A Look at the Situation

There appears to be no end in sight to the reign of phishing as the cyber attackers’ number one threat delivery and communications vehicle. Whether it’s a script kiddie just goofing around, a member of one of the world’s most sophisticated nation-state-based attacker groups trying to impact global politics, or a cybercriminal focused on turning digital information into digital cash, they all use email in their attack repertoire.

Why is this? What other digital medium is used by almost everyone on the planet to conduct all types of real-time business and can carry any type of content, hyperlinks or attachments? To top it off, it’s anonymous, has a marginal cost of use of zero and was not built from the ground-up to be secure. If one were inventing a cyberattack delivery tool from the ground up, it would look a lot like today’s email!

Clearly the situation is bad, but all is not lost. By following the advice in the following Gartner research note, organizations can proactively defend themselves against phishing attacks. But as any regular student of security would expect, there is no silver bullet technical defense that will get the job done. Organizations need to understand the importance of an anti-phishing program which includes technical, procedural, and educational controls and emphasizes prevention, but they must remain realistic enough to know that no prevention is perfect. Thus, effective detection and response is an essential part of the program.

Attackers as a collective are smart. When you set up an anti-virus-based network defense against malicious attachments they use techniques to get around them. And when you parry with sandboxing of attachments they switch to using malicious URLs in their emails. And when you clog up that attack technique they move on to malware-less impersonation attacks or use ripped-off user credentials to expand their attacks from the inside. Ideally, your anti-phishing technical controls should combine all of these techniques and more. It is hard to keep up, but if you follow the advice in this research note you will be well on your way to success.

Source: Mimecast
Effective mitigation of inbound phishing attacks requires that CISOs take a multipronged approach that spans technical, procedural and educational controls.

**Key Challenges**

- Phishing is the most common targeted method of cyberattacks, and even typical, consumer-level phishing attacks can have a significant impact on security.

- Increasing volume and sophistication of phishing attacks are resulting in real financial damage to organizations in both downtime (such as “ransomware” attacks) and direct financial fraud (such as wire transfers).

- Phishing content does not always include a malicious payload, making phishing emails increasingly difficult to detect.

- Phishing attacks against employees have expanded beyond email to include social media, instant messaging, SMS and voice communications.

**Recommendations**

- Upgrade to the latest version of your secure email gateway (SEG), and request a policy audit from the SEG vendor to ensure that the most effective security controls are enabled and correctly tuned.

- Deploy URL filtering (that uses URL proxying and time-of-click analysis), attachment sandboxing, and content disarm and reconstruction (CDR). Ask incumbent SEG providers to improve notification to end users of suspect emails that cannot be blocked or quarantined.
Ensure proper desktop and Web gateway security is in place to avoid infections from malicious attachments and URLs.

Enforce higher-trust authentication for, at a minimum, all system administrators, users that handle sensitive information and users with remote access to corporate resources.

Implement real-time anti-phishing training, and expand the program to cover social engineering via multiple communication channels, not just email.

Strengthen internal process controls on financial transactions and other procedures that mitigate the risk of misguided employee actions motivated by phishing content.

Strategic Planning Assumption

Through 2020, email will remain the primary targeting method of advanced targeted attacks, and a common distribution method for consumer attacks.

Introduction

This research discusses the full scope of the inbound phishing threat, and identifies effective mitigation strategies. Chief information security officers (CISOs) should leverage this information to negotiate, design and maintain an anti-phishing program that effectively mitigates the risks of phishing of employees. See “Fighting Phishing: Protect Your Brand” for best practices to protect the corporate brand from being abused by phishing attacks on external recipients such as customers and partners.

