last year, the storm spam-malware hybrid was thought to grow to become the largest and most notorious of spam-driven robot networks breed. What was frightening about the Storm group then wasn't the fact that they had built such a large botnet, but that they proved large number of systems could be compromised by simply asking end users to install all kinds of malicious applications. People adhered.

Next came the part where botnets were duping Internet users into giving them the means to grow their businesses through the very same methods that spurred e-commerce growth – online marketing programs and email advertising. The masses were clicking on E-mail spam, banner ads, legitimate Web sites, image and .PDF files, which were all being co-opted and used as malware carriers, installing viruses, Trojan horses, worms and other forms of malware, on to e-mail recipients' and Web surfers' PCs, turning them into a network of remotely controlled and "zombified" slaves. To this day, botnets are still an ongoing problem because they allow spammers to scale without increasing their ability to be detected.

Another thing that is changing with spam patterns is the degree of sophistication and the scale of the botnets spam manufacturers employ today. It takes only a number of weeks to see the majority of spammers utilizing these same methods, which on a given day can decrease any organization's effectiveness and revenue significantly.

Following a brief period of latency, massive Storm-driven spam attacks again lighted up everyone's radar screens. Spam links to MP3 audio files, YouTube videos and Adobe .pdf documents are being used to gull recipients into downloading infected attachments and visiting Web sites that serve as malware distribution nodes, in turn further infecting their PCs and luring them into part of a network of remotely controlled zombie slaves.

Presently, the latest evolutionary wave follows an earlier Storm-driven spam onslaught in which users are lured into pump-and-dump stock trading schemes. How it works according to Kaspersky lab is that the first mass mailing of stock trading spam uses specially crafted graphic files that contained background noise, as well as Adobe .pdf files, which during the time are not detected by spam filters. Storm and other spam creators are extremely notorious for making creative use of timely events and topics such as, dancing skeletons for Halloween, cheap pharmaceuticals and prescriptions, electronic greeting cards, advertisements for credit reports, electronic discount shopping vouchers, and more that would entice recipients to open the file attachments or links to the websites.

So, can the spam problem ever be conquered? The fact is that while the risks can be minimized, spam cannot be totally eliminated as it has evolved into somewhat of a social problem. On top of this, the spam market today is valued at approximately several hundred million dollars annually. Being such a lucrative business, it is unlikely that spammers will ever be a dying breed. How can it as long as there are people who are willing to take risks and potentially make a quick fat profit?

One of the ways to minimize risks is to educate people on how they can start protecting their own computers, such as installing anti-virus software to prevent them from being used as botnets.

Secondly, the tools that are being used to create 'Storm' spam for example must not be readily available and accessible.

One of the ways to minimize risks is to educate people on how they can start protecting their own computers, such as installing anti-virus software to prevent them from being used as botnets.

continues on Page 30

From Page 29 — The Continuous Hurdle of Spam

Being human, more often than not our curious nature urges us to explore and question the origin and how things are created. With readily available tools on spam creation, curiosity kills the cat; this will slowly and potentially develop into a challenge and competition against the time taken to create spam, defend the users and complying with the laws. In addition, there is currently no financial incentive that encourages site operators such as Internet Service Providers to take action against botnets.

It is also difficult to charge a person if his computer becomes a victim of botnets unknowingly.

Today, there are legal issues surrounding spam/phishing processes in each country, with the United States leading the CAN-SPAM Act of 2003. In a recent case in United States, a social networking giant is set to receive $6million for a lawsuit the company filed against "Spam King" Scott Richter, who inundated its members with unwanted spam from hijacked accounts in August 2006. This lawsuit was filed under the CAN SPAM Act. So far, under this ACT, the law has managed to catch up with other 'Spam Kings' such as Alan Robert Soloway for spamming Microsoft's Hotmail Service in 2005, Alan Rasky and Sanford for international illegal spamming and stock fraud scheme.

The problem with spam will reach a stage where serious measures need to be emphasized and implemented and this will ONLY happen as a result of a breach to a large organization or government, causing massive financial loss and a tarnished reputation.

We, as consumers will need to be constantly vigilant and keep a lookout on all possible spam such as Nigerian scams, weight-loss claims, foreign lotteries and even fake investment schemes.

For now, spammers will continue investing in this profitable business, fighting the law enforcement agencies. Besides legislation and anti-spam devices, to ensure spam does not overtake our life maliciously, we can and should play a part to ensure the stop of this globally infectious disease.◊

By Stree Naidu,
Regional Vice President,
APAC & Japan,
Tumbleweed, now part of Axway

SPAM FILTERS ARE ADAPTIVE

91 percent of all spam filter manufacturers use artificial intelligence (AI) based filters. This has been established by a market survey of "spam filters" by Absolit Dr. Schwarz Consulting. The study examines 47 products on their filter methods. "Today, who has spam mail in his inbox has to blame himself alone. Modern filter methods block more than 99 percent of incoming spam mails, without loosing one single important e-mail ", says the e-mail expert Dr. Torsten Schwarz.

The approach of the artificial intelligence uses heuristic filters to arrange e-mails in mostly predefined classes (spam, no spam). In doing so, the self-learning filters compare new messages to already learned facts and as a result determine whether an e-mail is spam or not. An excessive use of special characters and capital letters, hidden HTML texts, unsubscribe lines (supposed possibility to opt-out from the list) and a high frequency of certain catchwords can be indicators of spam. These attributes are weighted with a score, which classifies an e-mail as spam if it crosses a specific number.

" Once the filters are trained, they adapt further on their own and even fit themselves to new techniques of spammers", says Janine Bonk, the author of the study. The filters orientate themselves by monitoring the typical e-mail behavior of the user. If, for instance, the user works in a bank, e-mails which contain repeatedly the word loan or the dollar-sign are not defined as spam. The quality of the filter depends highly on the quality of the training. If a filter is not well coached, it can generate a high interest in false positives. Most filters are already pretrained when purchased, but matching with one's own e-mail behavior must still be adapted. That's why it takes a little bit time until heuristic filters work perfectly.◊

Dr. ABSOLIT Schwarz Consulting offers independent strategy consultation on e-mail marketing and integration of electronic media

http://www.absolit.de

LIBERATING THE INBOX: HOW TO MAKE EMAIL SAFE AND PRODUCTIVE AGAIN

With spam levels breaking records every day, the quintessential business tool – email – has simultaneously become a major liability. With inboxes overrun with more and more unwanted email that threatens business productivity, regulatory compliance, and network security, organizations are having to look at what is being mailed in, out and around their network, at the gateway, at the mail server and at the endpoint.

Paul Ducklin, Head of Technology for Asia Pacific at Sophos, zooms in on the threats posed by unwanted emails that make it through to the inbox, explains the impact these threats have on organizations, and demonstrates what needs to be done in response to make email safe and productive.

Email in a business

Email today presents a serious risk to security, business productivity, and compliance with government and industry regulations. As the use of email for legitimate business purposes continue to go upwards, so does its use as a tool for unwanted, illegitimate, and occasionally dangerous, business activity. There are three predominant sources of risk that every organization faces: spam, information leakage, and compliance as it relates to email.

Spam

Professional spammers continue to clog up to 90 percent of unprotected mail stores and inboxes with unwanted emails that soak up bandwidth, upset end users with irritating or offensive content, and negatively impact employee productivity.

More recently, spammers have extended their role from the simply annoying to the outright criminal, using their emails as a beachhead for more malicious activity. As security vendors have become adept at blocking emails containing code which itself has a viral payload, spammers and malicious code writers have found more devious ways – such as the use of images and PDF attachments – to get spyware, zombie-creating Trojans, and other malware on to end-users' desktops.

Cybercriminals are increasingly spamming out emails offering, for example, a plug-in to view videos or pornography or even offering free bogus security applications. The emailed link in reality takes the duped user to an infected website from which a backdoor Trojan is downloaded. When the webpage loads, malware on the website infects the visiting computer, and is then used for a variety of criminal purposes, such as to steal data or to turn the computer into a spam-sending zombie. Phishing attacks continue to lure unwary users to fake websites where they hand over confidential information, such as bank or credit card details.

The reason spam continues to flourish is because it works. It can take just one person to hand over their money or their financial details – wittingly or by having them stolen – for a campaign to be successful.

The vast amounts of money accrued by spammers who have been arrested and prosecuted is an indication of just how much money can be made, and the handful of cybercriminals who are caught is nothing compared to the huge numbers left undetected to carry on their campaigns. In today's workplace, the task of blocking the wealth of malicious and productivity-hampering email, while allowing the free flow of legitimate business communication, is one of the biggest challenges IT departments face.

Email security – a multi-layer issue

In the past, organizations viewed the problems of email almost solely as an inbound threat – spam and email-borne malware causing a nuisance, consuming bandwidth and storage space, and increasingly infecting endpoint computers. As described above, the situation now is much more complex, and the threats posed by email exist throughout the whole email infrastructure. As networks increase in size and complexity and email use grows, more points in the system become vulnerable. Inbound, outbound and internal messaging are all vulnerable and need to be secured as part of an organization's overall network and data security.

Gateway security – inbound and outbound

The gateway remains the place where email protection "tradition -ally" sits, providing protection against threats such as spam and phishing attacks, viruses, denial of service attacks and

continues on Page 32

From Page 31— Liberating the Inbox

directory harvest attacks.

It is also at the gateway that offensive and other inappropriate inbound emails are blocked before they can reach the corporate servers. Outbound emails containing confidential or sensitive information or emails that flout regulatory or corporate compliance rules can also be effectively stopped here. As a result outbound content monitoring and filtering is an increasingly strategic concern for IT administrators.

Groupware security – internal

Internal threats are rapidly climbing the priority list of enterprise security threats and now account for three of the top 10 most serious threats facing corporations today – unintentional employee error, data stolen by an employee or business partner, and insider sabotage.

The threats associated with inbound and outbound mail – malicious emails, inappropriate content, confidentiality and compliance breaches – all apply at the groupware level, with internal mail servers acting as the conduit for all traffic. In addition, malware can remain dormant in stored email attachments, posing a threat to the wider network long after they enter the organization.

Endpoint security – the last line of defense

An additional, and perennially significant threat, is that of malware entering the organization at the endpoint desktops, laptops, and notebooks via, for example, webmail or a USB memory stick can use the internal mail network to spread. Within the context of the email system, the endpoint is the final line of defense.

Making email safer

While most organizations have experienced dramatic growth in their email infrastructure, many have not seen a corresponding increase in email security – even though email is already the number one source of security threats for organizations. Email protection has tended to be focused on the gateway, although there are in reality many points of vulnerability in an email system. This approach, as has been discussed, can leave a network exposed to a host of email related threats that bypass the gateway defenses. The traditional gateway email hygiene model is, therefore, now incomplete.

The key to making email safer is to secure all the points of vulnerability – protecting all layers and ensuring that the gateway and groupware solutions integrate anti-virus, anti-spyware, anti-phishing and anti-spam protection and also provide the ability to filter email for dangerous, unwanted or confidential content.

Maintaining up-to-date endpoint protection is vital to preventing infection via other means, as highlighted above. At all points, it is essential to provide completely up-to-date, proactive protection against the full range of malware threats. Leading anti-virus and anti-spam engines automatically detect variants of spam campaigns or virus families, providing a more deterministic approach to protection.

There also needs to be a clear and transparent framework for behavior, setting down what is acceptable and what is not when it comes to using email. An explicit, organization-wide Acceptable Use Policy (AUP), accompanied by the ability to audit its use and enforce its rules is a simple first step in demonstrating the intention to meet regulations and goes a long way toward avoiding liability.

Making email more productive

Just as there needs to be robust security to protect against malware, spam, denial-of-service attacks, directory harvesting, and so on, so there need to be capabilities in any solution that will let administrators enforce content filtering management and information leakage prevention policies. For example, security solutions should be able to automatically monitor email communications for keywords, strings such as Social Security numbers, and file types that might contain proprietary information.

There need also to be management features that lower the administrative overhead, giving administrators visibility and reporting capabilities that allow them proper control over the whole email infrastructure. This includes the ability to trace messages as they flow through the email infrastructure, and the ability to generate traffic and threat reports quickly and easily in order to paint a clear picture of what is passing through. This is particularly important in response to inquiries from senior management.

continues on Page 33

GUARANTEE A CLEAR OPPORTUNITY TO OPT OUT

The CAN-SPAM which is adopted by many governments demands a "clear and conspicuous" e-mail opt-out mechanisms. Some of its important aspects are briefly listed here that you should take them into consideration when sending out messages via e-mail:

- Don't ask for unnecessary information;
- Don't be a pedant, regarding misspelling and don't send a message containing just a - cryptic error message and number;
- Don't require to log in to your site to unsubscribe. Your site isn't that important;
- Don't make your reader say it twice, when he asks to be removed;
- Offer a variety of e-mail communications so that your reader has choices and may stay on your list;
- Handle it in real time, so remove the email address as soon as possible;
- If an error occurs while removing an address, don't just display a cryptic error message - instead send e.g. a friendly message telling how the address can still be removed.
- Send a confirmation notice with a link that invites to re-subscribe. It could have happened that someone unsubscribed by accident, or someone else unsubscribed the person without permission.

The recipient decides what e-mail he accepts and especially how often – and it's his choice! Of course none of us wants to see the circulation lists shrink, but nevertheless the unsubscribe process shouldn't be problematic for those who want to be removed.◊

From Page 32 — Liberating the Inbox

Summary

Since email is a mission-critical business tool, organizations have no choice about learning to cope with its related security challenges, both external and internal. There are ways to make this easier in terms of impact on users, security administrators, and the organization as a whole.

It is possible to regain control of inboxes despite the changing nature of malware and spam, and it is possible to do this efficiently.

Approaching email from the point of view of the infrastructure will help identify where best to put in place checks and balances. For example, archiving is best left to the groupware level, because it is here that internal as well as inbound and outbound mail can be captured.

Following the four basic principles for making email safe and productive – maintaining proactive, up-to-date protection against malware, phishing and spam, implementing an AUP, creating archiving and reporting processes, and monitoring and filtering content – will in the long run ensure an organization's system, and its users' inboxes, are freed from the tyranny of malware and spam.◊

THE GREAT BALANCING ACT: JUGGLING COLLABORATION AND AUTHENTICATION IN GOVERNMENT IT

At a time when emphasis in government is on the elimination of silos and promotion of secure collaboration across and within agencies, government IT managers are under the gun to ensure that the right people have the right access to the right resources.

Anytime, anywhere network access is critical for the effective and timely operation of government, particularly during times of crisis or disruption. Technological advancements over the past decade have created tremendous opportunity for federal agencies to provide employees and contractors with remote access to government resources, presenting greater potential for collaboration regardless of location. However, remote access can open a Pandora's box of security and authentication challenges for IT managers tasked with protecting sensitive data and preventing vulnerabilities and intrusions.

A typical government agency employs a wide range of personnel with a variety of security clearances in offices across the nation. Add to that a large number of part-time employees, contractors and consultants, and federal IT managers are faced with a daunting task: maintaining the delicate balance between securing the network and promoting collaboration across a diverse group of workers using a variety of endpoint devices. The need for authenticated network access control is increasingly important to ensure that individuals are granted the appropriate levels of access to the tools and information they need to effectively collaborate — around -the-clock and regardless of their location or device used.

So Many Users, So Many Authentication Challenges

The concept seems simple, but consider that on any given day federal agencies are confronted with having to provide just the right levels of access for an expanded set of users (guests, partners, contractors, employees) accessing the network from a wide range of mobile devices (both managed as well as unmanaged devices). It's a task that can quickly become unwieldy and ineffective from an identity management perspective.

When controlling remote network access, government agencies need to employ a holistic security approach that integrates authentication, data encryption and data protection. Two critical elements of identity management must be considered, namely:

Establishing effective authentication policies

Ensuring that only authenticated and authorized users have access to the appropriate applications is critical to regulate the flow of information accurately. Ensuring endpoint security compliance is also increasing in importance due to the mobility aspect highlighted above and the consequent security concerns associated with users accessing the network from personal laptops that may not comply with the security policies of the agency's network.

Managing user identity is particularly important for government agencies due to highly-sensitive data that could be compromised if the wrong user is given a higher level of access than is approved for their role. The first step in identity management is the creation of a set of policies that establish who is permitted access to what information and under what conditions. These parameters must apply regardless of user location or endpoint device.

Deploying appropriate technology "gatekeepers"

continues on Page 35

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 ◊

From Page 34 — The Great Balancing Act

As government users require network access from a number of locations, varying from the most carefully managed networks to vulnerable wireless "hotspots," the network must employ technology to enforce authentication policies for those seeking access and the equipment they are using. Comprehensive "network policing" of end users and equipment ensures appropriate authorization that protects against viruses, intrusions and other security breaches.

Secure Sockets Layer Virtual Private Networks (SSL/VPNs) are a superior means of gathering user identity and establishing endpoint security, while providing granular user access policy adherence. Coupled with firewalls and intrusion detection and prevention (IDP) solutions, agencies can ensure comprehensive network protection that lends insight beyond just IP addresses into who is actually traversing the network perimeter and what specific applications they are accessing. In addition, SSL VPN platforms can collaborate with IDP solutions to ensure that malicious, non-compliant users be quarantined and taken off the network, thereby proving end-to-end, real-time network protection.

While remote access can enhance inter- and intra-agency collaboration, federal IT managers must also ensure that users do so *securely* and *reliably*. With a robust access management solution that integrates network security, government agencies can create a responsive and trusted environment for accelerating the delivery of intelligence and vital resources to better serve and protect its constituents.◊

By Kang Eu Ween, Regional Enterprise Solutions Director, Juniper Networks

HOW TO AVOID SPAM

Spam is seen as a minor annoyance by some users, while others are so overwhelmed with spam that they are forced to switch e-mail addresses. But just how did spammers get your e-mail address in the first place? The answer usually boils down to the individual's online behaviour.

Research shows that e-mail addresses posted on websites or in newsgroups attract the most spam. Spammers use software harvesting programs such as robots or spiders to record e-mail addresses listed on websites, including both personal and institutional web pages.

Some spam is generated through attacks on mail servers, methods that don't rely on the collection of e-mail addresses at all. In "brute force" attacks and "dictionary" attacks, spam programs send spam to every possible combination of letters at a domain, or to common names and words.

While these attacks can be blocked, some spam is still likely to get through. Currently, there is no foolproof way to prevent spam, but educating users is still the crucial factor in fighting the nuisance.

