EdgeWave™

Beyond Spam – Email Security in the Age of Blended Threats

How Emerging Threats, Compliance Violations and Data Loss are changing the Messaging Security Landscape

The New Threat Reality

If the last decade is any indication of the types and volume of spam that companies are likely to see going forward, then it is clear that they are in for quite a battle from a variety of new, random and complex attacks with potentially catastrophic results. Spam started out simply enough as a way for advertisers to quickly and cheaply get their messages to a large audience. With thousands, to potentially millions, of unsuspecting people as targets, even meager response rates of less than one percent produced profitable spam campaigns and turned the in-box into the next "great" junk-mail marketing medium.

It wasn't long before email users declared spam a nuisance and the world witnessed the birth of the first anti-spam filters and Real-Time Black List (RBL). Unfortunately, as quickly as new spam-fighting technology and filters have been deployed to stop spam, spammers have been equally innovative, changing their tactics to bypass virtual roadblocks in pursuit of just a few users that would open the emails and click. It is these email users who are the target. Clever technology combined with email user error and ignorance has often placed cyber criminals at an advantage, proving that filters and corporate policies cannot stop everyone from opening doors to personal information and corporate networks.

This intense battle against cyber crime has never been as strong as it is today as spammers and cyber criminals strive to stay one step ahead of the latest email security improvements. They know that if they can get their messages around filters into email inboxes – even a few – they have a chance of turning clicks and data into profits. Like the scammers, security solution providers are constantly working to thwart these criminals, moving beyond simply stopping the campaigns to predicting where and when the next attack will be launched.

How New Threats Impact Organizations

It is important to realize that the costs associated with these increasingly more sophisticated attacks go beyond the financial loss inherent in criminal malware attacks to include risks to corporate reputation as well as bottom lines. These losses can have a debilitating effect on your organizations' name and assets. The damage can include: Regulatory non-compliance – Failure to comply with legislation such as HIPAA, GLBA, SOX and others can result in huge fines, lost revenue and even litigation. Some recent SOX violations have involved the failure to protect data and they incurred substantial losses. The totals below include settlement fees, lost business, fines and remediation costs all resulting from breaches in SOX regulations:

- American Home Products: $3.75 billion
- Bank of Credit and Commerce : $17 billion
- BAT Industries: $73 billion
- IBM: $6 billion
- Prudential Insurance: $4 billion

Secure Email Delivery – We live in an age where virtually every organization depends on email to communicate whether to customers, clients, partners, vendors, or others. And organizations need to have confidence that the private and critical email they send will be securely delivered and protected from intrusion. The loss of an important invoice or order or the exposure of confidential information to the wrong entity can have severe and lasting consequences.

Brand/Reputation Damage – Harder to quantify but equally troubling is the brand damage that can occur when an email-borne attack results in litigation or fines or other high-profile consequences. Once an organization's good name is sullied, it may take years for it to regain a good reputation and solid industry footing.

Lost Email – Experts have reported that virtually all organizations experience email interruptions whether planned or unplanned events. Recent studies have found that companies lose typically 40 hours per year in email downtime. In addition to the inconvenience this poses, the prospect of losing business-critical email cannot be underestimated. Emails in transit that are lost due to server or power interruptions can adversely impact corporate bottom lines and cause delays in or losses of customer orders, invoices and other vital communications.

This white paper will focus on defining the new threat reality, which includes new tactics and designs, embedded links, spear phishing, malware, botnets and mobile attacks that are more sophisticated and catastrophic. We will provide examples and analysis of the next generation of threats and risks in an effort to arm organizations with the knowledge and tools required to keep them from becoming victims. We will also give you a preview of some next-generation technologies that can mitigate these threats and protect organizations of all sizes and in every market.

Seven Emerging Email Threats

The following section outlines eight threats that have emerged recently and are likely to continue to trend upward for the foreseeable future.