Phishing is a widespread, high-impact threat that relies on social engineering to enable illicit access to personal and corporate assets. Currently, an average of roughly one out of every 4,500 emails is a phishing attack. The rate of phishing emails is highly variable, depending on the attack campaigns, but the trend line for the rate of phishing emails is increasing (see the Appendix). Although a broad spectrum of products and services have emerged to enable more effective detection and prevention of damage from phishing, many enterprises are unaware of the full scope of the phishing threat, and many more are struggling to implement effective defenses. CISOs should develop a comprehensive program of phishing prevention and detection to protect internal infrastructure, financial transactions and sensitive data.

At one time or another, each of us has received phishing email. Although the exploit mechanism contained within the email might vary, the basic intent is consistent: the message attempts to persuade the recipient to take an apparently benign action that will actually result in a security compromise. Many high-profile breaches have started with successful phishing attacks (see Note 1), and most organizations experience a continuing flow of phishing attempts specifically targeting the company and its employees, also known as “spear phishing.” In response, many organizations have deployed secure email gateways (SEGs), secure Web gateways (SWGs) and anti-phishing behavior management (APBM) simulation training. Most SWGs do not protect users when they are roaming or using unmanaged devices, and not all SEGs have the latest improvements in anti-phishing technology. Additionally, very few SEGs are able
to identify and block phishing messages that do not contain URLs or a malicious payload. This is particularly important given the recent increase in phishing emails that merely prompt the recipient to wire funds voluntarily to an external bank account, or take action in some other way that damages the enterprise.

A comprehensive and effective anti-phishing program should include the technical, procedural and educational controls explored in this document.

Analysis

Use Advanced Threat Defense at the Email Gateway

Better protection from targeted phishing attacks remains the most critical inbound protection capability of an SEG. Indeed, 96% of respondents to a Gartner survey indicated that this was an important or very important capability of their SEG.

In response, more SEG vendors are incorporating targeted phishing detection methods. The two most popular methods include time-of-click URL filtering and attachment sandboxing.

Currently, the best approach to mitigating the threat of malicious URLs in email is by using proxy and time-of-click analysis-filtering techniques. These are more effective at detecting fast-fluxing, link-based malware and phishing attacks because they double-check links at the time of click, rather than at the time of delivery. Click-through rates on phishing emails range significantly, but it is not unusual to see rates of 30% to 65%. So, stopping them from reaching the inbox or being able to neuter malicious URLs after they’ve crossed the threshold of the gateway and landed in the inbox are key components of this defense.

Sandboxing is a technique that executes suspicious files in simulated PC environments to detect malicious behavior and provide forensic information. Sandboxing is much more effective than traditional signature analysis, but it can be slow (that is, delays of up to 10 minutes or more), and malware authors are starting to build evasive techniques to elude sandbox detection.

Sample Vendors for URL and Sandboxing Protection

Cisco; Microsoft; Mimecast; Proofpoint; Symantec

Most organizations block executable attachments in email, but they cannot block files such as Microsoft Office documents or PDFs. Phishing attacks exploit this policy loophole by embedding active code like macros and JavaScript in these files or, more often, by using techniques to exploit vulnerabilities in the reader software itself. As malware sandbox evasion techniques improve, the use of content disarm and reconstruction (CDR) at the email gateway as a supplement or alternative to sandboxing will increase. CDR breaks down files into their discrete components, strips away anything that doesn’t conform to that file type’s original specification, International Organization for Standardization (ISO) standard or company policy, and rebuilds a “clean” version that continues on to the intended destination. This real-time process removes zero-day malware and exploits without impacting business productivity typically caused by sandbox detonation and quarantine delays.

Sample Vendors for Content Disarm and Reconstruction

Check Point; Glasswall Solutions; Mimecast; Opswat; ReSec; Sasa Software; Solebit; Symantec; Tresys Technology; Votiro
However, the use of CDR can decrease document usability by stripping out active code intended for legitimate purposes. A best-practice policy will develop around a combined approach that uses CDR on files for fast delivery, while simultaneously sandboxing them to determine which should be made available to the end user. It should also be noted that timely patching of Microsoft Office and Adobe programs will thwart 30% to 80% of document malware.