Check out the following methods to prevent spam:

Disguise e-mail addresses posted in a public electronic place

Opt out of member directories that may place your e-mail address online.

If your employer places your e-mail address online, ask your webmaster to make sure it is disguised in some way.

Be on guard when filling out online forms requesting your e-mail address

If you don't want to receive e-mails from a website operator, don't give them your e-mail address unless they offer the option of declining to receive e-mail. If you are asked for your e-mail address in an online setting such as a form, make sure you pay attention to any options discussing how the address will be used. Pay attention to check boxes that request the right to send you e-mails or share your e-mail address with partners. Read the privacy policies of websites.

Use multiple e-mail addresses

When posting to newsgroups or using unfamiliar websites, we recommend creating a particular e-mail address for that specific purpose. An online search for "disposable e-mail addresses" provides you immediately with a list of e-mail providers designed for one-time use e-mails.

Use a filter

Many ISPs and free e-mail services now provide spam filtering. You may also consider simply buying the appropriate software. Although filters are not perfect, they can certainly cut down the amount of spam a user receives.

Avoid using short e-mail addresses

They are easy to guess, and may receive more spam.

Pay attention to stripping specific non-essential attachment type files

It's proven that files that end with .bat, .exe, .pif, .scr, .vbs, or .crd often contain worms and viruses.◊

By Daniela La Marca

HOW TO ENSURE YOUR E-MAILS ARE NOT CLASSIFIED AS SPAM

Commercial e-mails have in general a sales focus - but that's exactly very often the criteria spam filter manufacturers make use of to identify spam. Attached you will find some tips which are quite easy to implement, so that your own mailing is not declared as spam.

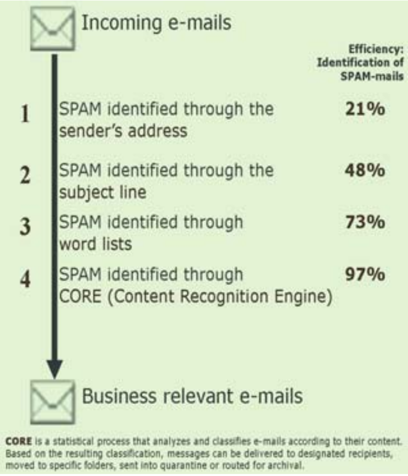
The race of the spam producers versus the anti-spam software solution providers is in full swing. While professional spammers vehemently try to outsmart the always improving filter solutions, unaware e-marketers often only stand on the sidelines and wonder why their e-mails apparently do not reach their customers. Yet, it is not so difficult to ensure that your e-mails aren't thrown out by spam filters.

Write the name of the addressee correctly

Next to the intrinsic e-mail address, the complete name belongs in the " To: " line of every e-mail. Accompanied with a personal salutation in the body of the mail, the risk of being blocked by spam filters already sinks significantly. Among the millions of spam mails which are dispatched daily, only a few e-mails can be found which correspond to this exemplary pattern. Spam filters are aware of this and therefore are more likely to bend the rules with properly addressed e-mails.

Use a genuine sender's address

Not only the address of the addressee, but also the one of the sender states a lot about the quality to be expected of the e-mail contents. E-mail marketing activities, which for organizational reasons aren't sent by a personal sender's address, are more likely delivered, if the sender's address consists of entire word or name combinations like for example newsletter@company.com.sg or John.Smith@company.com.sg.



Incoming e-mails

		Efficiency: Identification of SPAM-mails
1	SPAM identified through the sender's address	21%
2	SPAM identified through the subject line	48%
3	SPAM identified through word lists	73%
4	SPAM identified through CORE (Content Recognition Engine)	97%

Business relevant e-mails

CORE is a statistical process that analyzes and classifies e-mails according to their content. Based on the resulting classification, messages can be delivered to designated recipients, moved to specific folders, sent into quarantine or routed for archival.

Do not use cryptic characters, slogans, or abbreviations in the reference line

Spam filters are sensitive to certain buzz words, cryptic characters, slogans, abbreviations or even empty subject fields. Reference lines like, *WIN NOW* or *200% IN ONLY ONE WEEK* are classified and rightly eliminated as spam.

Don't use "non-words" in the mail body

The active wordlists of spam filters provide an immediate confiscation of the mail, if fishy words are detected.

Advanced solutions even permit a weighing of single words, so that if a defined threshold value is exceeded, the whole mail quickly gets moved into quarantine. That's why flowery phrases in the body of the e-mail should be avoided, besides the already mentioned slogans in the reference line, as for example "Super -Extraordinary-Special-Offer " and abbreviations like XXL, XXX, or similar. The best approach is to set the benchmark with common word and style elements of a classical professional letter.

Choose your e-mail appendix or attachment carefully

Appendices in JPG or DOC format are also often used by spammers. The Adobe Portable Document format, shortly named PDF on the other hand, has not yet been discovered as an appendix of a spam mail. So, if you dispatch your newsletter with an appendix, it is best to use the PDF format.

Avoid HTML versions

Graphics lovers will not like this tip, yet: It's proven that spammers have a preference for HTML formatted e-mails. Those of you who avoid this and stick to formulating e-mails as " plain text ", perhaps with hyperlinks to adequate, nicely formed web pages, endears himself to filters.

The inner workings of modern anti-spam filters

The following table shows the modus operandi of advanced anti-spam software. Steps 1-3 have already been explained.

Step 4 shows the latest statistical process technology which automatically categorizes e-mails with high accuracy as SPAM or NOT SPAM, after individual setup by the receiver.

No chance anymore?!

Many programs also use individual based Anti-SPAM lists. Once your e-mails have landed in such a personal exclusion list of a receiver, further contact with this addressee will be impossible.¨◊

By Daniela La Marca

*Based on
" So werden E-Mails nicht als Spam klassifiziert" by Markus Goss, VP Marketing, GROUP Technologies AG, Germany*

BLUE COAT S TOP SECURITY TRENDS FOR 2008

The Hack is back! Actually ill-intentioned hackers (who were never really gone) will continue to inject Mobile Malicious Code (MMC) into otherwise reputable sites.

Using SQL and iframe injections, plus other attacks, hackers go on infecting popular, legitimate Web sites with malicious code. Typically, the infections are timed for peak traffic at the site. The worst part is that visitors don't have to explicitly download any content to have their own machines infected. Simply browsing or "driving by" sections of these infected sites allows evil scripts to embed themselves in customer PCs and do tremendous damage. Because these are well-known, reputable sites—some of the most trusted names in online news and commerce—URL-filtering and reputation tools won't block users from visiting them.

Web sites will remain vulnerable to attack until security training and testing become mandatory for Web developers.

Web site developers are busy learning about new technologies such as Adobe Flex and Microsoft Silverlight. Security remains an afterthought. As well, evildoers continue to develop new programs for breaking through firewalls and infiltrating HTTP applications and SSL communications continues. To stay safe requires vigilance and reliable security solutions.

Malware infections will spread through widgets in Web sites and dashboards.

Even hailing from such leading developers as Microsoft and Yahoo!, widgets have been found to have insufficient security features, leaving them vulnerable to infection. Because widgets often have access to the host operating system, they pose major risks to users.

Thieves and "ne'er-do-wells" will continue to target laptops harboring valuable identity-based information.

The black market for personal records (about US$14/name) makes laptops attractive targets for thieves. A laptop with records for 10,000 employees, for example, is worth about $140,000 on the black market. Not bad for a dishonest day's work!

Online videos will become a channel for attacks.

Cisco has already had to patch its VOIP protocol to close a security loophole. Vulnerabilities surely exist in video formats, as well. The ever-growing popularity of videos and video sites such as YouTube ensures that hackers will not neglect this format for long.

Infected devices might even be sitting on your living room mantel!

Digital picture frames and memory sticks are now vulnerable to attack

In February, a major electronics retailer warned customers that a popular model of digital picture frame, which connects to a computer over a USB port to display images, had become infected with the Mocmex Trojan Horse. The popularity of digital photography and music downloads is leading users to connect a wide variety of devices to their computers. Unfortunately, not all these devices are safe.

Storm warning! Botnets, like the Storm botnet, will be responsible for the bulk of spam and malware infections this year.

Major botnets (networks of infected computers) are now for rent to spammers and criminals. The Storm botnet, comprising over 85,000 machines infected by a Trojan, sent about 20% of the world's spam in 2007.

continues on Page 39

From Page 38 — Blue Coat's Top Security Trends for 2008

Researchers have recently discovered new, even more insidious botnets, such as MayDay.

Through social network sites, we'll find old friends—and new malware.

Facebook and MySpace continue to add users at an impressive clip, but these sites and their myriad applications are vulnerable to attack. For example, security researchers recently identified Facebook's image uploader as a significant threat to end user security.

In response to identity thefts, companies will begin using custom identity numbers rather than Social Security numbers to identify individuals.

New identity standards such as Open ID will gain popularity as organizations try to minimize exposure to identity theft.

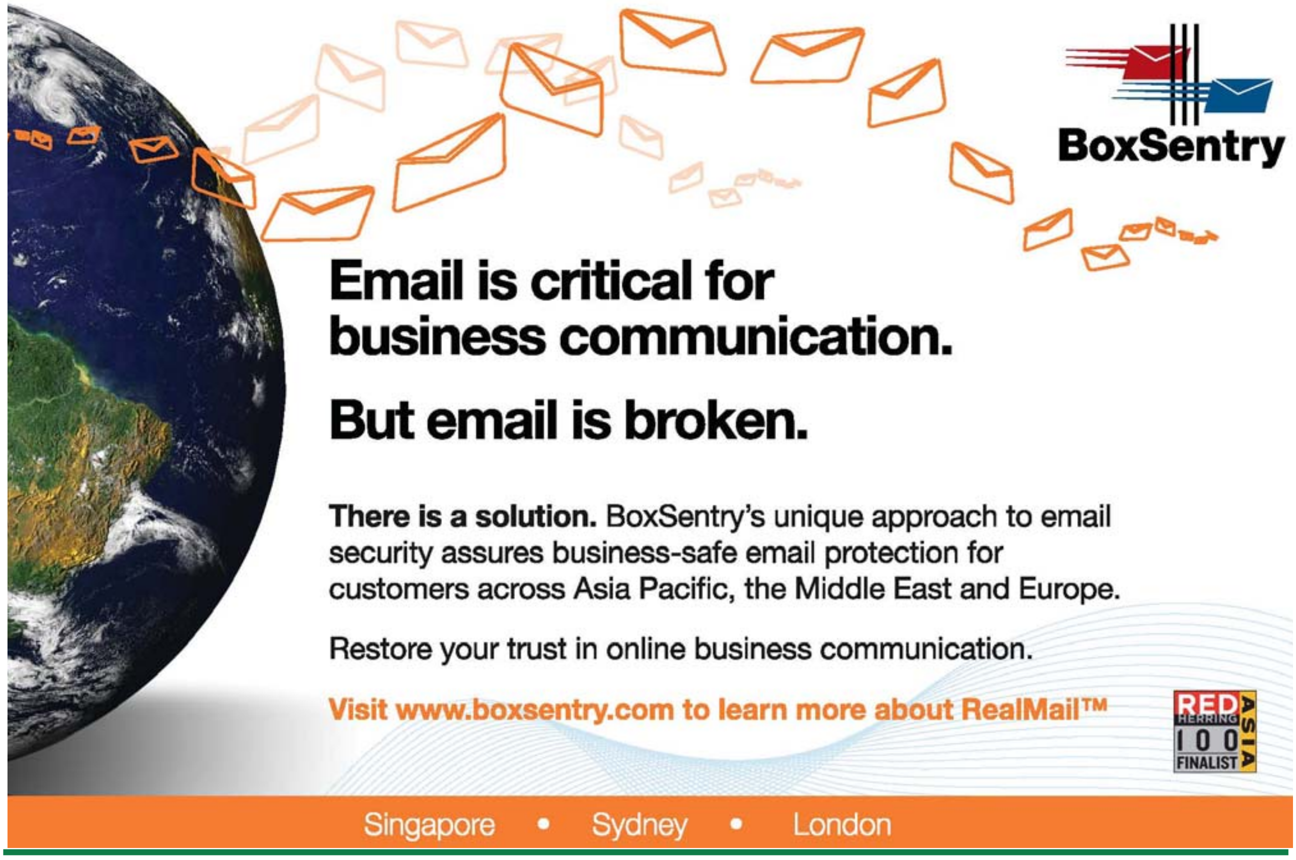
Web security will continue to be thwarted by the performance and scalability limitation of most Web gateway products.

A "dirty little secret" of the IT security industry is that most Web security gateway products are architecturally incapable of scaling to meet enterprise needs. Enterprises will continue to find themselves short-changed by products that promise comprehensive network protection but don't deliver on performance.

Conclusion

Security threats still abound and some can be disastrous to company IT infrastructure and corporate data. To better protect your organization, Blue Coat suggests:

- Be aware and keep current of these threats
- Learn how to recognize their format and pattern and watch for them
- Educate all members of the IT Dept and Senior Managers
- Deploy tools to help you protect your data
- Do research and look for vendor tools that provide you with not just desktop anti virus protection, but also:
- Distributed application threat monitoring
- Information on employee web browsing activity
- Prevention from virus injected reputable web sites
- Filtering to block malicious URLs and code
- Laptop lock down and recovery processes ◊



THE UNDERGROUND ECONOMY

Symantec recently released a detailed study on cybercrime delving into an online underground economy that has matured into an efficient, global marketplace in which stolen goods and fraud-related services are regularly bought and sold, and where the estimated value of goods offered by individual traders is measured in millions of dollars. The report is derived from data gathered by Symantec's Security Technology and Response (STAR) organization, from underground economy servers between July 1, 2007 and June 30, 2008.

Two of the most common platforms available to participants in the online underground economy are channels on IRC servers and Web-based forums. Both feature discussion groups that participants use to buy and sell fraudulent goods and services. Items sold include credit card data, bank account credentials, email accounts, and just about any other information that can be exploited for profit. Services can include cashiers who can transfer funds from stolen accounts into true currency, phishing and scam page hosting, and job advertisements for roles such as scam developers or phishing partners. Advertisers on underground channels attempt to capture attention for their messages using techniques such as capitalization, multi-colored text, ASCII flares, and repeated sales pitches across multiple lines (similar to blanketing a wall with the same advertising poster). Typical advertisements list the available items, prices, and other details such as payment options, contact information, and qualifiers to describe their goods such as "100% successful," "fast," or "legit".

Since these channels are "always open," advertisers often use scripts to schedule automatic message broadcasts across many servers and channels. Along with selling specific items, advertisements are also posted requesting particular goods and services, such as credit cards from a certain country, or a cashier of a specific gender.

Many of the goods and services advertised on underground economy servers form a self-sustaining marketplace. For example, spam and phishing attempts are attractive because of their effectiveness in harvesting credit card information and financial accounts. Along with the potential financial gain from the sale of such information, the profits can also help build an underground economy business as profits from one exploit can be reinvested and used to hire developers for other scams, used to purchase new malicious code or new phishing toolkits, and so on.

The potential value of total advertised goods observed by Symantec was more than $276 million for the reporting period. This value was determined using the advertised prices of the goods and services and measured how much advertisers would make if they liquidated their inventory.

Credit card information is the most advertised category of goods and services on the underground economy, accounting for 31 percent of the total. While stolen credit card numbers sell for as little as $0.10 to $25 per card, the average advertised stolen credit card limit observed by Symantec was more than $4,000. Symantec has calculated that the potential worth of all credit cards advertised during the reporting period was $5.3 billion. The popularity of credit cards are easy to use for online shopping and it's often difficult for merchants or credit providers to identify and address fraudulent transactions before fraudsters complete these transactions and receive their goods. Also, credit card information is often sold to fraudsters in bulk, with discounts or free numbers provided with larger purchases.

The second most common category of goods and services advertised was financial accounts at 20 percent of the total. While stolen bank account information sells for between $10 and $1,000, the average advertised stolen bank account balance is nearly $40,000. Calculating the average advertised balance of a bank account together with the average price for stolen bank account numbers, the worth of the bank accounts advertised during this reporting period was $1.7 billion. The popularity of financial account information is likely due to its potential for high payouts and the speed at which payouts can be made. In one case, financial accounts were cashed out online to untraceable locations in less than 15 minutes.

During the reporting period, Symantec observed 69,130 distinct active advertisers and 44,321,095 total messages posted to underground forums.

continues on Page 41

From Page 40 — The Underground Economy

The potential value of the total advertised goods for the top 10 most active advertisers was $16.3 million for credit cards and $2 million for bank accounts. Furthermore, the potential worth of the goods advertised by the single most active advertiser identified by Symantec during the study period was $6.4 million.

Malicious tools

Malicious tools enable attackers to gain access to a variety of valuable resources such as identities, credentials, hacked hosts, and other goods and services. Some malicious tools and services are designed to counter security measures such as antivirus software to increase the lifespan of a malicious code sample in the wild. The result is a cycle whereby malicious tools must be continuously developed and used to produce other goods and services. The profits from these goods and services may then be reinvested into the development of new malicious tools and services.

Tools range from kits that automatically scan and exploit vulnerabilities to botnets. These tools may be used to provide services such as denial-of-service (DoS) attacks, spamming and phishing campaigns, and finding exploitable websites and servers. They can also be used to generate a number of goods, such as compromised hosts, credentials, personal information, credit card data, and email addresses.

The highest priced attack tool, on average, during this reporting period was botnets, which sold for an average of $225. A botnet can persistently produce many other goods and services; it can be rented out for specific attacks or on a periodic basis; and it can be upgraded to create new sources of revenue.

Exploits are another effective malicious tool. Exploits constitute vulnerability information and exploit code. They differ from the other categories of attack tools in that they are not automated by nature. When exploits are incorporated into automated tools, they can then be classified as attack tools. The exploits available in the underground economy are typically tailored to specific market demands. Profitable activities in the underground economy (such as identity theft, credit card fraud, spam, and phishing) require a constant supply of resources (such as compromised personal information, credit card numbers, and hosts). Many of these goods and services are produced by attackers who exploit vulnerabilities in Web applications and servers. The market for exploit code and vulnerability information is geared toward attackers and malicious code developers who wish to incorporate fresh exploits into attack toolkits and, therefore, represent a distinct category of their own.

The highest ranked exploit during this reporting period was site -specific vulnerabilities in financial sites, which were advertised for an average price of $740, with prices ranging from $100 to $2,999. In some cases, it appears the same vulnerability was advertised at both the low and high ends of the price range. This may indicate that the value of the exploit decreased as it became overtraded, resulting in many attackers exploiting the same vulnerability in the same financial service. Attacks such as these are very noisy and difficult to conduct without detection, increasing the likelihood that the vulnerability will be noticed and patched by the maintainer of the affected website.