Blended Threats - Botnets

One of the most rapidly growing types of spam today comes in the form of blended threats. In the early days of spam, messages typically served a single purpose; trying to get unsuspecting email users to respond to an email by buying a product or clicking on a link in an email. For many early spam campaigns, the person or entity sending the email made money when the email was opened or when recipients clicked on links embedded in the email. While the spam was unwanted, it was typically easy to spot, and quickly deleted. The level of the threat, however, quickly changed when the embedded links or attachments became malicious in nature. Cyber criminals started to use email to send viruses and malware executables, as well as linking to web sites that had malware embedded in the site's HTML code. A simple click on a link or opening an attachment could launch a virus giving remote access to a scammer half-way around the world or sending personal financial information stored on the PC to a host location.

Today, scammers have taken malicious spam to another level, distributing emails with blended threats that phish for personal or corporate information, as well as install viruses and route recipients to websites that lead to immediate malware execution. In addition, these emails come disguised in graphical wrappers that mimic trusted sites like national and community banks, and contain files that have trusted extensions, including .doc, .pdf and .jpg.

For instance, an e-Card spam campaign discovered In December 2009 appeared to come from American Greetings' BlueMountain.com.

The email, with the subject line "You received a BlueMountain e-Card!," suggests that users "need to install the Macromedia Flash Plug-in" to see the "complete version" of the e-Card. The entire body of the email, including the header and footer of a legitimate Blue Mountain e-Card, was an executable. Clicking on any part of the message would launch a browser window, and depending on a user's browser security settings, could have automatically downloaded a virus with a single click. The spam was distributed by a botnet and had been aggressively targeting Internet Service Providers. The virus was also identified as a banking Trojan, which are used by cyber criminals to steal banking credentials from computer hard drives or web forms or by capturing keystrokes. Most banking Trojans stay dormant until an unsuspecting customer logs on to his or her banking website. The Trojan then steals usernames and passwords and sends the information back to its creator(s).

People like e-cards and trust sites like BlueMountain.com. Consequently, senders with bad intentions are utilizing commonly used Internet services, going as far as designing the fake emails and corresponding web sites to have the same look and feel as the actual brands.

The BlueMountain attack illustrates the danger of botnets, networks of compromised computers controlled by criminal third parties. They are different from Spam, Phishing and Viruses that current solutions address in three respects: First, botnets are usually controlled by organized criminal syndicates or state actors with a malicious purpose, as compared to individual or small groups of hackers engaging in pranks, on-line graffiti, or spam marketing. Second, botnets are active exploits designed to get inside your network, often by social networking or piggybacking on devices brought in from outside, such as laptops, smartphones, and USB drives. The bots that form botnets are very stealthy and can lurk deep inside your network for weeks or months. They remain inactive until they communicate with their command and

control hosts (C & C hosts) outside your network to receive instructions. Once the bot reports "I am here waiting for instructions", they begin to receive commands. They may be told to "replicate themselves" or to "infect other machines in the network". They can also receive instructions such as "steal credit card numbers from your customer database". By contrast, most spamware is acted on by the user, not through the control of a remote party. Third, botnets are designed to steal your most valuable data, be it customer credit card numbers, your personnel data, or your engineering designs.

Botnets are Notorious

A breach by a botnet is an expensive problem to fix once discovered and the longer it remains undetected the worse it will be. There is the obvious financial cost of remediation, but there can also be significant damage done to an organization's brand reputation from public exposure and being forced to pay fines for failing data security compliance regulations. Careers of executives and IT/security personnel are often damaged, as well. In a few extreme cases, a breach can be serious enough to shut a business down.

In 2010, the Waledac botnet was formed after initially infecting organizations via email. It spread by sending e-mail containing links to copies of itself and also opened backdoors on compromised computers. In just a short period of time one Waledac domain was able to resolve to multiple hosts acting merely as proxies. Its fast-flux DNS (Domain Name System) made it harder to track the source, which was one of Waledac's defense mechanisms. Although the original Waledac attack was eventually thwarted by Microsoft, a second version was found recently that contained nearly 500,000 stolen email passwords, allowing massive spam-producing networks free reign in spreading malware.

Other high profile botnet cases have included attacks on Sony PlayStation, which forced them to shut down their gaming network after personal accounts for more 100 million customers were compromised. There were similar attacks on Citibank and Amazon. The Sony breaches are estimated to have cost one billion dollars to remediate. In a well-known study by the Ponemon Institute, the average cost of a security breach for a large enterprise is almost $7 million, with a range of $750,000-31,000,000.

