Today's New Breed of Email-based Cyber Attacks—and What it Takes to Defend Against Them

Overview

More often than not, businesses are being targeted by today's new breed of cyber attacks. In fact, during the time it takes you to read this newsletter, odds are that your organization will have been targeted by a cyber attack.

Today's new breed of cyber attacks routinely circumvent firewalls, intrusion prevention systems (IPS), anti-virus (AV), and other defenses—and enable cybercriminals to achieve their goals, whether they are looking to make financial gains, steal intellectual property, or further nation-state objectives.

Traditional defenses are not working because today's attacks are ...

- **Dynamic.** Today's sophisticated attackers can quickly morph their attacks so they are new, never-been-seen-before attacks, causing them to go undetected by legacy signature-based security solutions.
- **Targeted.** Advanced attacks are sent only to the specific industries, companies, and individuals being targeted. By avoiding the "noise" of larger, scatter-shot campaigns, these highly targeted attacks can stay under the radar—and go undetected by anti-virus and spam detection mechanisms.

- **Multi-faceted.** Many attacks combine Web and email tactics in multiple stages so evade Web-only and email-only defenses, which focus on just one stage of an advanced attack. But a single cyber attack may be comprised of sophisticated malware that exploits a zero-day vulnerability, a spear phishing email, malicious websites appearing on dynamic URLs, and a complex network of command servers for controlling compromised devices and stealing targeted assets.

Source: FireEye

Featuring research from Gartner

Spear Phishing: A Common Launch Point of Advanced Attacks

The new breed of cyber attacks has combined a range of different tactics, but it is clear that there is one very common characteristic: spear phishing is the primary channel through which the attacks are initiated. Operation Aurora, GhostNet, Night Dragon, the RSA breach, and the majority of the other attacks that have been publicly documented have been initiated at least in part through targeted spear phishing emails.

Spear phishing attacks often combine such tactics as victim segmentation, email personalization, sender impersonation, and other techniques to bypass email filters and trick targets into clicking a link or opening an attachment. By mining social networks, for example, the personalization and impersonation used in spear phishing emails can be extremely accurate and compelling to the recipient.

Understanding the tactics and characteristics of these spear phishing attacks is vital as security teams seek to establish effective defenses. FireEye® researchers have discovered the following in analyzing spear phishing activities.

Most Common File Names

Often, attackers attach malicious files to spear phishing emails. To lure unsuspecting users into opening these files and initiating the malicious code, attackers typically use file names with common business terms. The terms used tend to fall into three general categories: shipping and delivery, finance, and general business (see Figure 1 for the top five terms).

Figure 1: Top 5 malicious email attachment names used in spear phishing attacks[1]

Rank	File Name
1	Details.zip
2	UPS_document.zip
3	DCIM.zip
4	HP_Document.zip
5	Report.zip

Top Words in Malicious Attachments

Figure 2 outlines the top five terms that show up in malicious email attachment file names. Similar to the top terms used in email attachment names, these terms relate to shipping.

Figure 2: Top 5 terms that show up in malicious email attachment file names[1]

Rank	Word
1	'ups'
2	'details'
3	'document'
4	'fedex'
5	'myups'

Malicious Email Attachment Extensions

In evaluating email file attachment extensions, it quickly becomes obvious that .zip files are currently the most common malware file type employed. This is because organizations typically do not block these file extensions, and attackers understand this. Further and more critically, attackers understand that, by embedding malicious payloads within .zip files, this code will go undetected by scanners.

Malicious URLs in Emails

Cybercriminals are increasingly employing malicious URLs for only a brief period of time before they move on to using new URLs. "Throw-away" domains are malicious domain names used only a handful of times, in approximately 10 or fewer spear phishing emails. These domains are so infrequently used that they fly under the radar of URL blacklists and reputation analysis and remain largely ignored and unknown.