Targeted phishing attacks that do not include a payload (that is, a URL or attachment) are more difficult to detect. These attacks typically use spoofed email addresses and social engineering to trick users. Recent attacks have been very sophisticated, even including previous email chains to convince victims that the request is part of a previous correspondence. Using Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting and Conformance (DMARC) are useful to detect exact-domain-spoofed messages. However, these standards can be hard to adopt for large organizations, and do not cover spoofed messages that leverage near-match domain name misspellings.

SEG content inspection for keywords commonly associated with phishing attacks – keywords such as “wire,” “transfer,” “bank account,” “password” and “username” – will become more successful in detecting these types of attacks, especially when combined with IP and domain reputation. Over the long term, the concept of sender trust will work its way into the market and provide email recipients with a visual indicator of the trustability of email senders. Vendors such as Cloudmark, Microsoft, Mimecast, Proofpoint and Vade Retro have early versions of products that will notify recipients based on near-match domain name misspellings, common keywords or other suspicious indicators of phishing.

Attackers often lurk on targeted employees’ PCs and in email accounts, monitoring usage until they detect a tempting email involving financial transactions. Security operations groups that detect phishing messages that closely mimic legitimate email communications, or those that seem to have an inside view of corporate structure, should investigate for the presence of malware and for unauthorized access to Web mail accounts.

Recommendations

- Upgrade to the latest version of your SEG, and request a policy audit from the SEG vendor to ensure that the most effective security controls are enabled and correctly tuned.

- Deploy URL filtering (that uses URL proxying and time-of-click analysis), attachment sandboxing and CDR. Ask incumbent SEG providers to improve notification to end users of suspect emails that cannot be blocked or quarantined.

- Implement mail transfer agent (MTA) rules to detect spoofing of internal addresses, and add a notification banner to email from external senders to make the source of messages clearer to users.

- Ensure proper desktop and Web gateway security is in place to avoid infections from malicious attachments and URLs.
Don’t Rely on Passwords Alone for Authentication

Phishing attacks frequently target users with access to sensitive data, and attempt to capture passwords in order to impersonate corporate officers. Passwords should not be considered sufficient for anything other than the lowest-risk applications.

Requiring higher-trust authentication methods (such as one-time password [OTP] tokens, cryptographic credentials or biometric traits) can reduce the risk of impersonation or otherwise thwart attacks against passwords. It should be implemented, at a minimum, for the following users that are considered rich targets for attack:

- System administrators and other privileged account users.
- Users that handle sensitive information, such as those working in corporate finance and human resources.
- Users with remote access to corporate resources – this includes Web mail, such as Outlook Web Access (OWA), especially for senior management.

See “How to Choose New User Authentication Methods” for guidance on how to choose user authentication methods that best provide the necessary balance among trust (authentication strength and accountability), total cost of ownership and user experience for each use case.

Recommendation

- Enforce higher-trust authentication for, at a minimum, all system administrators, users that handle sensitive information and users with remote access to corporate resources.

Use Anti-Phishing Behavior Management

Anti-phishing products that focus on behavior management of employees are part of a security awareness and communications program; a critical element of a people-centric security strategy. APBM products improve employee retention of key security messages and behaviors, and measure the impact of the product on the security performance of employees.

APBM products simulate phishing attacks, and provide computer-based remediation training for employees that exhibit inappropriate behavior in response to simulated attacks. These products focus on both educating employees and correcting behavior when the employee responds to a phishing message by clicking on a URL, opening an attachment or performing some other action. Organizations use APBM products to improve the resilience of their employees to the social engineering techniques commonly found in phishing messages. While a list of representative vendors is included below, see “Innovation Insight for Anti-Phishing Behavior Management” for more detailed information on these products.