Classic Phishing

While blended threats are on the rise, classic phishing campaigns still pose a significant threat to email users and corporate networks. Not only are swindlers using phishing attacks to target average consumers, such as the Nigerian 419 phishing campaign that continues to find victims, they are also targeting business professionals, including the legal community that is fighting to stop them. Today's phishing attacks have also stolen the branding elements of trusted organizations, once again hoping that email users are not paying attention to the details.

Among recent examples of highly publicized phishing attacks is one involving the Center for Disease Control and Prevention (CDC) during the height of the H1N1 Vaccination concern.

The email with the subject line "State Vaccination H1N1 Program," suggested that recipients "need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website." When users clicked on the embedded "Create Personal Profile" link in the email, they were sent to a page that had a CDC-branded header and footer, as well as the U.S. Department of Health and Human Services logo. Visitors to the site were notified that their "Personal H1N1 Vaccination Profile" is an "electronic document, which contains your name, your contact details and your medical data" and needs to be downloaded. The file was actually an executable that contained a Trojan virus identified as W32/Vacc.A!tr. Email recipients that downloaded the "electronic document" would have installed the virus on their computer allowing the malware to use the computer to send out additional spam. For those that visited the site, but did not download the file, the fake web site also contained malware that exploited recent vulnerabilities in Adobe Reader and Flash software.

This particular hoax posed a threat to email users and corporate networks, and also forced the CDC to scramble to address the media attention.

Spear Phishing

A spear phishing campaign is a highly targeted form of phishing that typically focuses on a single organization. Recent examples of spear phishing campaigns however are more sophisticated, targeting a large number of domains with highly personalized and customized messages. Emails appear as if they come from a trusted source, such as an employer who would normally send an email to the entire company or a well-known organization. Because of the familiar sender ID, email recipients may not pay attention to the other details in the email, and are likely to do what the email asks.

One example of this type of phishing attack occurred on the campus of Dominican University in Chicago in the spring of 2009. As a result of the attack, Dominican was blacklisted by several major email providers, including MSN, Yahoo and Hotmail. The phishing emails warned users that their university web mail accounts were going to be cancelled unless they replied to the emails with their usernames and passwords. Unfortunately, some users became victim to the scam, and it wasn't long before their email accounts were being used to send spam messages around the world. The attack forced the university's IT department to constantly monitor its email queues to determine which accounts were being spoofed, while the multiple attacks frustrated efforts to clean the university's domain.

A more recent example of spear phishing threats can be found in a report related to the botnet attack on Sony. Customers who were victims of the Sony breach were warned to watch out for spear phishing scams resulting from the original attack. Experts said that the cyber criminals who compromised Sony gathered enough personal information to launch spear phishing attacks on unsuspecting victims. In a statement, Sony urged customers, to be "especially aware" of these scams. "Sony will not contact you in any way, including email, asking for your credit card number, Social Security number or other personal information," the company said in a letter to customers posted on its Web site. "If you are asked for this information, you can be confident Sony is not the entity asking." These attacks worry Sony and other vendors who have been breached because the damage clearly doesn't end after a botnet or worm has been detected and remediated. With the personal information gathered in these attacks, cyber criminals launch customized email campaigns aimed at reaching the real goal of the original breach, financial gain, by getting customers to reveal their credit card or social security numbers.

Social Media

Another significant target of this New Threat Reality is specifically targeted at social networking sites like Facebook, Twitter, MySpace, etc. These sophisticated phishing attacks combine email and spoofed social networking sites in an attempt to solicit personal and financial information.

With more than 400 million users, Facebook has almost become ubiquitous, making Facebook users a prime target for cyber criminals. By spoofing the branding elements of these social networking sites, criminals prey on users' comfort levels with these brands to gather personal information that will grant them access to a variety of private and confidential data.

While Facebook has been the object of numerous spam campaigns, in the fall of 2009, scammers distributed a massive blended-threat Facebook spam attack that included a phishing scam and a notorious banking Trojan virus. A link within the spam email took users to a spoofed Facebook login page requesting the user's Facebook account information. After entering their credentials, users were then prompted to download "updatetool.exe," a Zbot Trojan variant that is known to scour the infected hard-drive for personal banking information and various login credentials, as well as perform key-logging and other nefarious activities.