Spam and phishing tools and related goods and services marketed on underground economy servers were also observed by Symantec during this reporting period. Products include spam software, spam relays, compromised computers to host phishing scams, and content such as phishing scam pages and phishing scam letters. Spam is often used to advertise black-market products—such as pharmaceutical drugs, pump-and-dump stock scams, and pornography—and to distribute malicious code and launch phishing attacks that steal credentials, personal information, and credit card numbers.

The highest priced kit during this reporting period was for the hosting of phishing scams, which was offered for an average price of $10. Prices for this service ranged from $2 to $80. Scam hosting services are often advertised with guaranteed uptime, and virtual hosts may be included in the scam page service. Scammers may also acquire domain names by using stolen currency and credit cards to buy from domain name registrars. Additionally, some advertisers offer periodic rates for daily, weekly, and monthly hosting. Periodic hosting services range from less than $1 per day to $15 per day.

Diversity is the name of the game

The underground economy is geographically diverse and generates revenue for cybercrimi-

continues on Page 42

LOSING EMAIL IS NO LONGER INEVITABLE

It goes without saying that spam is a problem. Today's anti-spam filters struggle to distinguish good email from junk. But is the cure worse than the disease?

In response to the vast numbers of spam emails being received, anti-spam software vendors have endeavored to stop spam from entering inboxes through various means like anti-spam filters and firewalls. These current-generation email security solutions in use rely primarily on English-centric keyword and content filters to scan through incoming emails, and send suspected spam to the rarely checked junk email folders. Worse still, often the filtering technology completely removes the email and the intended recipient has no knowledge that the email was ever sent to them.

Email recipients in countries in the Asia Pacific region are particularly vulnerable to the keyword, character and IP filtering undertaken by the anti-spam filters. The majority of the solutions in operation have been designed for English language email markets and applied to Asian language markets without any significant thought as to the effect of the rules on the variety of character sets and language strings used in the region.

Although there is a variance in estimation and calculation of the global spam problem, industry analysts acknowledge the problem is a large and growing one. Ferris Research has predicted that the global cost of fighting spam in 2008 could be as high as $140 billion, and the total number of spam sent this year could reach 40 trillion messages. In 2006, the Radicati Group found there were 1.1 billion email users worldwide with over 171 billion messages sent. Radicati concluded that over 80% of all messages were spam.

What does this mean for businesses?

To put it simply, the volume of messages moving through the internet and the methods used by the anti-spam vendors to solve the spam epidemic have significantly increased the risk of legitimate emails being classified as spam. One of the most widely adopted approaches has been for the anti-spam filters to

become more aggressive in their filtering techniques in order to show customers that their inboxes are protected from this disease.

"False positives," or legitimate email incorrectly identified as spam, often go into a junk mail folder, or do not get through to intended recipients at all. The email filter's arbitrary judgment about what is a real email versus what is spam creates significant additional work for IT staff, network administrators and ISPs as disgruntled customers ask

continues on Page 43

From Page 41 — The Underground Economy

nals who range from loose collections of individuals to organized and sophisticated groups. During this reporting period, North America hosted the largest number of such servers, with 45 percent of the total; Europe/ Middle East/Africa hosted 38 percent; followed by Asia/Pacific with 12 percent and Latin America with 5 percent. The geographical locations of underground economy servers are constantly changing to evade detection.

Governments have become more sophisticated in their awareness of cybercrime, and specific legislation has been developed at various national and international levels to combat online fraud. As with crime anywhere, the online underground economy will continue to be a struggle between participants looking to profit from fraud and the various authorities and antifraud organizations trying to shut them down.

"As evidenced by the Report on the Underground Economy, today's cybercriminals are thriving of information they are gathering without permission from consumers and businesses," says Stephen Trilling, vice president, Symantec Security Technology and Response. "As these individuals and groups continue to devise new tools and techniques to defraud legitimate users around the globe, protection and mitigation against such attacks must become an international priority."◊

From Page 42 — Losing Email is No Longer Inevitable

them to find out why they did not receive an email sent by a known correspondent.

Privacy also becomes an issue for business, as anti-spam filters scan through emails containing commercially sensitive information. In industries such as the health industry, not only is the privacy issue a major concern, but the subject matter often overlaps with terms used by spammers to entice people to use adult web sites. This results in the industry unable to rely upon email communications.

Certainly by using more aggressive filtering techniques, the number of spam reaching inboxes decreases significantly, but the risk of losing legitimate email also rises. This leads to lost business, eroded customer service, lost customer confidence and miscommunication among business contacts.

How is this issue being addressed?

Is it possible to stop spam, and still receive all of your legitimate email? Absolutely.

False positive prevention (FPP) is the latest category in email security that specifically addresses the protection of legitimate email. Revolutionizing email security, FPP shifts the focus to protecting legitimate email first and then blocking spam, rather than just blocking fraudulent and malicious emails and losing legitimate email in the process. False positive prevention software – used alone or in conjunction with existing anti-spam technologies – ensures that legitimate emails are fast-tracked to the user's inbox, bypassing the risk of the anti-spam filter misclassifying the email. This not only guarantees that legitimate emails reach the user's inbox, it also means that content does not need to be scanned, which ensures complete privacy in the communication.

How does the technology work?

False positive prevention software uses technologies like authentication, reputation, Sender ID, and DKIM. By using safelists, as opposed to blocklists, the technology focuses on ensuring that authentic emails are protected from anti-spam filters. This methodology is further enhanced when companies register their adherence to best practice email-sending techniques with organizations that manage safelists, like Return Path, to ensure positive email reputation.

This new solution category can also incorporate aspects such as automated whitelisting of a company's correspondents and reference of a suspect email against various reputation data feeds available in the industry. By ensuring that innocent emails are saved from the scrutiny of anti-spam filters, false positive prevention guarantees that one-to-one emails are always delivered. It could be considered very similar to the APEC lane at the airport where "pre-authenticated" passengers are fast-tracked through immigration channels and not subject to additional checks imposed on the general passengers.

No room for errors

The only two people who can be absolutely certain that an email is authentic, are the sender and the receiver. By trusting anti-spam filters to make guesses on which emails are spam and which are authentic, companies are allowing for errors.

Once a company has positive email reputation, the anti-spam software which it faces at the recipient's end becomes less relevant. When email comes from a trusted sender, it gets fast-tracked and sent straight to the intended recipient's inbox. There is no content-filtering or re-routing involved.

Losing legitimate email is no longer acceptable. Losing legitimate email is no longer inevitable. The latest evolution in philosophy and approach to email protection solves the problems created by anti-spam filters.

With the widespread use of email today, companies and Internet Service Providers have a responsibility to ensure that email communication is safeguarded. False positive prevention software has the power to guarantee, without doubt, that an email you send will be received - no questions asked.◊

By Manish Goel, CEO, BoxSentry

LOCALIZED MALWARE GAINS GROUND

Cybercriminals are increasingly crafting attacks in multiple languages and are exploiting popular local applications to maximize their profits, according to a new McAfee, Inc. report.

"This isn't malware for the masses anymore," observes Jeff Green, senior vice president, McAfee Avert Labs. "Cybercrooks have become extremely deft at learning the nuances of the local regions and creating malware specific to each country. They're not skilled just at computer programming — they're skilled at psychology and linguistics, too."

McAfee Avert Labs examined global malware trends in its third annual Global Threat Report, titled "One Internet, Many Worlds." The report is based on data compiled by McAfee's international security experts and examines the globalization of threats and the unique threats in different countries and regions. In the report, McAfee details the following trends and conclusions:

- Sophisticated malware authors have increased country-, language-, company-, and software-specific attacks
- Cyber-attackers are increasingly attuned to cultural differences and tailor social engineering attacks accordingly
- Cybercrime rings recruit malware writers in countries with high unemployment and high levels of education such as Russia and China
- Cybercriminals take advantage of countries where law enforcement is lax
- Around the world, malware authors are exploiting the viral nature of Web 2.0 and peer-to-peer networks
- More exploits than ever before are targeted at locally popular software and applications

"Malware has become more regional in nature during the past couple of years," notes Green. "This trend is further evidence that today's cyber-attacks are targeted and driven by a financial motive, instead of the glory and notoriety of yesteryear's cybergraffiti and fast-spreading worms. We're in a constant chess match with malware authors, and we're prepared to counter them in any language they're learning to speak."

Geographical trends:

The United States: The Great Malware Melting Pot

Once the launching pad of all malware, today, malware in the US includes elements of malicious software seen around the world. Attackers use increasingly clever social engineering skills to trick victims and are looking to exploit the viral nature of Web 2.0. Although the United States has cybercrime laws in place, the lack of international cybercrime laws and the differences in extradition treaties make it difficult for enforcement agents to prosecute criminals across borders.

Europe: Malware Learns the Language

With 23 languages in the European Union alone, language barriers used to be a hurdle for miscreants. Consumers in non-English speaking countries often simply deleted English-language spam and phishing e-mail. Today, malware authors adapt the language to the Internet domain site where the scam message is being sent, and malicious Web sites serve up malware in a language determined by the country the target is located in. Cultural events such as the FIFA soccer World Cup in the summer of 2006 prompted email scams and phishing sites luring in soccer lovers. With the increased sophistication of malware, computer users in the EU are under attack.

China: Virtual Entertainment

With more than 137 million computer users — a quarter of whom play online games — malware authors are cashing in on virtual goods, currency, and online games. A majority of the malware found in China is password-stealing Trojans — designed to steal users' identities in online games and their credentials for virtual currency accounts. China has also become a breeding ground for malware writers, as a large number of skilled coders do not have legitimate work. The conditions have driven these hackers to cybercrime in search of money.

continues on Page 45

From Page 44 — Localized Malware gains ground

Japan: Losing to Winny — Malware Spreads from Peer to Peer

Winny, a popular peer-to-peer application in Japan, is prone to malware infestations that can cause serious data leaks. When deployed in the corporate setting, malware on Winny can expose data, steal passwords, and delete files. Unlike in most countries, malware authors in Japan are not motivated by money — instead authors seek to expose or delete sensitive data on machines. Another common target in Japan is Ichitaro, a popular word processor. There have been several attacks against Ichitaro users that exploited unpatched security vulnerabilities to install spyware on the target machines.

Russia: Economics, Not Mafia, Fuel Malware

The technical skills of Russians in a stumbling economy make for an active market of hackers. Some of the most notorious attack toolkits are produced in Russia and sold in underground markets. These gray-market malware tools, combined with lack of legislation against cybercrime, lead experts to believe that the Russian mafia will soon — if they haven't already —latch onto computer crime. Although the Russian economic situation, like that of China's, has driven many hackers to a life of cybercrime, Avert Labs predicts that with a strengthening economy and stronger law enforcement, Russian-made malware will gradually decrease.

Brazil: Bilking the Bank

Miscreants have made an international showcase out of Brazil when it comes to bilking online bank accounts. With a majority of Brazilians banking online, cybercrooks use sophisticated social engineering scams to trick Brazilians into giving up personal information. In 2005 alone, the Brazilian Banks Association estimated losses at R$300 million (about $165 million USD) due to virtual fraud. Malware creators rapidly adapt password-stealing Trojans to the changes banks make to their Web sites.◊

Global View of Threats — By the Numbers:

- 371,002 — Total threats identified by McAfee Avert Labs as of Feb. 1, 2008
- 131,800 — Threats identified by Avert Labs solely in 2007
- 53,567 — Unique pieces of malware in 2006
- 246 percent — Growth of malware from 2006 to 2007
- 527 — New malware identified daily by Avert Labs at the start of 2008
- 750 — Expected number of new malware identified daily by Avert Labs at the end of 2008

CYBER-CRIME SHOWS NO SIGNS OF ABATING

Secure Computing Corporation's Q2 Internet Threat Report has revealed that enterprises and home users are increasingly being attacked through malicious Web content and blended security attacks.

The company's research states that even though the overall spam volume is up 280 percent from Q2 2007 to Q2 2008, spam volumes have decreased by 40 percent this quarter. In addition, Q2 of 2007 witnessed over 300,000 new zombies per day, and during the second quarter of 2008 Secure saw half that amount. Even though both spam and new zombies are down this year, Secure Computing researchers point to other areas that are increasingly problematic, including:

✦ Over 16 percent of all spam originates from the U.S., more than twice the amount of the No. 2 country, Russia. In Asia, the top spam originators are China, India and South Korea.

✦ Male enhancement, product replica and prescription drug spam hold the top three places of types of spam, proving that you can't beat the oldies but goodies.

✦ Swizzor, a rapidly growing ad/spyware family, now makes up more than 30 percent of all new malware in Q2 of 2008.

✦ The ZBot spyware family is another such ad/spyware family that has grown significantly this quarter. ZBot steals users' sensitive data while establishing a backdoor on infected computers to give the attackers full control over compromised systems.

50 percent of all websites are now published in languages other than English.

continues on Page 46

From Page 45 —Cyber-crime shows no signs of abating

"We are witnessing change every single day in how the cyber-criminals are developing new vectors of attack through spam, malicious Web content, spyware and botnet deployments," says Dmitri Alperovitch, director of intelligence analysis at Secure Computing. "Through our advanced TrustedSource global reputation system and our research team's ability to analyze and classify terabytes of email, Web and network traffic in real-time, we are in an excellent position to identify new trends and protect our customers from new insidious threats."

Summary of Key Threats in Q2 2008:

✦ The threats challenging the enterprise today are becoming a blended variety that challenge both Email and Web security. Without integrated and correlated protection between the two, the ability to stay ahead of these threats will become increasingly difficult.

✦ Threats are becoming more and more sophisticated as recipients of threats are better educated on what to look for. Users are more cautious and this has lead to a rise in more cunning ways to harvest personal information without users' apparent involvement.

✦ Spammers are continuing to use pop culture and current events (elections, Olympics) to entice end users into responding or clicking on links whose sole purpose is to download malware. The excitement over seeing a video of breaking news of an earthquake in China or the new sensational photos of your favorite celebrity can occasionally encourage even the most cautious users to open what could be suspicious mail.

Threats are and will continue to be driven by financial motivations. No matter what the threat is, or how it is delivered, the perpetrator is almost always looking for financial gain.

Forecast and Predictions

Brace Yourself: Spam Flood likely Heading Your Way Once Again

According to Secure Computing, one prediction that's relatively easy to make given the nearly half a decade of historical observations of this trend is the fact that every single year, spam volumes increase dramatically in the second half of the year and peak by December/January before declining in the first months of the new year. There are many theories floating around concerning this trend but whatever it is, come late August/early September, expect your mail volumes to start their annual dramatically (sometimes by as much as 50-60%).

Secure Your Wireless Router

The bad guys have discovered networking equipment as an additional vector to gain control over computing resources. Since most users never touch their wireless router once it's set up (and many times not even change the standard password), utilizing the wireless router for attacks is very tempting to adversaries.

Secure Computing warns to expect more attacks of internal network infrastructure during the coming year. Once such a device is exploited, malware can do its job more or less clandestinely. While this is mostly a threat for home networks, enterprises should also make sure that there infrastructure is secure. Vulnerabilities in network printers are not unheard of too. When was the last time you checked your printers for malware?

iPhone

The iPhone has been making its presence felt in Asia too over the last few months. It has set itself apart as a new kind of personalized device, fusing personal information, location awareness, and mobile networking capabilities. With this sum total of personal intelligence carried by the device, Secure Computing expects that malicious parties will begin to develop malware for the purpose of harvesting these devices for data, which can be made available through a black-market botnet, and additionally attempt to turn these devices into zombies capable of saturating not only networking targets, but telephone-based targets. Furthermore, the iPhone's combination of camera, audio, location awareness, and personal data in a full features operating environment makes it a good target for a type of spyware used as voyeurism, cyber-stalking, or other very directed forms of phishing.

Other Developments to Watch

- Topical spam was on the rise this year and Secure Computing expects a surge of topical spam and malware attacks
- More and more legitimate site being compromised through iframe injections, cross-site scripting attacks and ad-network compromises.
- Integration of social networking components into a wide variety of sites is going to continue to grow

Secure Computing researchers recommend that both enterprises and consumers assure their software and patches are up-to-date, and that they implement a multi-layered approach to preemptively detect and block attacks.◊

By Shanti Anne Morais

ASIAN ANTI-SPAM ACTS

Spam is viewed as a growing problem and threat everywhere, and Asia has not been spared. The questions, does anti-spam legislation help has been thrashed by many, and was one of the questions posed at MediaBUZZ's Anti-Spam panel discussion on October 23, 2008.

All the panelists there agreed that while anti-spam legislation is a step in the right direction it in no way will stem the tide of spam. The major reason for this is the fact that most spam originate from outside (how much of the spam in your Inbox actually originates from a Singapore source?).

In this article, we take a brief glance at some of the Anti-Spam laws in the region.

Singapore's Anti-Spam Act of 2007

This law which came into effect on the 15th of June 2008, was by no means an easy issue for the Singapore government. Its goal is not the prohibition of spam but the control of spam. It applies only to electronic messages and does not cover mail, voice mail, fax and telemarketing. It also only applies to commercial emails unless part of a dictionary attack or address harvesting software scheme. There is a government exception relating to public emergencies, messages that touch public interest and security and national defense. The Act applies to unsolicited commercial mail that are sent in bulk via electronic mail, text messaging (SMS) to mobile phones, multi-media messaging to mobile phones – and only those with a Singapore link. By this, it means that the message originates in Singapore; the sender is in Singapore and the device used to access the message is in Singapore; the recipient is in Singapore when the message is received.

Bulk unsolicited email may still be sent out though, but it must include an unsubscribe facility that must be in English (additional languages are o.k.). The unsubscribe facility must be clear and conspicuous, cannot cost more than normal, must be valid and capable and able to receive the requests, maintained for 30 days from date message was sent. Companies are given 10 business days to comply and cannot disclose details to other parties without consent.

In addition, labeling must be provided. Here the subject/ header of the message cannot be misleading, <ADV> must be included at the beginning of the subject for email and the message for SMS/MMS. The email address that is sending out has to be accurate and functional.

Who's liable for non-compliance to the Act?

- The sender or person who causes or authorizes the sending
- Any person who knowingly allows his product/services to be advertised or promoted unless that person has taken reasonable steps to stop the sending of such messages
- The Consequences?
- Civil liability – anyone can take action so long as loss or damage can be proven
- Any person who contravenes or aids/abets/procures a contravention may be sued

Statutory damages are capped at S$25 per electronic message and cannot exceed S$1 million unless actual loss is greater.