Sample Vendors for Anti-Phishing Behavior Management

KnowBe4; PhishLine; PhishMe; SANS Institute; Terranova; Wombat Security Technologies
Today, APBM products are mostly delivered by dedicated security or phishing education services. We anticipate, however, that some of the aforementioned SEG vendors will add APBM as a component of their products. Since an SEG is already intercepting the real-world phishing attacks being made on an organization, it can neuter these and leverage them as part of an APBM campaign. This can avoid the common complaint that the simulated phishing emails used in APBM are not “real world.” SEG vendors are also creating reporting that is specific to targeted attacks to provide forensic information about attacks and users’ behavior. These reports are valuable for incident response as well as employee education.

Although phishing attacks primarily target email, the attack method is not restricted to this communication medium. Despite this reality, most enterprises focus employee training and automated security controls solely on email traffic. Significant residual risks are found in phishing attacks transported via social media, instant messaging, SMS (“smishing”) and phone calls (“vishing”).

Most automated detection and prevention approaches for phishing focus on email, forcing CISOs to prioritize training as primary risk mitigation for phishing attacks outside of email. Training products that provide attack simulation for non-email phishing are available, but only sparsely adopted. As social engineering attacks spread to other messaging platforms, technological and behavioral control providers will expand their capabilities to improve attack resilience. For now, the sample training vendors that provide behavior management support for non-email phishing attacks include the vendors listed below.

Sample Vendors for Non-email Phishing Mitigation

KnowBe4; Lucy Phishing; PhishLine; PhishX; Wombat Security Technologies

Recommendation

- Implement real-time anti-phishing training, and expand the program to cover social engineering via multiple communication channels, not just email.

Strengthen Internal Process Controls

Although the majority of phishing attacks rely on the recipient clicking on a URL or opening an attachment, a growing number of attacks seek to motivate the recipient to take an action outside of the context of the phishing message itself. For example, a popular spear phishing attack involves a message purporting to be from a traveling CEO directed to the CFO (or equivalent) requesting an expedited wire transfer to a specified offshore account. The email is sent when the CEO is otherwise out of reach, having left the office on personal leave or company business. In multiple instances, funds have been transferred purely on the basis of an artfully crafted spear phishing attack. Variations of this attack include requests for personal information of employees. This attack style is also prevalent in voice-based phishing (“vishing”) wherein the attacker speaks directly with the target and attempts to convince them to take an inappropriate action.

Training can be used to improve the ability of employees to detect social engineering attacks. However, this training is most effective when supported by an optimized alert and escalation process that enables employees to escalate a suspected attack and
receive a rapid response. They should not just delete suspect emails, but should direct them to the security team. A rapid response can enable the computer security incident response team (CSIRT) to gather evidence on attackers, and to extract malicious object IP information, which can be disseminated to other security control points.

In addition, internal processes that are likely targets for phishing attacks (such as funds transfers, changes in bank information, new account creation or transfers) should be improved with standard operating procedures designed to limit the success of phishing attacks. Some examples of procedures include requiring dual-authorization of defined actions and out-of-band verification of the action request (that is, email requests should be confirmed by phone or vice versa).

**Recommendation**

- Strengthen internal process controls on financial transactions and other procedures that mitigate the risk of misguided employee actions motivated by phishing content.

---

**Appendix**

**Figure 1. Mimecast Review of Customer Traffic Patterns Across U.S.- and U.K.-Based Traffic From 23 October 2015 Through 26 February 2016**

![Incidence of Phishing per Weekday as a % of Accepted Mail](image)

*The number of accepted messages falls at weekends although rejections typically remain fairly constant, hence weekends are omitted from the chart to avoid misleading spikes. Over period shown (including weekends), the total incidence of phishing equates to 1 phishing mail per 4,586 accepted mails. For weekdays only, the equivalent number is 1 phishing mail per 5,233 accepted mails.*

*Source: Mimecast*
Evidence

1 Gartner conducted an online survey of 120 vendor-supplied reference customers in May and June of 2015. Forty-two percent of respondents had more than 5,000 seats, and only 14% had fewer than 1,000 seats. Forty-six percent of respondents were self-identified as being “responsible for daily operation, policy configuration and incident response.”


