ATYXIT

Phone: (847) 796-3177
Website: https://atyxit.com

Best Practices for Dealing with Phishing and Ransomware

Original Report Composed by: Osterman Research

WHITE PAPER

Best Practices for Dealing With Phishing and Ransomware

An Osterman Research White Paper

Published September 2016

Sponsored by

Trustwave®
Smart security on demand

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Phishing and ransomware are serious problems that can steal or disable access to corporate or personal finances, sensitive employee data, patient data, intellectual property, employee files and other valuable content. Both ransomware and phishing attacks and their variants – spearphishing/whaling and CEO Fraud/Business Email Compromise (BEC) – are increasingly common and are having devastating impacts on businesses of all sizes. The financial impact of cybercrime in general – and phishing and ransomware in particular – is hard to assess for a variety of reasons, but the FBI estimates that ransomware alone cost organizations $209 million in just the first three months of 2016[i].

Phishing, which can be considered the delivery mechanism of choice for various types of malware and cybercrime attempts; and ransomware, which is a specialized form of malware that is designed for the sole purpose of extorting money from victims, are critical problems that every organization must address and through a variety of means: user education, security solutions, vulnerability analysis, threat intelligence, good backup processes, and even common sense. The good news is that there is much that organizations can do to protect themselves, their data, their employees and their customers.

KEY TAKEAWAYS

- Both phishing and crypto[ii] ransomware are increasing at the rate of several hundred percent per quarter, a trend that Osterman Research believes will continue for at least the next 18 to 24 months.

- The vast majority of organizations have been victimized by phishing, ransomware and a variety of security-related attacks during the past 12 months. In fact, phishing and ransomware are among the four leading concerns expressed by security-focused decision makers as discovered by Osterman Research in the survey conducted for this white paper.

- Security spending will increase significantly in 2017 as organizations realize they need to protect against phishing, ransomware and the growing variety of other threats they face.

- Most organizations are not seeing improvements in the security solutions they have deployed and in the security practices they follow. While many of these solutions are effective, most are not improving over time, in many cases because internal staff may not have the expertise to improve the performance of these solutions over time. On balance, only two in five of these solutions and practices are considered "excellent".

- Security awareness training is a key area for improvement in protecting organizations against phishing and ransomware, since our research found that organizations with well-trained employees are less likely to be infected.

- There are a variety of best practices that organizations should follow in order to minimize their potential for becoming victims of phishing and ransomware. Among these best practices are implementing security awareness training, deploying systems that can detect and eliminate phishing and ransomware attempts, searching for and remediating security vulnerabilities in corporate systems, maintaining good backups, and using good threat intelligence.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Trustwave – information on the company is provided at the end of this paper.

Both phishing and crypto ransomware are increasing at the rate of several hundred percent per quarter, a trend that Osterman Research believes will continue for at least the next 18 to 24 months.

KEY SECURITY CONCERNS

JUST HOW BAD IS THE PROBLEM?

Phishing, ransomware and other threats are getting significantly worse over time. For example:

- The Anti-Phishing Working Group (APWG) observed a 250% increase in the number of phishing Web sites between the fourth quarter of 2015 and the first quarter of 2016[iii].
- McAfee Labs discovered nearly 1.2 million ransomware attacks during the first quarter of 2016, a 24 percent increase compared to the fourth quarter of 2015[iv].
- A Kaspersky study during 2014 and 2015 found that total ransomware attacks during the period of the analysis increased by 17.7 percent, but that cryptoware variants had increased by 448 percent during that period[v].
- A US government interagency document published by the US Department of Justice in 2016 reported that in excess of 4,000 ransomware attacks have occurred each day since the first of the year, a 300 percent increase compared to 2015[vi].
- Attackers receive an estimated 1,425 percent return on investment for exploit kit and ransomware schemes ($84,100 net revenue for each $5,900 investment), according to the 2015 Trustwave Global Security Report.