As noted by the image above, the spoofed Facebook login page was fairly sophisticated and used www.facebook.com in the sub-domain portion of the malicious URL. As a result, people with small screen resolution or small browser windows/address bars size might think they are actually on Facebook's login page.

Another threat in 2011, involved 400 million Facebook users who were targeted by a spam effort to infect computers with a botnet that would steal user passwords and other personal data. The messages appeared to come from Facebook with a legitimate spoofed address such as "help@facebook.com". The messages said that the user's Facebook password was reset and that the user needed to download an attachment containing the new password. The attachment was actually a Trojan horse program, which could infect a computer transparently – leaving no clue to the user that anything had occurred. The spam message contained a variety of malware programs, including password stealers, rogue antivirus programs or botnet code.

It is this familiarity and user comfort level with these popular sites and services that spam developers are now targeting. Unfortunately in many of these attacks, millions of victims are at risk and when anti-virus engines don't detect the campaign, it can reach vast numbers of inboxes across the country and even globally.

Rapid-Evolution Malware

While viral mutation is nothing new to the industry, polymorphic virus technology continues to defeat many anti-virus engines that are the first line of defense. The ability for the virus to change its binary code each time it infects a file makes it difficult for traditional anti-virus engines to detect a pattern, and thus stop the virus from spreading. Embedding malware onto computers and networks has become a key motivator behind spam campaigns, and without the appropriate behavior-based malware detection and real-time defenses, polymorphic viruses may go undetected.

Viral mutating malware can corrupt computer systems while going undetected for extended periods of time. Depending on if/when the malware is detected, the virus can do everything from modifying files to point to malicious web sites to actually making a system inoperable.

Highly Permuted, Short-lived Campaigns

In an effort to further circumvent today's anti-spam technology, many spam emailers have increased the randomness and shortened the duration and reach of their campaigns. What were once massive attacks spread out over several days have now become focused attacks played out in a matter of minutes. Many anti-virus engines and anti-spam filters simply miss these campaigns because of the higher degrees of randomization. Before they know it, companies have become victims as security filters are unable to respond to the real-time threats. The randomness further complicates the situation because security administrators don't have the information they need to create filtering rules that will thwart future campaigns of this type.

Smartphone Attacks

With more people using Smartphones to send and receive email, network administrators are learning the hard way that security must extend beyond the desktop and the corporate network. Cyber criminals have started to develop sophisticated botnets specifically for Smartphones. Once installed on the phone, intruders have the ability to use the phone just as they would an infected computer.

An iPhone worm discovered in November 2009 took advantage of iPhone users who had unlocked their phones and failed to change the default password. This particular bot launched a popup window notifying the iPhone owner that his/her phone has been hacked. The victim was then sent to a web site that demanded a $5 ransom payment to remove the malware. A second iPhone bot detected the same month also targeted "jailbroken" iPhones. The bot gave the hacker the ability to use the phone to spread spam, pilfer data and seize online accounts. In this attack, the worm also changed the default system password making it difficult for users to regain control.

While the two iPhone examples mentioned above targeted people that had modified their phones' security settings, the growing and widespread adoption of Smartphones has presented a significant challenge for users and their employers.

Combating the New Threat Reality

In order to combat this New Threat Reality, companies need to understand that the attack methods of hackers and cyber criminals have changed and will continue to evolve. Unfortunately, security technology has not always kept pace with the threats. Spam was once seen as a nuisance with low overall impact on email users and networks. The massive attacks were spread out over long periods of time, making it easier for corporate defenses to filter out the spam and prevent any widespread problems. Email was the preferred medium and spam typically had a single purpose. Statistical defenses were adequate in thwarting the campaigns while false negatives and false positives were the focus for email security solution providers.

Today, the threats and risks every business faces go beyond spam. Risks inherent in email downtime and data loss combine with threats from criminal malware to form a matrix of potentially catastrophic consequences. These threats also include multiple components, incorporating elements of social media and privilege escalation in an attempt to bypass security and access private and confidential files, resources and information.

Reactionary solutions are no longer enough, as the new threats require real-time dynamic feedback that will protect users from yesterday's threats, as well as help predict emerging attacks, while providing end-to-end protection of organizations' critical messaging stream.