Source: FireEye

[1] "FireEye Advanced Threat Report – 2H 2012"

Combatting the New Breed of Cyber Attacks: The Key Requirements

Today, organizations need a next-generation threat protection platform, one that detects and blocks the new breed of attacks.

Organizations need an integrated, correlated view of all the potential attack vectors that spear phishers may use. This includes real-time, comprehensive views of the following threat vectors:

- **Email.** Spear phishing emails represent one of the most common approaches for launching an advanced attack. Guarding against these types of threats requires real-time analysis of URLs in emails, email attachments, and Web objects to determine whether they are malicious.
- **Web.** Browser-based threats and malicious communications can take many forms and move across a range of protocols, including FTP, HTTP, and IRC. Websites and communications need to be tracked in real time, across these different protocols to thwart advanced attacks.
- **Files.** Even if Web and email channels are secured, malicious files can still make it into a corporate network in any number of ways, whether through a USB drive, a mobile device, download from a cloud service, or a host of other means.

Intelligence from across these threat vectors needs to be correlated to be truly effective. In order to guard against sophisticated spear phishing attacks, security teams need capabilities for discovering a Web-based attack in real time, tracing it to the initial email that spawned the attack, and then doing the analysis required to determine if others within the organization have been targeted.

How FireEye Delivers Effective Defense Against Advanced Email Attacks

According to Gartner, the greater level of danger posed by targeted phishing email attacks is shifting the focus of advanced email security solutions within enterprises[2].

The FireEye platform supplements traditional defenses with a new model of security to protect against today's new breed of cyber attacks. The unique FireEye platform provides the only next-generation threat protection that dynamically identifies and blocks cyber attacks in real time.

Utilizing a signature-less, virtual execution engine that creates enterprise-specific threat intelligence across vectors, the FireEye platform secures against Web, email, and file attacks. By detonating Web objects, and suspicious attachments within virtual environments, the FireEye platform is uniquely equipped to detect zero-day Web exploits, spear phishing attacks, and malware resident on file shares. By correlating multi-vector threat intelligence, this enables the FireEye platform to quarantine zero-day spear phishing emails, block related multi-protocol command and control communications, and identify the intended victims.

The FireEye Threat Protection Platform

The FireEye platform secures against spear phishing email attacks that bypass anti-spam and reputation-based technologies. To quarantine the spear phishing emails used in advanced targeted attacks, the FireEye platform analyzes every attachment using a signature-less, Multi-Vector Virtual Execution™ (MVX) engine that can quickly and accurately identify zero-day attacks. It goes beyond signature and reputation-based systems by detonating each attachment against a cross-matrix of operating systems and applications, including multiple Web browsers and plug-ins. Administrators can quarantine emails with malicious content for further analysis or deletion.

In the research that follows, Gartner provides insight into targeted email attacks and data loss prevention[2]. FireEye believes that our research and the history of how cyber attacks have become more and more advanced, makes it clear that legacy security solutions need to be supplemented with next-generation threat protection to effectively protect intellectual property, sensitive information, and the integrity of business operations.

Source: FireEye

[2]Gartner Research, Email Security Focus Shifts to Address the Risks of Targeted Attacks and Data Loss, Peter Firstbrook, August 29, 2012

Research from Gartner

Email Security Focus Shifts to Address the Risks of Targeted Attacks and Data Loss

Email is still the most commonly used channel for corporate communications. As a result, it has become a conduit of targeted attacks and a potential source of data loss.

Impacts

- The greater level of danger posed by targeted phishing email attacks is shifting the focus of advanced email security solutions within enterprises.
- The wide variety and quality of data loss prevention solutions and use cases require email administrators to plan carefully.
- Email administrators are increasingly required to provide email encryption to meet corporate and regulatory compliance standards.