While the Singapore government can definitely be applauded to finally introducing this long-awaited bill, it has to be noted that the Act itself has been criticized often for its lack of ambiguity in certain areas such as if it applies to text messages sent to fixed lines and instant messaging. Some also criticize it for its support of businesses and marketers in general. It's important to note that unless the spam itself is unscrupulous in nature and origin, what one person views of as spam, may be a message of importance to another.

Japan's Anti-Spam Law

of the forerunners of anti-spam legislation in Asia is Japan. The country passed its Anti-Spam law in 2002 . However, the country's spam problem has evolved since its legislation came into play and this has resulted in amendments made to it in June 2008, the most substantial being that the country has switched from an opt-out regime to one that is completely opt-in.

As late as 2004, the vast majority of spam in Japan was sent to mobile phones rather than PCs. This no longer holds true: Japan has been largely successful in its efforts to reduce mobile spam; however, spam sent to PCs has exploded and now constitutes the vast majority of spam in the country. In 2006, close to 90% of spam in Japan was sent to PCs (it was less than 30% in 2004). Of the spam sent to PCs, more than 90% was advertisements for match-making (dating) sites, 2% was for adult sites and the remaining messages were for all other content.

The History of Japan's Anti-Spam Legislation

A large increase in spam sent to mobile phones gave rise to industry self-regulation in 2001 by

continues on Page 48

From Page 47 — Asian Anti-Spam Acts

mobile operators and, in 2002, two national laws were enacted to combat spam – the Law Concerning the Proper Transmission of Specified Electronic Mail (the "Anti-Spam Law") and the Law for the Partial Amendment to the Law Concerning Specified Commercial Transactions (the "Revised Transactions Law"). The Japanese government first amended the Anti-Spam Law in 2005 (the "2005 Anti-Spam Law"). Most recently, on June 6, 2008, the government amended the Anti-Spam Law a second time (the "New Anti-Spam Law") in hopes of curtailing its continuing spam problem. The New Anti-Spam Law will go into effect once the government issues an implementing order with regulations supplementing the law, which it must do by December 6, 2008. The Ministry of Internal Affairs and Communication ("MIC"), which is in charge of regulating the telecommunications and broadcasting industry, enforces the New Anti-Spam Law.

The New Anti-Spam Law applies to all commercial email sent to or from Japan by for-profit groups or individuals engaged in business. Therefore, the law is now applicable to any Sender who sends commercial email to recipients in Japan, regardless of where the Sender (s) are located.

Several substantial amendments to the 2005 Anti-Spam Law were made in June 2008:

- Previously, the law provided for substantial categories of commercial email that were exempt from its rules. These exemptions no longer exist.
- Before the amendments, the law established an "opt-out" regime, much like the U.S.'s CAN-SPAM Act. Japan has decided that this framework is insufficient to curtail unwanted spam and has switched to an "opt-in" regime where recipients must affirmatively agree to receive commercial email before Senders can send it.
- Fines for violating the law or relevant regulations have been substantially increased.

Permitted Recipients of Commercial Email (Opt-In)

Under the New Anti-Spam Law, a Sender may only distribute commercial email if the recipient falls into one of the following categories:

- Individuals who have notified the Sender in advance that they request or agree to receive commercial email;
- Individuals who have provided the Sender with their own email addresses;
- Individuals who have a pre-existing business relationship with the Sender; and
- Individuals (limited to those engaged in for-profit activities) or groups that publicly announce their own email addresses.

Because all of these categories require affirmative acts by the recipient before a Sender is permitted to transmit commercial email, Japan has essentially adopted a modified opt-in system for commercial email regulation.

The New Anti-Spam Law does not describe how individuals must notify Senders of their email addresses for the opt-in to be valid. Nor does it indicate what constitutes a "business relationship" or how an individual or group "publicly announces their own email address" for opt-in purposes. These are expected to be clarified in the government's implementing order (expected to be out in December 2008).

Additional Requirements

In addition to requiring opt-in consent; there are four further requirements under the New Anti-Spam Law that Senders must fulfill:

- Senders must keep records which prove that the recipients requested the emails;
- Senders must honor opt-out requests received from individuals;
- Senders must include certain information in the commercial email sent; and
- Senders are prohibited from sending email using programs that generate email addresses and from falsifying information about themselves.

Record-Keeping Requirements

Senders who send commercial email must keep records that prove that the recipients agreed to receive commercial emails in advance. The implementing order will specify exactly what information the Sender must preserve to fulfill this requirement.

Honoring Opt-Outs

Senders are prohibited from sending commercial email to recipients from whom Senders have received subsequent opt-out requests. There is no "grace period" for complying with such a request.

Labeling Requirements

Commercial email must contain the Sender's name and title, as well as an email address that recipients can use to send opt-out notifications. These items must be clearly indicated so they are visible on the recipient's screen. Although these requirements are less strict than those imposed by the 2005 Anti-Spam Law, the Japanese government may impose additional labeling requirements when it issues the implementing order.

continues on Page 49

From Page 48 — Asian Anti-Spam Acts

Computer Generated Email Addresses and False Sender Information

Senders may not send email to email addresses that have been generated using a program that automatically combines symbols, letters and numbers to create email addresses. They may not send blank emails, which attempt to obtain active addresses, or disguised emails, such as those apparently from friends of the recipient. Senders must also not disguise or falsify the email address used to send commercial email or the symbols, letters or numbers that identify the electronic communication device or facility used to send the email.

Penalties for Violation

If a Sender violates its obligations under the New Anti-Spam Law, the Minister of MIC can order the Sender to take measures to bring itself into compliance. The Sender may also be subject to a fine of up to ¥1,000,000 or imprisonment for up to a year if it violates such an order.

The Minister of MIC may also require Senders to submit reports regarding the Sender's transmission of commercial email, and may inspect the Sender's premises, books and other documents. A Sender may be subject to a penalty of up to ¥1,000,000 if they refuse to submit such reports or to cooperate with an inspection.

In addition, under the New Anti-Spam Law, Senders may face additional penalties if their agents violate the provisions of the law. A Sender whose agent violates an administrative order from MIC to comply with the law is subject to a fine of up to ¥30,000,000. If a Sender's agent refuses to cooperate with a MIC investigation, the Sender is subject to a fine of up to ¥1,000,000.

Lastly, the New Anti-Spam Law authorizes MIC to share information with foreign governments.] Accordingly, non-Japanese Senders may face scrutiny from their home regulators in regard to commercial email they send to Japan.

Vietnam's Decree on Spam

A survey by the Vietnam Computer Emergency Respond Team (VNCERT) under the Ministry of Information and Communications (MoIC), the agency compiling the decree on spam email, revealed that around 30% of the survey participants said that 80% of the emails they receive are spam emails. Half of them said that over 30% of the spam emails are in Vietnamese. More than 78% said they hate spam and 63% want to have regulations to control spam emails. Bearing this in mind, it's no surprise then that Vietnam is the latest Asian country to introduce anti-spam legislation.

The country's Anti-Spam Decree bans organizations and individuals from using electronic means to deliver spam mails, exchange or trade e-mail addresses or deliver software products that collect e-mail addresses, etc. Senders of spam e-mails and text messages which aim to cheat, disturb people, diffuse viruses, or advertise will be fined.

Fines of from VND200,000 to VND500,000 will be imposed on those who collect e-mail addresses for advertising without the consent of the email owners.

Fines of between VND5-10 million will be imposed on those who allow others to use their electronic means to deliver spam emails.

Fines of VND20-40 million will be given to those who trade in and diffuse software products that collect e-mail addresses.

Organizations that provide advertising services through email and text messages which don't have the receivers' consent will be fined up to VND80 million.

Hong Kong's Unsolicited Electronic Messages Ordinance (the UEMO)

The Unsolicited Electronic Messages Ordinance (the UEMO) was enacted in May 2007 and came into full effect in December 2007, with the aim of regulating the sending of all forms of commercial electronic messages (CEMs) with Hong Kong links. It establishes the rules for sending CEMs such as providing accurate sender information and unsubscribe facilities as well as the launch of the do-not-call registers, and prohibits professional spamming activities such as the use of unscrupulous means to gather/generate recipient lists for sending CEMs without the consent of recipients, and fraudulent activities related to the sending of multiple CEMs.

According to the Ordinance, all senders of commercial electronic messages (including emails, short messages, faxes, pre-recorded telephone messages) are now required to provide clear and accurate sender information in the message, including name, contact telephone number and address. If the message is an email, the sender is also required to provide the contact email address. It is also not permitted to send email messages with misleading subject headings. Senders are required to provide an "unsubscribe facility" for their recipients to submit "unsubscribe requests", and honor such requests within 10 working days after the requests have been sent. Unless consent has been given by the registered user of the relevant telephone or fax number, commercial electronic messages should not be sent to numbers registered in the Do-not-call Registers.

continues on Page 50

From Page 49 — Asian Anti-Spam Acts

China's regulations on Internet Email Services

On 20 February 2006 the Chinese Ministry of Information Industry (MII) of P. R. China adopted the "Regulations on Internet E-Mail Services". The regulations took full effect on 30 March 2006 and aims to regulate Internet email services and to protect end-users.

According to the regulations, one should not send commercial emails without prior consent from the recipients, which means the "opt-in" principle is adopted. Even if one has prior consent from recipients, the law states that the sender has to add the label "AD", which is the abbreviation for "Advertisement", in front of the subject line of a commercial email. The sender of commercial email should also provide valid contact information for the recipients to unsubscribe. It's prohibited to get others' email addresses by harvesting, selling or sharing harvested addresses.

Consequences: The MII can send a simple warning to the sender, or apply a fine. In addition, online fraudulent activities and misuse of computer resources, such as spreading viruses, are considered criminal violations according to other Chinese laws, and can be punished with more severe penalties, such as detention.

Compared to other national anti-spam laws, the Chinese regulation does not only regulate the sending of email messages, but also the provision of email services. For example, email service providers are asked to strengthen the protection of their email servers to avoid their fraudulent utilization by spammers. Also, to make it easier to find the evidence of spamming, ESPs are asked to log the email related behavior of their users. In addition, ESPs are also asked to accept users' complaint reporting. Users who receive spam are also encouraged to report to the Spam Reporting Center run by Internet Society of China accredited by MII.

Malaysia Communications and Multimedia Act of 1998

There are no specific provisions on the illegality of Spam. However, the Communications and Multimedia Act of 1998 states that a person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence.

According to the Malaysian Communications and Multimedia Commission (MCMC), Malaysia has no immediate plans to legislate. It will pursue this recourse when there is no other viable alternative. MCMC is of the opinion that for legislation to be effective, anti-Spam laws in all countries must be of similar nature and standard so as to prevent spammers from forum shopping. It also feels that legislative action would consequently be dependant on continuous cooperation between countries and legal systems to ensure that Spam received in one country will result in legal action being taken in another. Thus, the MCMC will continue to follow closely the development of countries that have enacted anti -Spam legislations.

The MCMC's approach to tacking spam includes self-regulation by users through education and awareness initiatives and management by service providers. It has a four-tiered strategy in place to address spam:

Tier 1 :

Self-management by users

Tier 2 :

Forward complaint to Service providers

Tier 3 :

If complaints remain unresolved, next recourse is to complaint to Consumer Forum of Malaysia

Tier 4 : Still unresolved, matter escalated to the Malaysian Communications and Multimedia Commission

Anti-Spam Law in Korea

The Information Network and Privacy Protection Act ("INPPA") of Korea sets out the minimum procedural requirements for lawful online transmissions. In Korea transmissions of advertised materials against recipients' refusal to accept are strictly prohibited. Although these rules are applicable to unsolicited commercial e-mails via the internet, they were intended to apply to all modes of telecommunication such as cellular phones, facsimiles, etc.

The Korean government has made continuing efforts since 1999 to curb the increase in spam mail and has since been monitoring the effectiveness of the implementation of additional provisions. The new law targets senders of spam mail that are commercial in nature. Consistent with its effort to protect minors from being exposed to obscene and violent materials online, the Korean government has also included a provision in the INPPA that requires senders to label those materials as such.

The sender must disclose his name, contact information (e.g. e-mail/ mailing address, telephone number), the purpose/ content of the transmitted materials (i.e. "advertising materials") as well as an opt-out procedure both in Korean and English.

continues on Page 51

From Page 50 — Asian Anti-Spam Acts

New Zealand Unsolicited Electronic Messages Act

New Zealand's Unsolicited Electronic Messages Act came into force on 5 September 2007. The legislation prohibits unsolicited commercial electronic messages with a New Zealand link from being sent. It also requires marketers to obtain the consent of the receiver of any commercial electronic message before the message is sent. The term "commercial electronic message" includes electronic messages (email, SMS text, instant messages, but not voice calls or facsimile) that market goods, services, land or business opportunities.

The Act affects not only those who send the commercial electronic messages but also those who are directly or indirectly knowingly concerned in the sending of them. However, telecommunication service providers are not caught by the new legislation merely by the fact of their providing telecommunication services that enable the electronic messages to be sent. Also, even although a message does not contain marketing material, it may still be caught by the new legislation if it provides a link or directs a recipient to a message that does contain marketing material.

Key points for compliance:

- a commercial electronic message must not be sent unless the receiver has first consented to receiving the message;
- all commercial electronic messages must (unless agreed otherwise) include a "functional unsubscribe facility" which allows the recipient (at no cost) to inform the sender that such messages should not be sent to them in the future;
- all commercial electronic messages must include information which clearly identifies the person who authorizes sending the message and how that person can be contacted;
- "Address–harvesting software" must not be used in connection with, or with the intention of, sending unsolicited commercial electronic messages. "Address-harvesting software" is software that searches the Internet for electronic addresses and collects and compiles those addresses. Restrictions also apply to the use of lists produced (directly or indirectly) by use of this software.

Obtaining consent

The consent requirement applies to all commercial electronic messages sent, whether to new contacts or existing contacts. This means that senders of commercial electronic messages will need to have consents from persons on their existing electronic marketing lists.

A positive consent (or an "opt-in") to receive future emails is required. Including an unsubscribe message – "tick the box if you don't want to receive these types of emails" – will not of itself suffice for consent. The consent requirement applies to the sending of one-off emails as well as bulk mail-outs. The consent of recipients can be either express, inferred or deemed.

Express consent is a direct indication from the recipient that they consent to the sending of the message. This consent can be given by the person responsible for the electronic address or any other person who uses it. Inferred consent arises from the conduct and the business and other relationships of the sender and the recipient. Such relationships giving rise to consent are likely to exist, for example, between a service provider and subscribers to the service. Recently the Federal Court of Australia has observed that it can be reasonably inferred (in the absence of evidence to the contrary) that a purchaser by email order would wish to be kept aware of the business of the vendor. In the case in question the purchaser's consent to receiving future emails could reasonably be inferred. However, the Court also recognizes that whether consent can be inferred from the relationship of the sender and the recipient will always be a question of fact and the particular circumstances. The deemed consent provision only applies where:

- the recipient's electronic address has been published;
- the publication is not accompanied by a "no spam" type statement; and
- the message being sent to the recipient is relevant to the recipient in a business or official capacity.

On the flipside, if you use an email addresses on a business website, you should include a "no spam" statement if you do not wish to be "deemed" to have consented

Australia's Spam Act of 2003

Under Australia's Spam Act 2003, it is illegal to send, or cause to be sent, unsolicited commercial electronic messages. The Act covers email, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing.

The Australian Communications and Media Authority (ACMA) is responsible for enforcing the Spam Act and actively works to fight spam in Australia.

For more on Australia's Spam Act 2003, read our article 'Anti-Spam Legislation and Enforcement Down-Under'◊

By Shanti Anne Morais

SOCIAL NETWORKS: THE NEW FRONTIER FOR SPAM

Social Networks have become the new playground of spammers.

While earlier this month, the US federal court awarded MySpace nearly US$230 million in its suit against Sanford Wallace and his partner Walter Rines -- aka the "Spam King" and scoring a win for those fighting the anti-spam war, the battle is far from over.

Yes, the judgment, especially given the size of the award, represents a decided victory for e-commerce sites in their costly battle against spam. Yes, it is so far, the largest award since the enactment of the CAN-SPAM Act in 2003. In case you are wondering, MySpace received $223,770,500 in damages under CAN-SPAM, $1.5 million in antiphishing damages allowed by California statute and $4.5 million for legal fees.

Yes, the pair were found responsible for orchestrating a phishing scam designed to harvest MySpace login credentials, prior to bombarding members with messages punting gambling and smut websites. As many as 730,000 bogus messages, rigged to appear as though they came from their friends, were sent to MySpace members.

However, there is unfortunately a bleaker side to the picture. Namely, the amount of the award provides a telling look into the costs companies incur when they fight spam, In addition, it's doubtful MySpace will ever see any of the money.

This gloomy expectation fuels doubts that the award -- or the law underpinning it -- will serve as any deterrent whatsoever against the volume of spam flowing into in-boxes. While the CAN-SPAM Act of 2003 has a very large share of detractors, it and the penalties it establishes are better than nothing. This latest prosecution for example at the very least sends a clear message to fraudsters and spammers. In addition, the fact that such amounts are potentially recoverable under the anti-spam legislation provides additional incentive for firms such as MySpace to prosecute offenders, thereby heightening their risk levels.

Social Networking Vulnerabilities

The case also highlights the lax security on social networking sites, Matt Shanahan, senior vice president at AdmitOne Security. Elaborating on this, he notes, “It is very easy to hijack an account," he said, and when that happens -- especially on a massive scale -- the network's brand suffers.”

In fact, MySpace did receive a lot of negative press in connection with these incidents -- particularly over the delivery of spam containing links to porn Web sites to minors' in-boxes.

Web 2.0 sites like MySpace have to adopt the same mentality that banks and financial institutions did several years ago concerning Internet security, Shanahan continued. "All the banks have worked very hard to become trusted names online, establishing cutting-edge security controls."

Spam and Social Networks: The Cycle Continues

So if you have been under the impression that social networks are safe havens from spammers, think again. Junk messages are following users and advertising dollars to social networking sites, according to an anti-spam researcher, who found that spam levels have tripled in recent months.

Recently, Cloudmark, a company which specializes in anti-spam platforms for service providers says it tracked a 300 percent rise in junk messages at a major social network site it works with. In fact, according to the company, in the six months leading up to March 2008, social networking sites saw a four-fold growth in the amount of spam on their network. In addition, at several major social networking sites, 30 per cent of new accounts created are automated fraudulent 'zombie' accounts, designed to be used for the purpose of sending advertising messages, spam and other malicious attacks.