Phishing, particularly highly targeted forms of phishing like spearphishing and CEO Fraud/BEC, as well as ransomware, are the logical evolution of cybercrime. Because there have been so many data breaches over the past few years that have resulted in the theft of hundreds of millions of records, there is a glut of this information on the market. The result, as there would be in any other business driven by the economics of supply and demand, is that prices for stolen records are dropping precipitously: a leading security firm estimates that the price of a stolen payment-card record has decreased from $25 in 2011 to just $6 in 2016.

Consequently, cybercriminals are turning increasingly to more direct means of theft. For example, ransomware will extort money directly from victims without requiring stolen data to be sold on the open market where it is subject to economic forces that can reduce its value. CEO Fraud/BEC can net hundreds of thousands or millions of dollars in a short period of time by getting victims to wire funds directly.

Phishing, particularly highly targeted forms of phishing like spearphishing and CEO Fraud/BEC, as well as ransomware, are the logical evolution of cybercrime.

SECURITY INCIDENTS DURING THE PAST 12 MONTHS

The research conducted for this white paper found that a wide range of security incidents have occurred during the past 12 months among the organizations that were surveyed. The most common incidents involved phishing attacks that were successful in infiltrating the corporate network, successful ransomware attacks, and malware infiltration through some unknown source, as shown in Figure 1. However, a wide range of other security incidents have occurred – in fact, only 27 percent of the organizations surveyed reported that they did not experience any of the security problems shown in the figure below.

Moreover, our research found that security incidents are generally not one-off events, but occur with some frequency:

- Fifty-one percent of the organizations surveyed have experienced between one and five ransomware infections, hacker infiltrations, malware infections, etc. because an employee clicked on a phishing link or attachment. Another 13 percent have experienced six to 10 such attacks, and 11 percent have experienced more than 10 attacks.

- While CEO Fraud/BEC attacks are less common than phishing or ransomware, 27 percent of organizations have encountered such an attack during the past 12 months: 24 percent of organizations have experienced up to five such attacks during the past year, while two percent have experienced between six and 10 attacks, and an equal number have experienced more than 10.

Figure 1
Security Incidents That Have Occurred During the Past 12 Months

Problem	% of Organizations Affected
An email phishing attack was successful in infiltrating our network	34%
One or more of our endpoints had files encrypted because of a successful ransomware attack	30%
Malware has infiltrated our network, but we are uncertain through which channel	29%
Sensitive/confidential info was accidentally or maliciously leaked through email	17%
An email spearphishing attack was successful in infecting one or more senior executives	14%
Our network was successfully infiltrated through a drive-by attack from employee Web surfing	12%
An email as part of a CEO Fraud/Business Email Compromise attack successfully tricked someone in our organization	11%
Sensitive/confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	5%
Sensitive/confidential info was accidentally or maliciously leaked through a social media application	3%
Sensitive/confidential info was accidentally or maliciously leaked, but how it happened is not certain	1%
None of these things happened	27%

Source: Osterman Research, Inc.

PHISHING, RANSOMWARE AND CEO FRAUD/BEC EXAMPLES

Here are a few examples of phishing, ransomware and related types of attacks that have occurred in the recent past:

- As of August 2016, Bournemouth University has been infected with ransomware 21 times during the previous 12 months, for an average of one infection every 17 days[vii].

- Leoni AG, a large German manufacturer of optical fiber, wire and related products revealed in August 2016 that it had been the victim of a CEO Fraud/BEC attack. The cybercriminals responsible for the $44 million theft had apparently studied the company's payment processes – possibly the result of earlier phishing attacks that had allowed them to infiltrate the corporate network – and so were able to convince the CFO at the company's Bistrita, Romania factory that a spoofed email she received requesting the funds transfer was actually from one of the company's senior executives in Germany[viii].

- In April 2016, MedStar Health, a network of 10 hospitals in Maryland, was infected by the SamSam (Samas) ransomware variant, taking down its systems. One source identified a vulnerability in a JBoss Web application server as the method that cybercriminals used to wage its successful attack[ix].

- In February 2016, the payroll department at Snapchat was the victim of a phishing attack that resulted in the company divulging sensitive information to an unauthorized party. This information included the victims' names, Social Security numbers, 2015 wages earned, states of residence, states of work, employees' contributions to their retirement accounts, and taxes withheld, among other sensitive data[x].