Recommendations

- Larger organizations and those that are often targeted should look for products that provide techniques to detect highly targeted phishing. Ideally, solutions will include malicious attachment and Web redirection techniques, and provide advanced reporting and forensic information. Currently, however, no solutions do it all.
- Email administrators should make an effort to understand business requirements for DLP over the next three years, and evaluate vendors and solutions accordingly. Employing an isolated SEG DLP solution is acceptable for a number of use cases; however, when IP protection is the primary requirement, an enterprise DLP solution is preferred.
- Organizations not yet using email encryption should start collecting business requirements and plan deployments within the next 24 months. They should also consider encryption-critical criteria when selecting an SEG solution. Incumbent SEG vendors offer opportunities to simplify encryption deployments, but only if the encryption solution meets business requirements and is well-integrated.

Strategic Planning Assumption

Enterprise use of email encryption and email data loss prevention will grow from 30% in 2012 to more than 60% of enterprises by 2015 and, thus, become a standard of due care for protecting private information.

Analysis

Despite the growth in other communications channels, email remains the foundation of corporate communications. The prevailing use of email has made it a preferred conduit of targeted attacks and a significant, potential source of data loss or compliance issues.

Secure email gateways (SEGs) have become adept at defending against typical spam and virus attacks, at the same time that spam volumes are declining. While there is still work to do to improve spam detection accuracy and clean up irritating bulk email, administrators should be turning their attention to more difficult-to-detect inbound targeted attacks, which are on the rise.[1]

IT organizations are becoming increasingly aware of the business risk of careless data handling with each new regulation and data breach. Email is the easiest way to exchange files and data with colleagues and partners. Unrestricted email usage can result in careless storage and transmission of sensitive information. Data loss prevention (DLP) techniques are the primary mechanism to prevent the misuse of sensitive information; thus, it is emerging as a critical requirement of email security systems. However, eliminating all sensitive data from email is impractical for most organizations; therefore, email encryption is a necessary function.

The greater level of danger posed by targeted phishing email attacks is shifting the focus of advanced email security solutions within enterprises

Some of the leading SEG solutions (for example, Cisco, Symantec and Proofpoint are starting to focus on the very difficult problem of detecting targeted phishing messages, which are used to

FIGURE 1 Impacts and Top Recommendations for Email Security

Impacts	Top Recommendations
The danger posed by targeted attacks is shifting the focus of email security solutions.	• Targeted organizations should look for products that provide techniques to detect targeted phishing. • Ideally, solutions will include malicious attachment and Web redirection techniques.
The variety and quality of DLP solutions and use cases require email administrators to plan carefully.	• Understand business requirements for DLP over the next three years, and evaluate vendors and solutions according to needs.
The requirement to provide email encryption to meet compliance is increasing.	• Organizations not yet using email encryption should consider deployments within the next 24 months, and start collecting business requirements.

Gartner (August 2012)

initiate targeted attacks.[2] These attacks are also called "spear phishing." These messages are difficult to detect because they look like any other person-to-person emails. Targeted attacks typically use two methods to infect their target's endpoint: malicious attachments, which contain the initial exploit, or Web redirection, which lures the reader to a malicious website. In 2011, approximately 60% of malicious emails used attachments, while 40% used Web redirection.[3] These attacks are usually aimed only at high-value employees (such as C-level executives and privileged administrators), and often are researched using content from LinkedIn, Facebook and other public information to tailor the spear phish method.

Malicious Attachments

Most organizations already block or quarantine executable attachments,[4] so attackers now use document-type attachments that have high business use and are difficult to block by policy. Currently, the most common malicious attachment types[3] are PDF, zip/RAR, Office documents and RTF. These files typically exploit vulnerabilities in the reader application (that is, Adobe Reader or Word), exploit the powerful scripting capabilities within the reader, or are used as containers to camouflage the malicious executable files (that is, password-protected zip files).

Approaches to detecting advanced targeted attachment malware can be categorized in two buckets:

1 **Static code analysis:** Reading the file to detect and remove suspicious commands or code blocks. Most vendors do at least some level of static analysis, making it difficult to validate the marketing claims without testing.