The Modus Operandi

It does not help that social networks tend to have large populations of non-tech savvy users.

And yes, once again, just in case you are wondering, the type of spam advertised through social networks is the same type as that advertised by email spam and punted by much the same people. "There's an implicit trust in social networking. People don't think they're going to be attacked with spam. People don't trust email anymore. Spammers are following peoples' online habits. What’s more the size and viral nature of so-

continues on Page 53

From Page 52 — Social Networks: The New Frontiers for Spam

cial networks make Web 2.0 an attractive new target for spammers," states Cloudmark chief executive Hugh McCartney.

It is important to note that social network spam is not limited to friend invitations, but also includes social network tools such as pokes, chats, comments, bulletin board messages, blogs and application communications.

Social networking spam can be messages between users or posts to walls or other similar applications. Social network spammers most often hijack accounts using fake log-in pages. Phishing-like tactics, password guessing and the use of Trojans to capture keystrokes are also in play.

Junk messages, rigged to appear as though they came from their friends, are more likely to be acted on by recipients on social networking sites compared to the same messages received by email. Social network spammers try to recruit friends by posting profile pictures that depict them as attractive young women. By recruiting people into their groups or networks it's easier for spammers to subsequently send them spam.

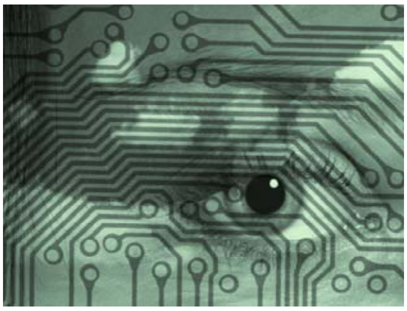
Furthermore, spammers are starting to use data-mining techniques to create spam lists, sorted on geographic and demographic criteria. Such lists are of premium value to spammers.

And of course, what's even more frightening is that despite anti-spam legislation, the problem is not expected to disappear but in fact is predicted to get worse. After all, anti-spam legislation while acting maybe as a deterrent can only do so much. At the end of the day, though, users must share some of the responsibility for protecting themselves. Once again, it seems that user education is one of the key strategies that has to be employed in the never -abating war against spam.

So once again Web 2.0 and Social Network users, the moral of the story is “Always be careful of what you click on." ◊

By Shanti Anne Morais

JUPITERRESEARCH: MARKETERS ON GUARD - EMAIL MARKETING FACING TOUGH TIMES



Email has been hailed as the ubiquitous form of communication, something which executives cannot live without. However, according to JupiterResearch, email is not without competition and is currently undergoing a downturn of its own.

The medium is facing an onslaught from new media like social networks and even from text message and mobile phone communication. In addition, email, says the research firm, is steadily coming under pressure from disenchantment with email proliferation and irrelevance of the medium.

Indeed, a recent report from JupiterResearch shows that permission-based email marketing is starting to lose its shine. According to the study, in 2008, 44% of email users purchased online as a result of promotional emails, while 41% made an offline purchase. While this might seem like a high number, the fact is that both these numbers reflect a decline from 2007, when 51% made an online purchase while 47 percent went offline.

In addition, after years of seeing stable volumes of consumer-reported email for their primary, personal email accounts, this year's survey revealed a decline. According to JupiterResearch, email users now report receiving a daily average of 24 email messages of all types (including friends/family, opt-in, work/school, spam and other) in these primary accounts--down from 41 per day in 2006.

This is a pretty huge drop. JupiterResearch attributes the fall in overall email volume partially to a decrease in spam messages. However, analysts say the declines also point to shifting communication channel usage patterns, particularly among young consumers. For example, younger consumers (those between the age of 18-24) tend to rely mainly on text messages while via social networks, they receive on 12 emails per day. However, email is still the way to go for the older generation: 45-54 year-olds tend to get an average of 28 emails per day. However, this is nothing to shout about as the older age group demographic is also seeing a dramatic decline – in fact, those aged 55 or older who reported receiving 31 or more emails per day has declined from 42% in 2006 to 24% now.

David Schatsky, president of JupiterResearch has this advice for marketers: “Consumers are using other forms of communication and marketers must therefore ensure their strategies adapt to consumers' changing behavior.”

He also cautions marketers to address the other worrying trends in the email marketplace especially the lack of relevance of emails which continues to be the top reason for unsubscribing. In fact, the firm’s research shows that 50% of total email users report that they unsubscribe when the offers/types of content do not interest them. In particular, marketers have to pay attention to the fact that the percentage who unsubscribe from irrelevant messages is even higher among those who have made four or more online purchases during the past 12 months: 60%.

The second-highest driver of unsubscribes is frequency. If you send your emails out too frequently, beware: 37% percent of all users say they unsubscribe when they receive emails from a sender "too often." It’s also no surprise then that 33% report that they unsubscribe from offers because they get "too much" email. Furthermore, 39% say they believe that signing up for permission-based email leads to getting more spam email while 30% state they don't trust that the unsubscribe link in email offers work. Scarily, 26% reveal that they use the spam button to unsubscribe.

Explaining these above trends in greater detail, David Daniels, VP, research director, JupiterResearch and lead analyst of the company’s report entitled "The Social and Portable Inbox: Optimizing E-mail Marketing in the New Era of Communication Tools" shares, "Consumers' confidence in email have become shaken by irrelevant communications and high message frequency, which are top drivers of subscribers' churn and channel scepticism. Their behavior and attitudes are driven by the unfettered volume of spray-and-pray untargeted email offers, blurring the distinction between spam and permission-based email.”

He warns that it has never been more important than now for marketers to ensure they are sending relevant email responsibly.◊

THE IMPORTANCE OF REPUTATION AND MESSAGE RELEVANCE

A recent report from Jupiter Research highlights the fact that deliverability is the number-one consideration for marketers when selecting an email service provider (ESP).

Unfortunately, there is only so much even the best ESPs in the market can do in order you in getting your marketing messages to the inbox. So what are ESPs good for you may ask? They provide the infrastructure that high-volume senders need to get through to the inbox. ESPs should also keep up with the latest in authentication methodologies and provide workflow that enforces current best-practices so senders can rest assured that every message sent is compliant with the best-practices and laws of the email marketing industry. These are all essential pieces of the email deliverability puzzle, but email senders and marketers also have a key part to play here, they have to closely keep in mind two other factors: reputation and message relevance.

Reputation – The Holy Grail of Email Marketing?

One of the most common mistakes email marketers tend to make relates to the misperception of using a brand new IP address. Many marketers think that this gives them a chance to start their broadcast/campaign on a clean slate, however, in reality; it actually can have a negative impact on the sender's reputation. Why? Simply because spammers tend to frequently change their IP address often in order to hide or evade the filters. Thus, ISPs very often tend to be highly skeptical of new IP addresses. However, you can build a strong reputation fairly rapidly by sending consistently good email using the same IP address over time.

Good list hygiene also does wonders for a sender's reputation. You should never second-guess your email lists or addresses. Also do not assume your recipients' preferences; i.e. if you're not completely confident that an address rightfully belongs on your list, for any reason, you should remove it. After all, it is better to be safe than sorry. In addition, poor list hygiene can have dire consequences and lead to undeliverable email and/or complaints – both of which are red flags for ISPs.

Recipients can and often will complain to their ISPs in a variety of ways. For example, the "spam" button within the user interface is a popular choice. Customers everywhere are overwhelmed everyday by marketing messages on a daily basis, and reporting email as spam is an easy, efficient way for them to clear away the clutter. In fact, many will use the "spam" button as a one-step method of unsubscribing from messages they explicitly requested. In fact, the Email Sender and Provider Coalition (ESPC) reported last year that 80 percent of respondents in their study of consumer email behavior delete or report messages as spam without opening the actual message. Those decisions were largely based on the "from" and "subject" lines.

This moves us onto the importance of relevance (both of your email subject line as well as your entire message). Always bear in mind that your email messages should be both useful as well as meaningful to your recipients. Ensure you are immediately recognizable in the "from" line and ensure your "subject" line is well thought out and eye-catching.

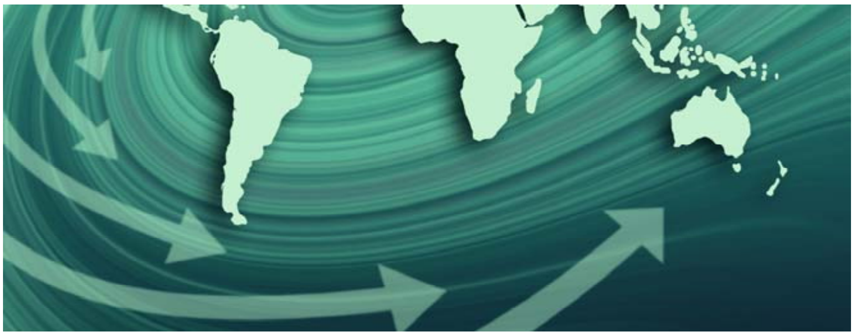
Relevance will not only increase your deliverability by minimizing complaints but also lead to higher open rates, customer engagement, conversions and overall return on your investment in the email channel.

It is also a good practice to ensure your recipients know how often to expect an email from you. Even better, allow recipients to set preferences for how often to email them to ensure that you are not inundating your customers.◊

By Shanti Anne Morais

ANTI-SPAM LEGISLATION AND ENFORCEMENT DOWN-UNDER

Australia is one of the pioneers and leaders in the Asia Pacific when it comes to Anti-Spam legislation. It is also one of the few countries in Asia, which has successfully caught spammers in their country and enforced their Anti-Spam Act. Here's a brief overview of the legislative aspect of the country's Spam Act.



The Australian Communications and Media Authority (ACMA) is responsible for enforcing Spam Act 2003. ACMA has a comprehensive, multi-pronged and practical strategy to fight spam, which focuses on the following key areas:

- directly enforcing the Spam Act 2003
- undertaking effective education and awareness campaigns as well as activities
- working in partnership with the industry
- developing technological and spam-monitoring processes, such as the SpamMATTERS spam reporting toolworking with other governments around the world on international activities to combat spam.

The Australian Spam Act of 2003 prohibits the sending of 'unsolicited commercial electronic messages' (known as spam) with an 'Australian link'. A message has an Australian link if it originates or was commissioned in Australia, or originates overseas but was sent to an address accessed in Australia.

The Spam Act covers emails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (iM) and other electronic messages of a commercial nature. However, the Act does not cover voice or fax telemarketing.

ACMA can take any of the following actions for breaches of the Spam Act:

- issue a formal warning
- accept an enforceable undertaking from a person or company—these undertakings usually contain a formal commitment to comply with the requirement of the Spam Act that ACMA has found that person or company to be in breach of. A failure to abide by an undertaking can lead to ACMA applying for an order in the Federal Court.
- issue infringement notices
- seek an injunction from the Federal Court to stop a person sending spam
- prosecute a person in the Federal Court.

Penalties of up to $1.1 million a day apply to repeat corporate offenders. The penalty units referred to in the Spam Act are equal to $110 each. For example the penalty under section 25 -(5)-(b) of the Spam Act for a company with a previous record of spamming and who sent two or more spam messages on a given day without consent has is a maximum fine of 10,000 penalty units. This equates to a maximum fine of $1,100,000.

The penalty provisions of the Spam Act came into force in April 2004. Initially ACMA focused on educating electronic message senders and raising awareness of the requirements of the Act.

Companies identified during the first few years as possible spammers were in the first instance advised of the requirements of the Spam Act and how they could meet them. In general only serious repeat offenders had enforcement action taken against them.

Having completed this extended education and awareness campaign, ACMA is now committed to vigorous enforcement of the Spam Act. In fact, during the first three years of enforcing the Spam Act, ACMA issued:

- eleven formal warnings
- five enforceable undertakings
- fifteen infringement notices
- one prosecution in the Federal court in Perth - ACMA vs Clarity1/Wayne Mansfield. In October 2006 penalties of $4.5 million and $1 million respectively were handed down against Clarity 1 and its Managing Director.

Since the enforcement provisions of the country's Spam Act 2003 came into effect in April 2004, Australia has gone from tenth in the Sophos list of spam relaying countries (sources of spam) to thirty-fifth for the 2007 calendar year.

Action ACMA has taken against spammers

- **November 2008** - ACMA issued a formal warning to The Ad Company for alleged breaches of the *Spam Act 2003*

continues on Page 57

HONEYPOTS AND SPAM

Wikipedia describes spamtraps very aptly as "honeypots used to collect spam". Spam traps are usually email addresses that are created not for communication, but rather, to lure spam.

In order to prevent legitimate email from being invited, the e-mail address will typically only be published in a location hidden from view such that an automated e-mail address harvester (used by spammers) can find the email address, but no sender would be encouraged to send messages to the email address for any legitimate purpose.

Since no e-mail is solicited by the owner of this spamtrap e-mail address, any e-mail messages sent to this address are immediately considered unsolicited. If you send email to such addresses, you risk being labeled a spammer.

In practice, which addresses are spam traps, where they come from, and how they're used vary enormously. For an address to be useful, it must receive some amount of email.

Many organizations use spam traps. They include DNS blocklists, large ISPs, many spam filter providers, and email reputation organizations.

The specifics of how the spam traps are utilized vary from organization to organization, even from spam trap to spam trap. For example, some organizations rate the value of their traps based on their previous usage; others look for hits on multiple traps; and still others use them only in an advisory capacity along with other metrics.

There are many different types of spam traps, but the most common ones which also tend to be more relevant to email

continues on Page 58

From Page 56 — Anti-Spam Legislation and Enforcement Down-Under

as a result of sending commercial electronic messages by email without the consent of the recipient. It is also alleged that a quantity of the messages did not have an unsubscribe link or information on how to unsubscribe within the messages.

- **August 2008 -** ACMA issued an infringement notice to mBlox Pty Ltd, a multinational company headquartered in the United States, for alleged contraventions of the *Spam Act 2003*. mBlox has committed to work with ACMA to ensure its e-marketing customers are complying with the Spam Act and has paid the $11,000 penalty.
- **August 2008** - Best Buy Australia issued an infringement notice for $4,400 for allegedly breaching the *Spam Act 2003* by sending commercial electronic messages without the consent of the recipient. In particular, customers received emails from Best Buy Australia, including after they had requested to be removed from its mailing lists.
- **July 2007** - DC Marketing issued with a $149,600 penalty for 'missed call' marketing. - Missed call marketing involves the sending of short duration calls to mobile phones, thereby leaving a 'missed call' message on the phone. When the mobile phone owner returned the missed call, they received marketing information from DC Marketing. ACMA penalized DC Marketing for 102 contraventions of the Spam Act 2003 relating to missed call marketing activities in July and August 2006.
- **June 2007** - The ACMA fined the Pitch Entertainment Group (Pitch) $11,000 for extensive breaches of the Spam Act.. ACMA found that the Pitch Entertainment Group, which trades as Splash Mobile in Australia, sent over one million commercial electronic messages to mobile phones without a functional unsubscribe facility. Pitch and its directors have also entered into an enforceable undertaking that requires future compliance with the Spam Act and contains stringent compliance reporting and staff education obligations.
- **June 2007** - ACMA fined International Machinery Parts Pty Ltd (IMP Mobile) $4,400 for breaches of the Spam Act. IMP Mobile also failed to provide a functional unsubscribe facility when sending messages to mobile phones.

27 October 2006 – Justice Nicholson in the Federal Court in Perth today to award a pecuniary penalty of $4.5 million against Clarity1 Pty Ltd and $1 million against its managing director, Mr Wayne Mansfield, for contravening the *Spam Act 2003* (Spam Act). ACMA submitted to the Federal Court that Clarity1 Pty Ltd and Mr Wayne Mansfield sent out at least 231 million commercial emails in twelve months after the Spam Act commenced in April 2004, with most of these messages unsolicited and in breach of the Act. On 13 April 2006, Justice Nicholson found that both Clarity1 and Mr Mansfield were in breach of the Act for both sending unsolicited commercial electronic messages, and for using harvested address lists. ◊

From Page 57 — Honeypots and Spam

marketing are honeypot and dormant addresses.

Honeypots

Spammers of course, compile lists of email addresses to send their spam to. They often get these addresses by roaming the Web looking for any email address listed on a website. Very often, they also sell such lists to other spammers. If they find one, they copy the address and include it on their list.

This process is known as email address harvesting and is usually automated using special "address harvesting" software.

Some organizations involved in tackling spam put specific email addresses on a website for the sole purpose of attracting harvesting software. These addresses are never used for any other purpose: they are merely listed on a web page in such a way that no human would ever discover them or seek to send email to them. Address harvesting software can dig them out of a website, though.

Any email sent to such "honeypot" addresses are immediately classified as spam. The address owner never added the email voluntarily to any email list: they just put it up on a website, so if and when used, it must have been harvested by a spammer and added without permission to a mailing list.

Organizations monitor their honeypot addresses to help them identify both spam emails and their sources.

Dormant addresses

Email accounts often fall into disuse because they are abandoned by their owners or shut down. As a result, the account is unable to receive email.

Legitimate senders of email will stop sending messages to such addresses. They notice a dead address and remove it from their system. Spammers will just keep on sending regardless.

So some organizations (like webmail services) will take dead email accounts and, after a suitable period of time has elapsed, repurpose them as spam traps.

It is important to note that if you send an email to a spam trap, then that hurts and negatively affects your reputation as a sender of email to that particular organization. Sending email to spam traps tends to earn you a tick on the "is this a spammer?" checklist. It also means that your emails to the organization involved will be given closer scrutiny or even blocked from delivery.

How to avoid spam traps? The answer is you normally can't, simply because they are meant to be undetectable. The best advice to avoid falling into spam traps is to get permission before adding an address to your list. Always ensuring your lists are well -cleaned and maintained are also crucial.

Spamtraps also have their vulnerabilities:

A spamtrap becomes tainted when a third party discovers what the spamtrap email address is actually being used for. This opens the spamtrap to getting targeted by spammers.

Spammers using spamtrap addresses from their mailing lists as send addresses can cause backscatter when a reply is sent to the spamtrap address. Backscatter occurs when email servers receiving spam and other mail send bounce messages to an innocent party.

If the spammer put a spamtrap mailbox in the To or CC line, when any other recipient of the mail replies or forwards the message, their address will be considered as spam too.