EdgeWave Messaging Security Suite Offers Multi-Layered Comprehensive Defense

EdgeWave's proprietary Messaging Security Suite offers hosted services that arm organizations with the defense shield they need to fight emerging threats such as the ones discussed in this white paper. Offered in an integrated comprehensive suite of solutions, EdgeWave's has the next generation technology required to defend against threats that go beyond mere spam blocking. These services are integrated into EdgeWave's convenient management interface and can easily be enabled to provide comprehensive risk management and protection from threats.

Email Filtering

EdgWave's email security technology was developed to protect against the emerging messaging threats not handled by most anti-virus, anti-spam (AVAS) vendors. To meet these modern challenges and requirements, EdgeWave has developed the Zero Minute Defense Network and added layers of filters, which gather real-time knowledge to rapidly create new detection and protection rules. These rules are then pushed out continuously to customers through EdgeWave's fully managed Hosted Service. It is the company's combination of global reach, speed of rule execution, breadth of rules and layers of defenses that is helping EdgeWave provide customers with the tools to effectively face the new threat reality.

Email Continuity

This service defends against planned and unplanned email interruptions by automatically retaining organizations' email if the server is unavailable for any reason. Once enabled, messages are automatically spooled and users can easily access their email as if no interruption had happened, allowing them to read, compose, reply to, forward and delete messages or upload and download attachments. Sent messages can be automatically spooled so users can retrieve them later. This essential disaster recovery tool is quickly and easily enabled via the EdgeWave Messaging Security Suite management interface and will prevent any business downtime or lost messages that could result from a business-critical email interruptions.

Data Loss Protection

EdgeWave Email Security includes a content analysis and policy engine that uses proprietary technology to protect private information transmitted via outgoing email. As part of EdgeWave's Secure Content Management portfolio, this data protection technology analyzes data being sent out of your network to detect private content in data-in-motion and prevent sensitive and protected data from leaving your network. EdgeWave DLP helps organizations comply with government regulations, such as HIPAA and GLBA, and prevents the loss of all types of private data, including, patient healthcare information, financial information and social security and credit card numbers. This service provides essential analysis of the outbound email stream to prevent the regulatory violations and financial losses associated with proprietary or sensitive data exposure.

Encryption

EdgeWave Encryption Service provides secure delivery for any email leaving an organization and can be enabled on an automatic policy routing basis or individually enabled per sender. It employs park and pull technology designed to provide secure communication between the sender and the recipient of messages, even individuals outside and unrelated to the sender's organization. All emails using encryption can be routed based on a variety of rules leveraging EdgeWave's email filtering technology. Park and pull encryption is enhanced by EdgeWave DLP so that encryption can be triggered by DLP violations. Unlike end-to-end encryption, the park and pull technique does not require the installation of any software by the sender, recipient or on the email hosts of either. Nor does it require an encryption key to deliver the email.

Archive

As a SaaS solution, EdgeWave Email Archive delivers maximum scalability, provided by off-premises archiving that reduces costs and provides scalable storage capacity that can grow to meet your organization's demands without incurring additional costs. Our archive is easy-to-deploy and includes an intuitive interface via a browser, so implementation can be achieved within minutes and ongoing management and maintenance are virtually touch-free.

Summary

Clearly, not all email security solutions are built to defend against emerging email threats. Regardless of whether someone is using a desktop, laptop, netbook, tablet or Smartphone, an organization's umbrella of security needs to protect any device connected to their networks and deliver real-time protection from the variety of threats to email infrastructures. Implementing a suite of messaging security solutions that can meet tomorrow's threat reality with equally sophisticated, real-time, comprehensive defenses, gives organizations in all industries, a better chance of avoiding catastrophe.

About EdgeWave

EdgeWave, Inc. develops and markets on demand, on-premises, and hybrid Secure Content Management (SCM) solutions to the mid-enterprise and service provider markets. The EdgeWave portfolio of Web and Messaging Security technologies delivers comprehensive secure content management with unrivalled ease of deployment and the lowest TCO on the market. EdgeWave strives to deliver simple, high performance solutions that offer excellent value.

Based in San Diego, California, EdgeWave markets its solutions through a network of value added resellers, ISPs and MSPs, distributors, system integrators, OEM partners and directly to end users.