2 **Dynamic code analyses:** Executing the code in a sandbox environment to detect malicious behavior. Examples of vendors include FireEye, Trend Micro and AhnLab.

To detect malicious code in containers such as zip and RAR files, gateways should be capable of unzipping files. Although attackers often make it difficult to automatically unpack files, desktop-to-desktop encryption utilities can also make unpacking impossible for email gateways. Organizations need to set policies for handling packed files that cannot be opened by the gateway. One approach is to deliver these messages to the recipient's inbox with an append to the subject line that includes a warning and, depending on the end user, caution and endpoint protection. Higher-security organizations should quarantine the file for inspection by an administrator on an isolated machine; however, this increases the administration effort and requires experienced security operators.

Web Redirection

Most SEG solutions detect URLs in email and perform checks against a list of known bad URLs in an onboard database, or perform a real-time look-up with a cloud database. Some solutions (such as Cisco or Trend Micro) also use a "reputation" score to detect URLs that are not currently malicious, but are suspected to become malicious in the future. The weakness in these approaches is the dynamic nature of the current threat. The URL can point to "good" content at the time of delivery, but change postdelivery to the recipient's inbox.

More-advanced solutions (such as Cisco and Proofpoint) are starting to rewrite suspect URLs with a custom URL that points to the SEG provider. At the time when the URL is clicked, the SEG solution will perform a final inspection of the website to detect malicious activity, and, if none is found, provide the client with a URL redirect to the original site. It is important to make a distinction between solutions that simply check the database one more time and those that actually check the website for new signs of malicious activity. Some solutions (such as Cisco) will remain in-path and inspect the Web content as it is delivered to the end user using their cloud-based secure Web gateways to detect malware in transit to the client. Generic SWGs can also protect users from malicious websites, regardless of how the user is redirected to the website, and are an important component of a layered approach. However, SWGs typically do not correlate the Web click with a particular email, nor are they often under the management of the same team as the email gateway.

We expect to see leading SEG solutions provide more reporting and forensic information about targeted phishing attacks for security incident response teams.

Recommendation:

- Larger organizations and those that are often targeted should look for products that provide techniques to detect highly targeted phishing. Ideally, solutions will include malicious attachment and Web redirection techniques, and provide advanced reporting and forensic information. Currently, however, no solutions do it all.

The wide variety and quality of data loss prevention solutions and use cases require email administrators to plan carefully

In our 2012 reference customer survey,[5] 75% of respondents said that DLP was an important or very important critical capability of an SEG, 31% were actively using DLP capabilities, and another 35% had plans for DLP in the next 24 months.

Email DLP is critical for:

1 Regulatory and industry compliance

2 Keeping users from storing intellectual property (IP) or regulated data in the email system

3 Acceptable usage monitoring

4 Enabling automatic encryption of sensitive data

5 Protecting IP from accidental loss

Although it is not optimal, the SEG DLP capability can be implemented independently of enterprise DLP for the four use cases listed above. For IP protection, however, buyers of SEG DLP must understand how it will fit into an enterprise data management strategy. No SEG DLP solutions integrate easily with an enterprise DLP solution from other vendors. However, some allow for integration with the vendor's enterprise DLP.

Most SEG solutions are poor at managing the workflow for compliance officers, allowing policy objects to be reused and allowing for extensible notification emails that include dynamic information, such as the type of violation or event or the actual offending text.

Recommendation:

- Email administrators should make an effort to understand business requirements for DLP over the next three years, and evaluate vendors and solutions accordingly. Employing an isolated SEG DLP solution is acceptable for a number of use cases; however, when IP protection is the primary requirement, an enterprise DLP solution is preferred.

Email administrators are increasingly required to provide email encryption to meet corporate and regulatory compliance standards

In our 2012 reference customer survey,[5] 65% of respondents said that advanced encryption was an important or very important critical capability of an SEG, 34% already used encryption, and 32% had plans for email encryption in the next 24 months.