Many spamtrap addresses are listed in search pages like Google. The mailbox is therefore visible in that page and any can write it without knowing that mail will be caught as spam.◊

LEADING SECURITY THREATS TO SMBS

Unlike large enterprise organizations, small-to-medium sized businesses (SMBs) face multiple security threats with often limited resources to protect assets, data and customer information.

Security threats to SMBs are just as real as they are to enterprise organizations," says Eric Aarrestad, vice president of Marketing at WatchGuard Technologies. "The tragedy is that many SMBs are simply unaware of the unified threat management (UTM) appliances that can combat these threats."

The company's research team has recently identified 10 leading security threats to SMBs:

Insiders – In many SMBs, business records and customer information is often entrusted to a single person. Without adequate checks and balances, including network system logs and automated reports, data loss from within can stretch over long periods of time.

Lack of Contingency Plans – One of the biggest threats to SMBs relates to the business impact of post-hack, intrusion or virus. Many SMBs lack a data loss response policy or disaster recovery plan, leaving their business slow to recover and restart operations.

Unchanged Factory Defaults – Hackers publish and maintain exhaustive lists of default logins (username and password) to nearly every networked device, and can easily take control of network resources if the default factory configuration settings are not changed.

The Unsecured Home – In many small businesses, employees often take laptops home to work. In an unsecured home network environment, a business laptop can be dangerously exposed to viruses, attacks and malware applications.

Reckless Use of Public Networks – A common ruse by attackers is to put up an unsecured wireless access point labeled, “Free Public WiFi” and simply wait for a connection-starved road warrior to connect. With a packet sniffer enabled, an attacker stealthily sees everything the employee types, and is then able to utilize that data for personal gain.

Loss of Portable Devices – Much SMB data is compromised every year due to lost laptops, misplaced mobile devices and left behind USB sticks. Although encryption of mobile device data and use of strong passwords would mitigate many of these losses, many SMB users simply fail to secure their mobile devices and data.

Compromised Web Servers – Many SMBs host their own websites without adequate protection, leaving their business networks exposed to SQL injections and botnet attacks.

Reckless Web Surfing – Now more than ever, malware, spyware, keyloggers and spambots reside in innocuous looking websites. Employees who venture into ostensibly safe sites may be unknowingly exposing their business networks to extreme threats.

Malicious HTML E-mail – No longer are attackers sending e-mails with malicious attachments. Today, the threat is hidden in HTML e-mail messages that include links to malicious, booby-trapped sites. A wrong click can easily lead to a drive by download.

Unpatched Vulnerabilities Open to Known Exploits – More than 90 percent of automated attacks try to leverage known vulnerabilities. Although patches are issued regularly, a short staffed SMB may likely fail to install the latest application updates and patches to their systems, leaving them vulnerable to an otherwise easily stopped attack.◊

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.◊

EMAIL AUTHENTICATION TOOLS STILL NOT WIDELY USED

Only 40 percent of the Fortune 500 companies use tools for e-mail authentication according to an investigation of Secure Computing.

In consideration of the fact that companies could fend off spam and phishing effectively, this is an astounding result, especially since both threats are a constant problem for IT administrators.

Furthermore, data falling into the hands of unauthorized third parties has also to be prevented. Therefore, it is crucial to track both the outgoing and incoming email traffic thoroughly to ensure comprehensive mail security.

According to a survey by Secure Computing, 60 percent of Fortune 500 companies forgo e-mail authentication tools such as Domain Keys Identified Mail (DKIM), or Sender Policy Framework (SPF). Moreover, of the 166 companies who at least employ SPF, only 65 companies use the safest policy, which recommends that the recipient refuses e-mails from unauthorized senders. The remaining 101 enterprises are satisfied with weaker policies, namely the fact that authorized senders are listed. On the other hand they also recommend accepting messages from non-listed senders. Still, such e-mail authentication tools can be a first step towards a better email security.

E-mail authentication with DKIM or SPF

With the Yahoo DKIM standard, companies can encrypt their emails asymmetrically in order to determine whether an e-mail actually comes from the stated domain. The electronic message gets a signature which the recipient can verify with one in the Domain Name System's (DNS) available public key. For that purpose, both the receiving and the sending servers have to be equipped with the appropriate technology. Filtering techniques can then automatically block e-mails that have not been sent through the alleged domain. eBay, for example, used this method for a short time in cooperation with Gmail. Emails from eBay or Paypal, whose signatures are not positively verified get automatically deleted by the provider. And therefore phishing emails that want to attack eBay user data have no chance with Gmail users.

With the Sender Policy Framework (SPF), it can be verify whether a mail server is entitled to send e-mails for a certain domain. To do so, e-mail administrators have to publish SPF records in DNS where it is deposited which computers have the permission to send emails to the domain. However, there have to be available the SPF records of many domains if possible. The larger the spread, the lower the chance of spammers and phishers, simply because if they use a false sender address, they can be quickly traced.

Content Analysis and Encryption

It is not all about protecting the company network from invading emails only.

Outgoing, “outbound” data traffic requires comprehensive monitoring, too. Ultimately, a false handling with confidential information internally, whether intentionally or inadvertently, can make the fall into the wrong hands possible. Also, there are numerous statutory directives that support the strict surveillance of various electronic data. In this case, a content analysis that reviews outgoing e-mails on certain words and data such as social security or bank account numbers can be helpful. In particular, sophisticated technologies possess adaptive word recognition and image analysis technologies.

Numerous compliance requirements demand e-mail encryption in addition that often differentiate between guideline-based cryptographic techniques for B2B and B2C.

Many employees are not familiar with the various encryption options and are irritated by the numerous given ways. Ideally, however, are solutions, where the encryption happens automatically at the gateway. Security risks, posed by failed or inappropriate encryption, can be excluded in this way.

Pro-active security by reputation systems

A pro-active security strategy against malware, denial-of-service attacks but also against spam and phishing are also supported by so-called reputation systems which try to understand the behavior of individual IP addresses both as a receiver as well as sender of messages and to establish appropriate standards.

If an IP address, for example, sends instead of usually ten suddenly 5,000 emails a day, it deviates from the standard and the system classifies the IP as a suspicious. In addition, reputation systems such as that of Secure Computing, Trusted Source, also analyze the content of the messages. The correlation of a "conspicuous" IP address with an unusual outcome of the content analysis (such as unwanted keywords), could result in the general blocking of messages from this specific sender from the gateway itself.

continues on Page 62

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 cost 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

continues on Page 63

From Page 61 — Email Authentication tools still not widely used

These emails then are no risk to the enterprise network and this has not only advantages for the employee who no longer has to delete spam e-mails permanently, but also for the stability of the network as a crucial amount of data is already blocked in the run-up and therefore doesn’t put a strain on the network.
As can be seen, databases play a crucial role when it comes to the accuracy and the quality of the reputation system..

Conclusion

E-mail authentication tools are useful, though so far little-used defence mechanisms. For companies, such standards can only provide additional security. In addition, companies have to check their outbound traffic. Reputation systems seem to be particularly promising for a proactive protection that intercepts dangerous or suspicious mail already at the network gateway.◊

From Page 62 — False positives are on the radar, but spam filters should not be disregarded

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. 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

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 more in-depth from spam.

SUPPLEMENT CONTENTS

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.

Photo: Arun Chandrasekaran

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.

Chandrasekaran believes that legislation definitely helps in

continues on Page 66

From Page 65 — Frost & Sullivan: Do not underestimate spam

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 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

Photo: Participants of MediaBUZZ's event on UTM in 2008

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. Sentinel bridges the gaps in require-

continues on Page 68

From Page 67 — Packing even more of a punch in email security

ments 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. 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 intel-

continues on Page 69

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

continues on Page 70

From Page 68 — Packing even more of a punch in email security

ligence 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

From Page 69 — Spam's not going away and more security with control needed

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, 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

UNIFYING EMAIL SECURITY IS KEY

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

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

continues on Page 72

From Page 72 — Unifying Email Security is Key

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. 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

continues on Page 73

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 cybercriminals' 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 has been making its presence heard and felt, and the whole security industry in

continues on Page 74

From Page 72 — Unifying Email Security is Key

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. ◊

From Page 73 — Email Reputation and Authentication are Crucial in the War

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. 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 only is 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 shares 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 off-shore, 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."◊

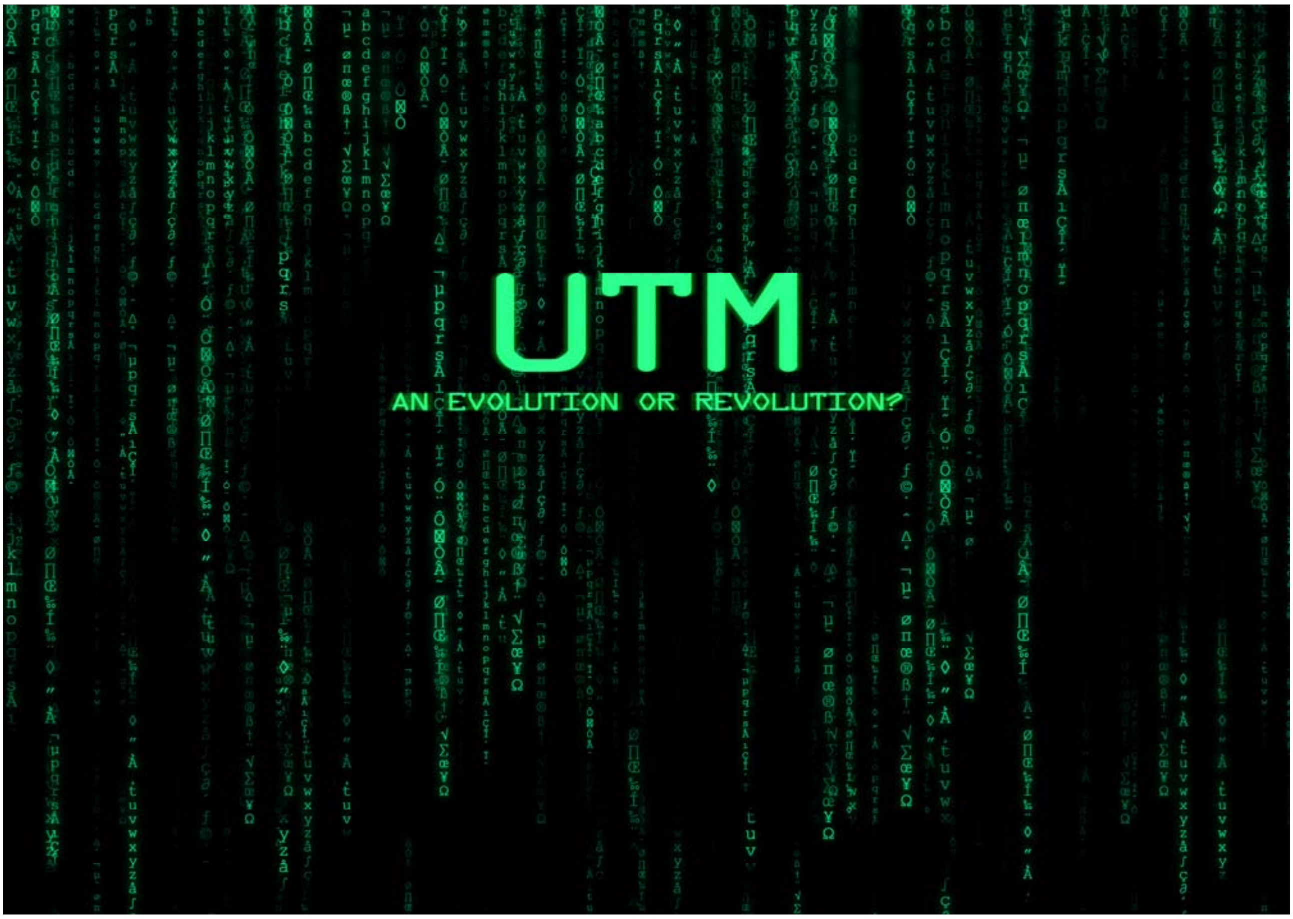
By Shanti Anne Morais

UTM: AN EVOLUTION OR REVOLUTION?

It's no secret that security threats are on the rise. Everywhere you look; there are reports on new breaches, hacking/phishing attacks, spam, malware, Trojans, botnet attacks and more. Security threats to SMBs (small & medium enterprises) are just as real as they are to enterprise organizations. Unfortunately, the tragedy is that many SMBs are simply unaware of Unified Threat Management (UTM) and how it can combat these threats. After all, secure networks afford businesses the freedom to be productive and operate efficiently.

So what exactly is UTM? Originally coined by IDC, UTM refers to comprehensive network infrastructure devices in which multiple security technologies - often firewall, intrusion prevention, antivirus and spyware - are combined into a single appliance. Because these devices provide a single, integrated interface, UTM aims to simplify network security management. Most UTM devices are firewalls or IPS devices at the core, with other technologies available as optional components or modules. However, did you know that conversely, nearly all modern firewalls have UTM capabilities?

While UTM was initially targeted at SMBs, vendors have been trying to move the technology upstream to larger organizations. But just how successful has this strategy been so far? Do you know what UTM means and does for your company? UTM is definitely an up-and-coming trend in the network security world. MediaBUZZ's event "UTM: An Evolution or Revolution?" explored this technology in detail to find out more about it - its current trends and challenges, and what these mean for both users and vendors' alike. Read all about the findings and core discussion points!



THE MANY THREATS OF NETWORK SECURITY

During his presentation at MediaBUZZ's UTM event, Corey Nachreiner, senior network analyst, WatchGuard Technologies took us through the various attacks network security face, how Internet threats have changed since 2003 and just why these threats are more dastardly than we think or even know.

Photo: Corey Nachreiner

Nachreiner put the threat landscape humorously and succinctly in an anecdote: We've all been told, "Oooo, if you use the Internet, a malicious hacker might get you." Right? This kind of talk promotes a mental picture like this: Here's the Internet. Here are a bunch of us innocent folks, using the Internet. Here's you, just another Internet user. Some bad guy pops up. He wants some of your money. So he sends you a scam email: "I'm a poor crippled widow in Nigeria who happens to have a gazillion dollars, and I'll give you half of it if you'll just help me get it to the United States. But first I need you to pay some legal fees on my behalf." Ever gotten an email like that? He sends the email. You receive it. You delete it. The bad guy twirls his handlebar mustaches and says, "Curses! Foiled again!" Then he sends you a virus. Your antivirus stops it."

While Nachreiner trivialized the above for humor's sake, this is exactly what the threat to computer users was in 1998.

A lot of us still carry that mental picture today but the fact is, it is ten years later. Some may ask if the Internet has changed much in ten years. Well, YouTube, Skype and social networks were unseen ten years ago.

In 2003, security professionals noticed a change in the quality and purpose of malicious software, which is called "malware" for short. It soon became apparent that organized crime had moved onto the Internet, essentially changing the face of Internet threats and security forever.

While once upon a time, all we had to worry about was computer viruses' worms and maybe some spam or a server attack or two, nowadays, there is a wide range of malicious code directed at us.

For instance:

- Drive-by downloads lie in wait on web sites so that as soon as we browse there, an attacker's code gets pushed onto our computer.
- Phishing and pharming are deception techniques designed to trick us into giving up sensitive information by convincing us that we are dealing with a legitimate site, when it's really a look-alike under the attacker's control.
- SQL injection is an attack on our web applications that allow attackers to gain control of our website's underlying database, and any sensitive data it may contain

What the above shows, is that today's Internet attacks and threats are very diverse, and this is not going to change for the better but instead probably worsen.

Attack code is big business today, and as a result, attackers want to get onto any computer they can. Another anecdote by Nachreiner: Suppose you're an attacker and you know of a security hole in Internet Explorer. Here's what you do. You create malicious web code that can tell if someone visiting a web site runs Internet Explorer.

You sneak your malicious web code on as many legitimate sites as possible, using various techniques. When victims visit the site, your malicious code exploits the security hole in Internet Explorer to gain access to their computers. Did you target a specific person? No. Did you target a company? No. You targeted the vulnerability itself. Once you get your code on a mass of computers, then you can figure out what is on each of them. The point is, it doesn't matter if you're a small company, or that you mean no harm.

Attackers will still come after you if you have vulnerabilities on your network. It's not personal.

Many of today's attacks are automated mass attacks. Attack code wanders all over the Internet looking for victim machines. By comparison, it has become relatively rare for an attacker manually send an individual attack to against a specific computer or company network.

What's happening nowadays in the network security world is that there are structured teams going after innocent computers now, and they are focused on efficiency. Setting aside rare and exceptional cases, there is almost no such thing as you defending yourself against "a single hacker." We are now up against roving armies of well-coded attackers, financed with

continues on Page 77

From Page 76 — The Many Threats of Network Security

big money, organized by a highly motivated and skilled team, who will rob us if possible while barely noticing we exist, emphasizes Nachreiner.

He adds that the main driving force of hackers is very straightforward – it's all about money for them.

Secondly, hackers/attackers require a lot of computing power and therefore require our computers as resources. "Our computers can help them reach their goals if they have Internet connection, hard drive space so they can stash their files, and email (after all why would an attacker spam from his own computer if he can send it from the computers of 20 or 40 or 100 strangers?). This is why attackers are coming after our machines, regardless of who we are.

Some of today's attack trends include:

Application Vulnerabilities

Attackers used to primarily target vulnerabilities in our operating systems and/or servers. However, vendors have fixed many of the most severe OS and server vulnerabilities, and our firewalls do a pretty good job of protecting our perimeter from external attacks. So lately, attackers have been forced to change their focus, and instead exploit vulnerabilities in client applications, like our web browser, media player, or chat client. These attacks come from the inside-out rather than the outside-in, and they target the weakest security link - users.

Web-based attacks

In general, web-based attacks have become more prominent than email-based attacks. Even the least savvy users have figured out that they should avoid email attachments, so the criminals have moved on to greener fields …. the web.

Blitzkrieg attacks

Attackers rarely target single victims anymore as it's too inefficient and unprofitable. Instead attackers try to automate their attacks on a massive scale.

The advent and rise of botnets

Botnets allow attackers to blend many types of malware into one convenient package. Almost every large scale hacking campaign in the past few years has had a botnet behind it.

New technologies

Finally, attackers are quick to leverage trendy new technologies. For instance, they are already attacking VoIP, IM, P2P, Web 2.0, and many mobile technologies. Since attackers quickly adopt these new technologies, they sometimes figure out ways to attack us that we never dream of let alone anticipate.