3 Notification texts, such as “From External Domain” or “Notice: This email was sent from a person outside of (Company Name),” can be appended to the subject or body of incoming emails from external domains. This can be applied to incoming emails for all employees or more narrowly focused on emails sent to a subset of employees, such as those with the authority to approve or initiate outbound wire transfers. “Organization-Wide Disclaimers, Signatures, Footers, or Headers” from Exchange Online shows how this can be configured through Microsoft Exchange Online Protection. Alternative approaches exist based on email server or provider. For example, in Exchange Online and Exchange Server 2013 and 2010, organizations can set an External Recipients MailTip to notify senders when an external recipient is present in the recipient field.
of a message. Before implementation, new MTA rules should be tested for potential impact to other business processes, which may depend upon specific message content or formatting.

4 This type of spear phishing attack is also referred to as “CEO fraud” or a business email compromise (BEC) scam. According to a Business Email Compromise public service announcement from the Federal Bureau of Investigation’s Internet Crime Complaint Center (IC3), more than 7,000 U.S. companies have been victimized by BEC scams between October 2013 and August 2015, with total dollar losses exceeding $740 million. This figure doesn’t include victims outside the U.S. and unreported losses.

5 “IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s.” IRS. March 2016.

Note 1

High-Profile Data Breaches and Cyberattacks That Started With Phishing


8. TV5Monde: “Phishing Email’ the Key to Hacking of TV5Monde.” The Local Europe. April 2015.

9. 2015 Verizon Data Breach Investigations Report (DBIR): “In the 2013 DBIR, phishing was associated with over 95% of incidents attributed to state sponsored actors, and for two years running, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing.

Source: Gartner Research, G00300446, Neil Wynne, Andrew Walls, Peter Firstbrook, 17 March 2016
How to Take Action

Now that you have the key elements of an anti-phishing program, where do you start? On the technology front, make sure you have the absolute best secure email gateway (SEG) in place that you can get. With the advent of malware-less impersonation attacks, internally generated email threats, or hyper targeting of attacks, yesterday’s SEGs won’t cut it today. For the vast majority of organizations this also means using a SEG service in the cloud. Why in the cloud? There is no better, more efficient way to inspect your inbound, outbound, and internal emails for threats and potential data leakage than in the cloud. Going it alone with on-premises-based SEGs means you’ll miss out on the network effects and the economies-of-scale and scope that are inherent with a shared cloud security service that pivots in real-time against the latest threats.

On the educational front, build anti-phishing awareness and regular testing into your employee education program. Don’t just make it a yearly, click-through video-watching chore for your staff. Make it a seamless part of their day.

And finally, review and focus on your most critical business processes – as these are likely the most financially attractive to the attackers – to make sure you have no single point, or person, of failure. Taken together, these steps can move you well on your way to standing in the way of the cyber attackers and their abuse of your most mission critical communications application.

Source: Mimecast
About Us

Mimecast makes business email and data safer for more than 26,400 customers and their millions of employees worldwide. Founded in 2003, the company’s next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management in a single, fully-integrated subscription service.

Mimecast reduces email risk and the complexity and cost of managing the array of point solutions traditionally used to protect email and its data.

For customers that have migrated to cloud services like Microsoft Office 365™, Mimecast mitigates single vendor exposure by strengthening security coverage, combating downtime and improving archiving.

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging attacks, while preventing data leaks. Mimecast Mailbox Continuity enables employees to continue using email during planned and unplanned outages.

Mimecast Enterprise Information Archiving unifies email, file and instant messaging data to support e-discovery and give employees fast access to their personal archive via PC, Mac and mobile apps.

Contact us

www.mimecast.com

For more information call:
Europe: +44 (0)20 7847 8700
North America: +1 617 393 7050
South Africa: +27 (0) 105 009 950
Australia: +61 3 9017 5101