Email systems are not designed as secure repositories of critical information, and organizations should strive to keep sensitive information out of email storage; however, the utility of email to business means that sensitive information will find its way in regardless of policy. The deployment of DLP systems will usually result in the immediate deployment of encryption. Very few organizations will find no sensitive information in emails once they start looking, and it is rarely an option to simply reject these emails.

The encryption requirements for business-to-business and business-to-consumer (B2C) will differ, however. Most encryption vendors offer solutions that work with both use cases, and it should be a design goal to acquire a single solution for both use cases.

The majority of SEG solutions provide encryption via a partner (such as ZixCorp, Voltage Security or Echoworx). These dedicated email encryption partners often provide very extensive and mature encryption capabilities; however, access to the full management capabilities of the encryption solution is often lacking. As a result, setup monitoring and changes often require calls to vendor support rather than self-service. Native solutions that are integrated with the management console by the SEG vendor are preferred due to lower administration complexity, integrated email tracing, lower cost and simpler routing. However, these solutions may not be as robust as the dedicated partnership solution. We recommend that encryption buyers consider their incumbent SEG provider as a leading shortlist candidate, but acknowledge that buying directly from dedicated vendors may be a better choice for advanced needs.

Critical considerations for encryption include content versus transport encryption, the need for recipient clients, certificate management and integration with existing directories, and the experience for the recipient and sender using mobile devices.

IT organizations and email administrators should also recognize potential operational problems with email encryption and educate the business on steps to mitigate the impact of these issues. Email encryption sometimes requires endpoints to have a specific type of client reader or browser. Any time a new client component is required, it increases recipients' level of frustration and the amount of support required. This is especially true for B2C requirements. Encrypted emails often look "phishy" to recipients and, as a result, are not opened. Whenever implementing a new email encryption solution or changing an existing solution, send notifications and prepare post education/instructional resources for recipients ahead of the changes. Also prepare help desk resources to resolve issues arising from encryption. Advertise and maintain a consistent look and feel of encrypted messages so that recipients understand what they are. Encrypted email can also end up in spam quarantines. Avoid marketing messages within encrypted messages, because these may trigger spam filtering.

Recipients generally are not inclined to take multiple steps to read encrypted email unless it is something they are really interested in. Avoid multistep processes and use encryption only when the added inconvenience to the recipient is justified. Encrypted email that creates yet another password for recipients to remember will require self-service password reset mechanisms. For most use cases, passwords should not be required, because authentication to the email inbox may be sufficient identification. Where passwords are required, they should ideally be synchronized with other usernames and password systems, such as a website authentication directory, and set up self-service password recovery schemes.

Recommendation:

- Organizations not yet using email encryption should start collecting business requirements and plan deployments within the next 24 months. They should also consider encryption-critical criteria when selecting an SEG solution. Incumbent SEG vendors offer opportunities to simplify encryption deployments, but only if the encryption solution meets business requirements and is well-integrated. Do not ignore the potential operational challenges and recipient experience associated with encrypted email, and prepare to mitigate these.

Evidence

[1]From the June 2012 Symantec Intelligence Report. During the first half of the year, the total number of daily targeted attacks continued to increase at a minimum rate of 24%.

[2]Verizon's "2012 Data Breach Investigations Report" found that email was used in 17% of social engineering attacks, but "quite a bit higher, however, when examining breaches affecting larger organizations."

[3]"Internet Security Threat Report, Volume 17"

[4]Microsoft TechNet advice regarding attachment types to block.

[5]In May 2012, Gartner conducted an online survey of 111 vendor-supplied "reference" customers.

Gartner RAS Core Research Note G00215466,
John Pescatore 5 August 2011

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,000 customers across more than 40 countries, including over one-third of the Fortune 100.

For more information, visit: www.FireEye.com.

[4]Gartner Research "Email Security Focus Shifts to Address the Risks of Targeted Attacks and Data Loss", Peter Firstbrook, August 29, 2012