Types of Attacks include:

Drive by Downloads

Before 2003, we had to be careful when checking our email, but we could surf the web with indiscretion. This is no longer the case. Now we have to remain wary of malicious web sites that silently force malware onto our computers, called drive-by downloads (DbD).

Sometimes the web sites serving these drive-by downloads are operated by attackers. However, lately attackers have even started hijacking legitimate sites, and booby-trapped them with malicious code. So, perfectly normal websites that we visit often, could one day get hijacked and force a backdoor onto our computers.

In fact, Nachreiner says that web-based attacks like drive-by downloads have overtaken old fashioned email viruses. The statistics, he quotes are frightening. For instance, this year alone, over a million legitimate web sites were hijacked by massive automated attacks, and then forced to serve drive-by downloads. In these specific attacks, sites belonging to trusted entities such as Businessweek, Computer Associates, the Miami Dolphins, and many .edu and .gov sites were all hijacked and loaded with DbDs.

To make matters worse, the hacker underground even sells pre-made web attack kits that make it easy for criminals to launch these drive-by downloads attacks. Some of these web attack kits cost a few hundred to a few thousand dollars on undergrounds forums, others you can find for free. Some examples include kits like, Mpack, icepack, and firepack, which were all made and sold by Russian hackers. They are designed to detect the type of browser a web visitor uses and then exploit the vulnerability that is most likely to work against that browser. Some sellers even offer service and support for their web attack kits, updating them with the latest vulnerabilities.

Reflecting just how bad drive-by downloads have actually become, security firm Sophos finds about 6000 new DbDs links everyday.

Web Application Attacks

Today, we expect websites to deliver dynamic content personalized for us.

To do this, websites have become web applications and have been designed so that we can interact with them in ways we never did before. In the past, websites only displayed information. Now they allow users to post information to them as well.

continues on Page 78

From Page 77 — The Many Threats of Network Security

Unfortunately, this new level of interaction between users and a websites has opened up a new class of security vulnerabilities—Web application attacks.

Cross-Site Scripting (XSS)

One example of a web application attack is Cross-Site Scripting. If a web designer doesn't program his web application to interact with users securely, he gives attackers the opportunity to inject scripts into his web code.

For a long time, buffer overflows were the most commonly reported vulnerability, and one could argue, was the most exploited vulnerability on the Internet. This is no longer true. Cross-site scripting flaws have now become the most commonly reported vulnerability. Jeremiah Grossman, from WhiteHat Security, claims XSS vulnerabilities can be found in 70 percent of websites.

Cross-site Scripting allows you to do stuff on a victim's computer with the same privileges of some other trusted website. This means attackers can exploit XSS flaws to read the cookies of other websites (among other things). So if a banking site suffers from a XSS flaw, a phisher can leverage that flaw to steal the cookie used for you web session to your banking site. In other words, they could log in to your banking site **AS YOU**, and do whatever they wanted. They'd only have to entice you to click on some specially-crafted link for their attack to succeed.

SQL Injection

Most modern websites also rely on a backend SQL database. For instance, when you login to a site that requires authentication, the web application communicates with a database to check your username and password, and uses that to decide what content you should see. Like before, with XSS, if a web designer doesn't code this SQL interaction securely, an attacker can take advantage of flaws in his code to sneak unexpected SQL queries to your database server. This is called a SQL Injection.

There are many evil things attackers can do with SQL injection. They can steal confidential and private date from your database, such as your customer's credit card info, home address, SSN, etc. They can leverage logic tricks within SQL to bypass authentication mechanisms. They can even add, remove, or modify data in your database. For instance, attackers could leverage SQL injections to change the prices of your products on your ecommerce site.

Botnets

Botnets have been around for years. Most IT people first heard of them in 2000, when several thousand coordinated computers all asked to connect to eBay at the same time. That many requests saturates the phone lines and knocks the victim off the Internet. Thus, it is called a "Denial of Service" attack.

Botnets have evolved and matured over the years and are now ranked by every expert as the number one threat on the Internet. One of the biggest, and most infamous, botnets in 2007 was Storm, which some researchers estimated as having up to half a million infected computers all under the control of criminals.

In the Internet's underground economy, hackers trade code, assist each other, and even sell attack code for bots. The result is that evil code is pulling ahead of good guy code. Some of today's malware can be as sophisticated as the expensive commercial software you buy.

And if all this is not scary enough, attackers are always finding new ways to surprise us, targeting new, trendy technologies such as VoIP, SaaS, P2P, Web 2.0, RFID and so on. They also often find unusual vectors of attack that we never thought to consider. For instance, placing a warez server on a printer, or using a Dreamcast game system to sneakily packet sniff on a network. Finally, mobility is really taking off right now. Whether it's smart phones, or USB sticks, or ipods, confidential data is finding its way outside our network in many new ways.

According to Nachreiner, hackers are hard to catch for the following reasons:

Their Botnets protect them. Botmasters use their victim's computer to launch attacks, rather than their own. If authorities trace the attack machine, they end up at grandma's house and still need to find a way to trace the real attacker. Some botnets have multiple technical layers of separation between the botmaster and the computers doing the illegal activity.

In the past, when authorities found malicious phishing or drive-by downloads web sites, they could take them down in a few hours. Now, botnets can keep these malicious sites up for weeks using something called Fast Flux DNS. In short, a botmaster feeds hundreds of his victims' servers the exact same malicious web page. Then, the attacker creates a domain name for his malicious site, for instance, badsite.com. Usually, a domain name like badsite.com would point to only one IP address. However, by exploiting a design flaw in the DNS protocol, attackers can make badsite.com point to a new IP every few minutes. That way, his malicious web site is constantly jumping around to different bots. If the authorities track down one of the bots and shut down it down, the site just moves on to another.

continues on Page 79

From Page 78 — The Many Threats of Network Security

In addition, criminal networks are almost always geographically dispersed. In fact, the individual members of the criminal organization itself may also live in different countries. Depending on the international climate, and your relations with different countries, you can't always get cooperation in prosecuting foreign attacks. In fact, some countries don't even have strong laws against hacking.

Whenever we do find an only attacker, it often tends to be the "campaign managers".

This leaves the big boss to continue his illegal activities with other campaign managers. It's very similar to how hard it is for the authorities to break up real organized crime, like the mob.

In many cases where authorities have found attackers and tried to prosecute them, the legal battles lasted years and cost thousands of dollars. Often loses never get recuperated, and in some cases, the attackers have continued their criminal activity during and after their trials.

So what can be done?

The only completely secure computer is one that is not attached to the Internet. This is a trade-off: if you can use it, then it can't be 100% secure because, by definition, there is a way into your computer, over the network. Security and usability are often like opposite sides of a teeter-totter. One goes up, the other goes down. The trick is to find the balance.

Security experts have therefore introduced the notion of "layered security" to get around this problem. Nachreiner illustrates the concept this way:

Security professionals use the word "control" to refer to a generic defensive technique, without specifying what technique. So let's say you have a security control but it only stops half of the attacks coming at you. Behind it, you put a different security control. It only stops half of the attacks coming at it, too. But since the FIRST control already stopped half of the threats, and the second control stopped half of that half, together they are 75% effective against the total threat. If you keep stopping half of the half, if you line up five controls in sequence, you approach 100% effectiveness.

Nachreiner adds that in reality, a security product that's only half effective couldn't survive in the market. On top of this, various "controls" have to be selected carefully to make sure they really do supplement one another and not just repeat each other. Nachreiner points out here that "security vendors are always telling you to buy one more thing," in this sense, they have a point! The answer, he says, is simple – "defend in depth".

Historically, "defense in depth" required a lot of products such as anti-virus, anti-spyware, spam filters, web filtering to block users from malicious or time-wasting sites, virtual private networks for confidential transactions and firewall/intrusion prevention.

This approach has its own new problems, says Nachreiner, including:

- **Different user interfaces to learn**
- **No accountability among vendors**
- **Inconsistent quality**
- **Various updates and patches at random times**

Enter Unified Threat Management (UTM). A UTM appliance puts "defense in depth" all into one intelligent appliance that

- **Gets the defenses off your computers**
- **Runs off one management interface**
- **Gives you one throat to choke** *(i.e. When something goes wrong, the vendor is much less likely to point at the next guy – because he IS the next guy!)*
- **Updates become predictable and routine**
- **Pick the right one, and quality is assured for years**

Nachreiner says UTM was a really nice step forward in the world of security, to reinforce yet simplify a user's defensive posture.

However, recently, UTM devices are starting to become yesterday's news.

Why? Simply because the bad guys didn't stop innovating, and the Internet environment hasn't stayed the same. Now you have worms and malware traveling via Instant Messaging, and over peer-to-peer file sharing. Attackers are targeting Web 2.0 features, and putting spam in the comments on your blog, or trying to do SQL injection against your custom web application. If any of your users visit MySpace or Facebook, there are attacks specifically targeted at those communities. There is also the "insider" problem – i.e. employees who email sensitive data.

Essentially, UTMs were developed before it became normal to have heavy networking uses such as Voice over Internet Protocol, or streaming video.

What can solve an ever-evolving problem? According to WatchGuard, beyond UTM is XTM (extensible threat management). "Blended threats require blended protection. But you want protection that fits your business today, *and* leaves you with attractive options for tomorrow. That's the exciting promise of XTM," concludes Nachreiner.◊

By Shanti Anne Morais

FROST & SULLIVAN: THE POSSIBILITIES

There is no doubt about it, Internet threats are getting bigger, more malicious, smarter and more damaging. Arun Chandrasekaran, industry manager, Frost & Sullivan points out that the threat landscape has also been undergoing a dramatic shift – from PC viruses that were mainly floppy disk based to Internet viruses that were more email/network based, to malware that was more broadband/website based, to the present day scenario of more targeted attacks, as well as threats that are considered cyber-espionage.

He elaborates that the new security landscape is seeing more covert as well as targeted blended threats, making remediation even more complex. The advent of what Chandrasekaran refers to as "the underground economy" will continue to rise with no signs of abating as the primary motive of such cyber-criminals revolves mainly around the motive of financial gain. Attacks here include phishing, hacking, identity theft, money laundering, bot attacks and the like. In fact, according to him, this shadow Internet economy has been valued at US$105 billion, with this figure looking set to rise even higher.

As a result of all the above and the ensuing challenges in the enterprise ecosystem like disparate systems, little integration as well as high CAPEX & OPEX, Chandrasekaran says that a more holistic view of security that integrates the different dimensions (such as anti-virus, firewall, anti-spam filters, virtual private networks, identity and access control encryption, web security and so on) into a more unified solution is needed – hence the birth of Unified Threat Management – UTM. Chandrasekaran notes that Frost & Sullivan has also been seeing some major trends and shifts in the UTM market. For one thing, when it first started out, UTM appliances tended to be deployed by mainly small and medium enterprises (SMBs), mainly because it was a great value proposition for them. In the last 12-18 months though, Frost & Sullivan has noticed that more large multi-nationals are looking into and taking up UTM, mainly for their branch offices. "UTM is definitely becoming more viable as a platform. For example, it is becoming more scalable. Also, one of the biggest drivers of UTM is its ability to enable the convergence of multiple technologies on a single platform," he elaborates.

He adds that UTM is continuing its trend of climbing up the value chain. "On the services side for example, in the past, there were not many managed security services in UTM but this is now changing especially amongst bigger enterprises and larger managed security services providers," Chandrasekaran states.

With regards to the evolution of UTM, he observes that UTM has already seen a huge shift from its early days (from 2000-2003) when its appliances were predominantly for firewall and anti-virus purposes. Chandrasekaran explains further, "More and more technologies are being added on for example intrusion detection. Now, even web application security is being looked at. In addition, non-security technologies are being considered like WAN acceleration.

The possibilities with UTM are endless and we will definitely see it evolve even more over the next 6-12 months."

While UTM has many merits, he says, such as lower TCO, greater centralized management, evolving technology convergence, ease of use and affordability; it also still has its fair share of challenges – what Chandrasekaran refers to in his presentation as "the undelivered promises of UTM". These include scalability issues, lack of "best of breed" capabilities as well as lack of intelligent integration. However, he is quick to add that these challenges are something the key vendors are aware of and are keen to address. "Again, the evolution of UTM will probably iron out a lot of its issues." "Some vendors are already looking beyond UTM", he concludes.◊

By Shanti Anne Morais

THE UTM STORY

Over the past 5-6 years, the Unified Threat Management (UTM) market in the Asia Pacific market has been taking off. Anthony Lim, Security & Governance Chapter, SiTF, shares with us the colorful back story of UTM and his perspective on it.

Pre-UTM

The emergence of UTM, says Lim, was fuelled to a large extent by the increasing popularity of appliance security solutions made fashionable by Nokia, NetScreen, WatchGuard Technologies, Cisco Systems and more. "Even the likes of ISS, Symantec and Trend Micro had a tryst with these appliances, though I think some were more successful than the other," he observes. "Suddenly, everyone wanted an appliance firewall," he adds. Its popularity was driven mainly by its ease of deployment since the appliances were basically plug and play. Secondly, for the most part, these appliances were by default pre-configured to be ready-to-use. Lim elaborates, "These were important attributes because people were by then deploying them in a hurry and by the droves, due to the runaway proliferation of internet services, which were in turn, driven by the mainstream availability and high volume of broadband connectivity back then."

The end result of this was that other security solutions vendors decided to hop onto the appliance bandwagon resulting in the introduction of anti-virus, anti-spam filters, email security, IDS/IPS and so on. "By 2003/2005, it was not difficult to imagine an enterprise Security Operation Center (SOC) buying and stacking boxes, some of which were by then imaginably colorful (and I mean red, yellow, blue and green instead of the usual grey, black or silver)," he says tongue in cheek.

"So, it became logical to think that this wasn't the best idea because you can imagine rackfuls of security appliances, rackmount servers, patch-boards, hard disks, routers, switches and all the spaghetti in between – you get the idea!" Lim continues.

The Advent of UTM

What happened next was that security vendors endeavored to reduce the number of boxes at the SOC by trying to increase the number of security solutions within the given box (appliance), hence the UTM idea was born.

Notably, the first commercially known attempt at a UTM appliance was probably by Crossbeam Systems. "Here, I don't mean the bar refrigerator size server, $100,000 super-fast, industry product/solution," says Lim.

In 2003, Crossbeam Systems introduced the "C" series—a rather large appliance with a Check Point firewall, Trend Micro anti-virus and ISS' IDS all in the same box. Over the next few years, Crossbeam introduced different sizes and variances of the "C" series. "Not to be outdone, Check Point, ISS and Nokia were soon apparently accusing one another of trying to eliminate the other by introducing firewalls with IDS in the same box or vice versa. Again, you get the idea!" remarks Lim.

"Symantec soon decided their appliance was way too difficult to develop and deal with, preferring to focus instead on merging with Veritas. In the meantime though, WatchGuard, SonicWall, Fortinet, F5 Networks and the rest, proceeded to solder on and eventually formed the UTM market that we know today. It is interesting to note that they all began with different single application appliances," he expands.

"Today," he adds, "Check Point has re-introduced a new set of appliances, while Nokia has decided to put their security appliance division up for sale."

The Current UTM Market

According to Lim, the present day UTM market in the Asia Pacific looks set to grow and is healthy because of a number of reasons:

It is convenient to deploy – especially important amongst SMBs where it is often hard to hire experienced IT security professionals – and can be done both quickly as well as effectively.

UTM saves users the trouble of trying to decide a) which anti-virus, anti-spam or IDS solutions they want; b) what solution users may need that they may have forgotten and c) saves users the trouble of a human resource management issue in case different engineers on your staff prefer different brands or best of breed.

A challenge that Lim feels the UTM market will face is the fact that there may be an attempt to put too many applications into one appliance, in which case, users may end up facing a performance or software management issue.

"In addition, the question of what permutation of applications users will have in which UTM appliance might also arise," he shares.◊

By Shanti Anne Morais

BRINGING THE X FACTOR TO UNIFIED THREAT MANAGEMENT

A visionary and pioneer in the security-appliance marketplace since 1996, WatchGuard Technologies today, is recognized as an advanced technology leader of network-security solutions, with over 500,000 award-winning appliances installed in more than 150 countries.

Consistently named by IDC, Infonetics and Frost & Sullivan as a market leader for SME security appliances, WatchGuard is dedicated to protecting SMEs by providing advanced-security features in its appliances at affordable prices – ensuring all solutions are fully upgradeable to accommodate new features and meet new threats as they emerge.

Widely accepted as a strong viable technology provider for secure remote access, the company recently created a stir in the network-security industry with its announcement to introduce next-generation UTM solutions with extensible threat management (XTM) and connectivity capabilities. WatchGuard's increasing market share is evident in its 190 per cent increase in appliance shipments in 2007, most of which were UTMs – confirming the industry's acceptance of UTM solutions and paving the way for the new XTM platform.

Steve Fallin, director, Rapid Response Team WatchGuard Technologies, shares the company's vision and ideas on XTM with ***Asian Channels***.

What exactly is XTM according to WatchGuard?

Extensibility, the “X” in XTM means having the ability to add on to or extend threat-management capabilities.

WatchGuard's XTM vision is built upon the premise that network security solutions fundamentally need to have this quality. XTM appliances must be able to proactively adapt to dynamic network environments, as well as protect against the litany of known and unknown, future threats. With extensible protection, as a business grows, so does its security platform.

WatchGuard's XTM stands for the extensibility needed for best practices in network-security management and control. Network administrators do not have cookie-cutter environments and have to deal with a constant barrage of threats – known and unknown. Each environment is unique and, therefore, has individualized needs and concerns, depending upon the business and the industry. WatchGuard recognizes this and builds extensibility into its network management and user control features, so that administrators can maximize their XTM investments, which are customized to best suit their network and user needs.

WatchGuard's XTM represents extensible choice. Not only do XTM appliances need to fully interoperate and support mixed network infrastructures, but they need the inherent security technology to be flexible, too. This way, administrators can pick and choose the security service that they want from the XTM device. For example, some may want anti-virus (AV) protection provided at a different source other than the gateway. Now, an administrator can turn "off" the AV protection at the XTM appliance, whilst maintaining full firewall, IPS/IDS as well as web content filtering at the network gateway.

With WatchGuard's XTM, the customer has a choice of security services.

XTM thus provides extensible ownership and leads the industry with software upgradeable UTM devices. This allows businesses to maintain high security without having to rip out and replace older devices – giving unmatched asset protection and lowering the total cost of ownership (TCO). WatchGuard will continue to provide this extended life and functionality with its next-generation XTM appliances.

Lastly, the WatchGuard XTM vision opens the door to extensible market opportunities. WatchGuard envisions uptake of a new class of managed security service providers (MSSPs), who wish to provide highly reliable, "in the cloud", managed-security services to their customers. WatchGuard also foresees the possibility of providing a software platform – similar to that of other extensible applications, such as XML – so that third-party developers can create customized security applications that are tailor-made for WatchGuard XTM appliances.

What makes XTM stand out in the network security arena? What are its main benefits?

Extensible security means giving customers' unparalleled security against the next wave of unknown threats, giving customers uncompromised network management and user control, and giving customers unbridled flexibility and choice. Combining these benefits, WatchGuard is uniquely positioned to give businesses around the world the peace of mind of knowing that their networks as well as their employees' work and data is highly secure with our XTM solutions.

continues on Page 83

From Page 82 — Bringing the "X" Factor to Unified Threat Management

WatchGuard's extensible components include:

- Extensible protection to remain secure against the unknown future threats
- Extensible management for easy control in varied environments
- Extensible choice for interoperability and choice of security services, whilst maintaining exceptional standards of protection
- Extensible ownership through upgradeable devices, thereby offering extended product life and high functionality

The New Reality of Internet Security
What users think the threat is
INTERNET

Photo: Corey Nachreiner

Why do you think XTM is so necessary? Do you think XTM will change the face of network security?

By 2007, the UTM market had grown approximately 35 per cent year-over-year, to reach US$1.216 billion. By 2008, industry analysts estimate that sales of UTM appliances will surpass traditional firewall/VPN solutions. By 2010, sales of UTM devices are expected to exceed US $2.5 billion – creating infinite opportunities for the next-generation UTM solutions.

XTM solutions have the capability to change the industry landscape and redefine network security. As discussed above, they address needs not currently met by the prevailing UTM solutions. Although UTMs offer considerable deployment flexibility, the increasingly sophisticated and decreasingly conspicuous threats in an evolving environment require scalable appliances that can be modified, updated and customised so that high security is always maintained. The changing perimeter of the workplace calls for robust security technology to face the "x" factor of unknown threats.

Tell me about WatchGuard and its XTM vision and strategy? How does this strategy tie up with your overall business strategy and vision?

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high-performance UTM offerings. XTM is the next generation of UTM technology, predicated upon the substantive expansion of three foundational elements: more security; greater networking capabilities; and more management flexibility.

With threat management being constantly challenged and redefined, XTMs are much-needed security solutions in today's dynamic environment. For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilise mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner.

Because of the inherent flexibility found in XTM, these solutions will help businesses address the needs of regulatory compliance and future changes that are bound to come.

What are the key drivers of this strategy and vision?

Threats are becoming more sophisticated and less conspicuous. This leaves networks vulnerable to extremely targeted attacks that include blended threats, such as phishing e-mails with malware payloads. The challenge is to give businesses threat-management solutions that not only adapt, but can proactively address future and unknown threats so that the highest security is always maintained.

Adding to this, most network administrators work in mixed-network environments of disparate infrastructure components and solutions. For these administrators, it is imperative to have a flexible and scalable gateway-security appliance that can be modified, updated and customized to meet their particular security profiles and postures.

The XTM family will enable customers to choose exactly which security functions they want the device to perform, rather than being forced into buying bundles of capabilities, some of which may not be of interest.

What are your plans for this strategy especially in the Asia Pacific?

continues on Page 84

From Page 83 — Bringing the "X" Factor to Unified Threat Management

Are you targeting XTM at certain verticals, sectors and/or markets? Do you think it will be a major attraction to both enterprises as well as SMBs?

WatchGuard's recent vision to introduce next-generation UTM solutions with XTM and connectivity capabilities is keeping the company a step ahead in this competitive marketplace. Creating and designing network-security solutions – which have the ability to proactively adapt to dynamic network environments and protect against unknown threats – WatchGuard's XTM products ensure maximized productivity, with seamless, robust authentication for identity management and powerful endpoint protection for uncompromised network connections. With vastly expanded security features and functionality, networking capabilities and management flexibility, as well as automated processes, WatchGuard's XTM solutions are suited for SMEs and enterprises alike across varied sectors and verticals – purpose built to thwart attacks from today's smarter malware and botnets.

How do your partners in the Asia Pacific especially fit in with this strategy?

They service organizations that have been asking for some of the capabilities embodied by XTM.

APAC buyers are amongst the most discerning in the world. Our two-tiered, partner-centric sales model is designed to attract an expansive network of resellers focused on network-security solutions. Our tier-one distributors carry our full range of products and services to specialised and value-added resellers across the region – increasing our penetration in the SME and enterprise marketplace. We are growing our regional revenue at around 20 per cent per year with Hong Kong, India, Indonesia, Malaysia, Thailand and the Philippines as our key Asian markets.

We are currently recruiting more resellers to boost our UTM and XTM sales.

We are particularly interested in adding resellers with strong technical networking capabilities or those with security expertise.

You'll be announcing new products that will build on your XTM vision. Can you please elaborate on this?

Currently, WatchGuard's firmware release for Peak, Core and Edge appliances have built-in extensibility, so users can leverage this innovative technology today! Later this year, WatchGuard plans to release XTM-branded solutions that incorporate more XTM feature sets – addressing extensible threats (the next generation of blended-security threats), having extensible management (improved scalability and greater granular control), offering extensible choice (network interoperability and feature-set customization), and ensuring extensible ownership (network interoperability, total cost of ownership and return on investment). Global markets for security solutions are constantly evolving.

WatchGuard monitors these markets to ensure that we are aware of the optimal time for the introduction of new products and platforms.

What can we expect over the next 1 year from XTM and WatchGuard?

We have established a trajectory that portends more capabilities and more performance. We will be announcing our new XTM-branded products when the time is right.

Are there any major challenges when it comes to XTM in Asia? If yes, how do you think these challenges can be overcome?

The XTM approach blends seamlessly with the needs of Asian businesses today. For the discerning, skeptical buyer, it provides a sensible and innovative approach to meeting the region's need for flexible, easy-to-use, high-value security solutions. Leading the charge with its pioneering XTM solutions, WatchGuard will continue to create a stir in the Asian network- security market. ◊

By Shanti Anne Morais

UTM: BENT ON CREATING A STORM

WatchGuard's Norbert Kiss gives us the lowdown on Unified Threat Management, the company's strategy and vision on it and its key drivers in the region.

What's your definition of UTM? Is this definition different from the standard in any way? If yes, why?

Unified Threat Management, which stormed the ICT world in 2005, was created due to customer demand for a better way of managing network security for companies of all sizes. Coined by IDC as UTM, 'Unified' signifies that a single device can manage multiple threats, including blended threats – a one-stop shop for customers to manage their network security needs.

Our definition of UTM is the same as that of industry practitioners. However we execute this definition very differently from others within the industry. An example of this is our proxy-based architecture that thoroughly inspects everything that enters the network for threats, providing our customers TRUE Zero Day Protection – compared to most vendors who have packet inspection, thereby checking only a part of the contents. UTM is a gateway technology as opposed to a client technology, so it successfully prevents threats from entering the network. Client-based security only protects the network from threats that have already invaded the network. In spite of working under the same UTM umbrella, the delivery of the WatchGuard offering surpasses industry standards and practices.

Tell me about WatchGuard's vision and strategy when it comes to UTM?

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high-performance UTM offerings. Our vision is to provide customers of all sizes – SMBs or enterprises, with a single device, which is easy to deploy and manage, delivers a quick ROI and adapts well to changing threats.

Our strategy to achieve this is to integrate best-of-breed network-security technology into our UTM devices through innovation and partnerships with leading providers of technologies. The changing perimeter of the workspace, coupled with the "x" factor of unknown threats, has created an opportunity for future UTMs – XTM solutions with next -generation extensible- threat-management technology – which will change the industry landscape and redefine network security. We, as providers of this technology, continue to be evangelists in the market by demonstrating to customers and partners, that UTM and XTM have scaled newer heights to provide greater security technology than the traditional point solutions. We continue to provide our partners with leading channel programmes, education and incentives to ensure they bank on WatchGuard products whilst offering solutions to their customers.

What do you feel makes WatchGuard stand out in UTM market and from your competitors?

There are multiple reasons for WatchGuard's leadership in the network-security industry today. Firstly, WatchGuard's products have distinct technology advantages over our competitors. Being a pioneer of appliance-based network security since 1996, these include Proxy technology, logging and reporting features and more.

continues on Page 86

From Page 85 — UTM: Bent on Creating A Storm

Secondly, *WatchGuard's long-standing reputation as a leading provider of network-security solutions gives us an edge* in this crowded industry. With over 500,000 devices around the world protecting networks at this very moment, our technology speaks for itself. Thirdly, our sales model relies highly on our partners, who have successfully helped to build our brand in the market. We continue to provide them with superior products at competitive pricing, coupled with education and incentives, so they can, in turn, offer the best available technology to their customers.

From your experience, do you see any UTM trends that are particular to the Asia Pacific? Are you seeing a shift in trends in any way when it comes to UTM?

The face of the network security market is changing continuously due to increased internationalisation and globalisation, coupled with dynamically-changing and highly sophisticated internet threats. Even SMBs are finding they must maximise productivity for their remote and mobile users, whilst ensuring a highly secure network. With SMB networks expanding at an ever-increasing pace, UTMs play an important role in addressing these changing trends. UTM as a technology is standard across the world. We haven't seen any specific requirements by geography, apart from local language requirements and the need to manage and block local social-networking sites and chat rooms. However, we have seen a significant difference in the speed of adoption of this technology.

I would say that mature IT markets such as Australia, Hong Kong and Singapore have a high level of acceptance for UTM and penetration continues to grow in these markets. Japan, although a technologically advanced country, has been slow to accept the UTM technology, but we are currently seeing growing adoption there now. Other parts of the region have just begun to realise the varied benefits of UTM and the importance of network security in an increasingly mobile world, which represents a significant opportunity for us to tap into these fast-growing markets.

What are the key drivers of UTM? Do you think there are any underlying factors in the security landscape that are in particular, driving UTM?

All organisations, irrespective of their size, are exposed to the same set of security threats. However, SMBs today have limited budgets for internal or completely outsourced security for technology infrastructure management.

They seek security solutions that ensure increased productivity, lower cost of ownership, compliance assurance or ease of deployment and management, as well as resource scalability and availability. Constantly evolving network-security threats that can cause immeasurable inconvenience, affect a company's reputation and result in unpredicted support costs – forcing SMB management to address these needs.

Traditional remote-access-security solutions are no longer viable solutions for SMBs that require uncompromised network connections, so SMBs are turning rapidly to UTM solutions. WatchGuard's UTM appliances are purpose-built, not only to meet enterprise needs, but SMB needs as well.

Many regard UTM as a technology for SMBs. What's your take on this? Do you think the enterprise also benefits from UTM? Do you think the enterprise is ready for UTM?

It's true that UTM has been primarily focused towards SMBs. This was due to the fact that large enterprises had large IT budgets, multiple staff and would often roll out specific point solutions for specific security threats. This is changing rapidly in these more challenging economic times. The benefits of UTM, including improved threat management and performance are opening new opportunities for UTM in the enterprise space. We can see clear evidence of this as enterprises often take advantage of UTM in their branch offices and remote locations where having multiple point solutions is just not viable. UTM in the enterprise space offers significant benefits to the customers.

"Performance is one of the biggest gotchas in UTM"? Do you agree with this and what is WatchGuard doing in the area of UTM performance?

This has been an unfair perception of UTM for some time. If a customer buys a separate unit for SPAM and separate unit for Web blocking, a separate unit for IPS, etc. and then switches them all on, they will naturally see a slowdown in network traffic. The same is true with a UTM device. If you turn everything on, it will slow down the network. So the issue is not just true for UTMs, but for any network-security solution.

However, there are areas that can be improved. Multiple levels of hardware can improve the performance, giving customers the choice to move up the product chain to gain higher performance levels. Also, the UTM hardware itself has become much faster, with dramatic improvements in UTM performance over the past 12 months – a trend one will continue to see. In spite of this, UTM solutions have been widely accepted by

continues on Page 87

From Page 86 — UTM: Bent on Creating A Storm

customers, and the UTM market has seen enormous growth with vendor revenue of US$100 million in 2004 to US$1.3 billion in 2007. Sales are forecasted to exceed $2.5 billion in 2010*. UTM solutions have typically dominated the network-security arena essentially containing a firewall, network-intrusion detection and prevention, and gateway anti-virus capabilities.

WatchGuard created a stir in the market when it announced its plan to introduce next generation UTM solutions called extensible threat management. Can you tell me more about your XTM vision and how you are paving the way for your XTM solutions? What are the benefits of XTM, why do you think it is so crucial to businesses and what types of companies do you think will benefit the most from it?

Yes, XTM is a very exciting new direction for UTM indeed and we are focused on XTM research and development. WatchGuard is the first network-security vendor to provide a vision on what Chris Kolodgy, IDC Industry Analyst, defines as "the next generation of Unified Threat Management (UTM), integrated network-security appliances," called Extensible Threat Management (XTM). Fundamentally, XTM is the new UTM and is extensible in its ability to protect existing and future unknown threats.

We announced our XTM direction a few months back and expect to have the first products hitting the shelves in Q1 2009. These 10GB throughput products will offer best-of-breed, robust and comprehensive network protection, in-house management, using an intuitive, centralised console, options to for CLI-based management, along with local-language support and localisation. Customers across the board, from SMBs to large enterprises, will benefit from WatchGuard's new XTM technology. WatchGuard's XTM-branded solutions incorporate XTM feature sets – addressing extensible threats (the next generation of blended-security threats), having extensible management (improved scalability and greater granular control), offering extensible choice (network interoperability and feature-set customisation), and ensuring extensible ownership (network interoperability, total cost of ownership and return on investment), which without a doubt are essential and beneficial to any global organisation.

Primarily, XTMs offer enhancements in security, networking and management capabilities. In addition, XTMs will manage security threats from new emerging areas, such as VoIP and HTTPS and provide enhanced SSL security – which is unique to XTM. In the area of network capabilities, XTMs will offer features such as high throughput and high availability, clustering technology – what can be provided with UTM today. On the management side, there will be significant enhancements in visual reporting and connectivity to enterprise-management software such an Openview, Tivoli, etc.

Do you think XTM will change the face of network security? How?

Yes, XTM is on its way to becoming the new standard. XTM solutions have the capability to change the industry landscape and redefine network security. It is the next logical progression to UTM and it will mean that we can adapt faster to new threats, work in much larger networking environments and ensure ease-of-use in terms of management. There is a lot of talk about "cloud computing" and "application hosting" and many companies are now adopting these technologies, which open entirely new security threats – which is exactly what XTM is designed to address. XTMs address needs not currently met by the prevailing UTM solutions. The changing perimeter of the workplace calls for robust security technology to face the "x" factor of unknown threats, and XTMs have the ability to proactively adapt to dynamic network environments and protect against unknown threats.

When can we expect to see WatchGuard's XTM solutions in Asia?

Currently, WatchGuard's firmware release for our Peak, Core and Edge appliances have built-in extensibility, so users can leverage this innovative technology today! Early next year, WatchGuard plans to release XTM-branded solutions (XTM-1050 will be the first one in Q1 2009) that incorporate more purpose-built XTM feature sets – addressing extensible threats, having extensible management, offering extensible choice, and ensuring extensible ownership. Global markets for security solutions are constantly evolving. WatchGuard monitors these markets to ensure that we are aware of the optimal time for the introduction of new products and platforms. We are putting a lot of development effort into XTM and XTM will be the basis of our strategy and products in 2009.◊

By Shanti Anne Morais

INTERNATIONAL ANTI-SPAM LEGISLATION SNAPSHOT

Singapore	USA	Australia		Hong Kong	Japan
Date Commenced	15 June 2007	1 January 2004	11 April 2004 (some part came into effect 12 December 2003)	1 June 2007	1 July 2002
Legislation Title	Spam Control Act	CAN-SPAM (Federal)	Spam Act (Federal)	Unsolicited Electronic Messages Ordinance (UEMO)	Law on Regulation of Transmission of Specified Electronic Mail (Law No. 26 of April 17, 2002), as amended by Law No. 87 of July 26, 2005 (the "Anti-Spam Law")
Application	Singapore "link"	US	Australian "link"	Hong Kong "link"	Japan
Options	Opt-out	Opt-out	Opt-in [purely factual emails are exempt]	Opt-out	Opt-out
"Bulk"	Must be sent in bulk to be spam (>100 during 24hrs period, >1,000 during a 30 day period, >10,000 during a one year period)	No requirement for message to be sent in bulk	No requirement for message to be sent in bulk	Must be sent in bulk to be spam (>100 during 24hrs period, >1,000 during a 30 day period)	No requirement for message to be sent in bulk
Penalty	Not Criminal Injunction S$25 per message up to S$1million	Criminal□ US$250 per message up to US$2million	Not Criminal A$220,000 for individuals, A$1million for companies	Criminal HK$1million (individual)/ Maximum 5 years imprisonment	Criminal ¥1million (individual)/ Maximum 1 year imprisonment
Other	Not necessarily required to have a valid postal address <ADV> requirement Must be in English	Must have a valid postal address No specific reference to <ADV> (but must be signposted as an advertisement)	Even requested email require an opt-out function	Unsubscribe must be in Chinese and English	Must have valid postal address No specific reference to <ADV> (but must be signposted as an advertisement)

Prepared July 2008 by AOTA (Authentication & Online Trust Alliance))

Points to note:

- Criminal prosecution maybe under related legislation
- All require accurate header and sender info
- All prohibit dictionary attacks and address-harvesting software
- "Link" means the legislation not only apply to emails physically originated in that country but also sent by an organization having a legal entity in that country (regardless of where the offending email was commissioned and sent from)

Please note that this snapshot is not intended and should not be taken as a substitute for professional legal advice. Please consult your own legal counsel to ensure communications are in full compliance with Singapore and International law.

Reg. No. 200407301C

MediaBUZZ Pte Ltd aims to make an impact in the region through two unique electronic publications Asian Channels and Asian e-Marketing, and through events relating to and serving these two industries.

Asian Channels is the very first of its kind in the region and the only guide for technology channels in the Asia Pacific. More information: www.mediabuzz.com.sg/asian-channels/

Asian e-Marketing is a pioneer e-publication in the Asia Pacific, covering the digital age and zooming in on the increasingly valuable and indispensable tool of today's marketers – the Internet. More information: www.mediabuzz.com.sg/asian-emarketing/