- Also in February 2016, Hollywood Presbyterian Medical Center fell victim to the Locky ransomware variant, which disrupted operations for roughly two weeks before the hospital administration paid 40 Bitcoin (about $17,000) to recover its files[xi].

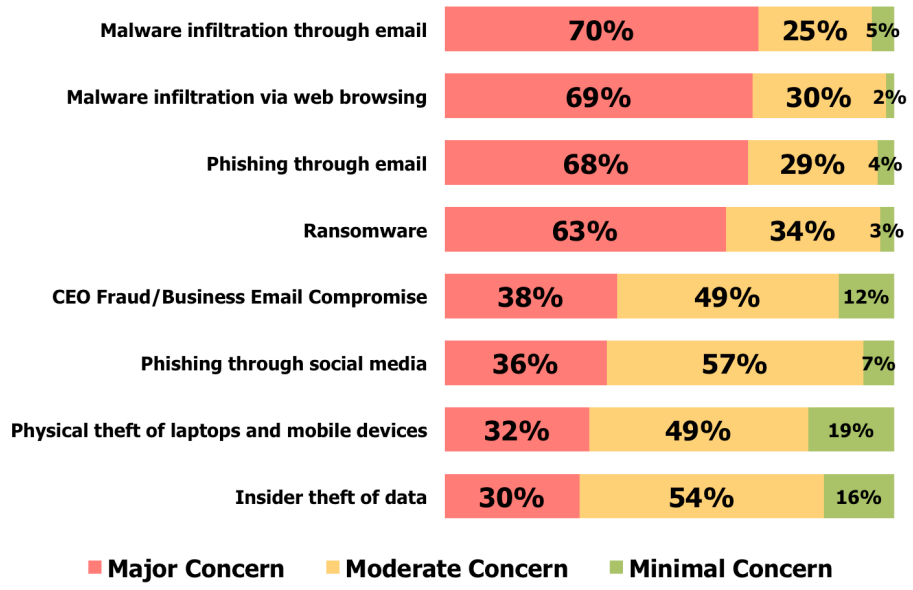
- In June 2015, employees of Ubiquiti Networks were victims of multiple CEO Fraud/BEC attacks that resulted in the company transferring $46.7 million to cybercriminals. These spearphishing attacks, directed at individuals within Ubiquiti's finance department, used simple email address spoofing[xii].

ISSUES THAT CONCERN DECISION MAKERS MOST

The CIOs, IT managers, IT directors, CISOs and other security decision makers we surveyed are concerned about a wide range of security-related issues. However, as shown in Figure 2, they are most concerned about malware infiltration through email and Web browsing, email phishing, and ransomware. Other issues of concern include CEO Fraud/BEC, social media phishing and more traditional avenues for data loss, such as physical theft of devices and malicious employee activities.

Email (through links and attachments in email messages) is the primary threat vector for many attacks and many users are suffering from "information overload" in email.

Figure 2
Issues With Which IT and Security Decision Makers are Concerned



Note: Totals may not equal 100% due to rounding error.
Source: Osterman Research, Inc.

WHY ARE PHISHING AND RANSOMWARE SO SUCCESSFUL?

The success of phishing and ransomware attempts is dependent upon a number of factors: the victim's gullibility or lack of skepticism when receiving emails and other opportunities to be fooled by cybercriminals, the amount and quality of training they have received, the quality of their organization's security infrastructure, and the level of threat intelligence they can bring to bear on potential attacks, among other

factors. However, there are several important reasons that phishing and ransomware are so successful today:

- Email (through links and attachments in email messages) is the primary threat vector for many attacks and many users are suffering from "information overload" in email, making them less likely to carefully scrutinize phishing, CEO Fraud/BEC and related attempts. A July 2016 Osterman Research survey of end users[xiii] found that 94 percent of users are experiencing some level of information overload via email – 32 percent report suffering "substantial" overload.

- Cybercriminals are simply getting better at creating content that can fool users and bypass detection technologies. The use of logos, professionally crafted messages, and personalization of content make phishing attempts more believable, and so potential victims are more likely to click on the links and attachments contained within them. One of the primary reasons that cybercriminals are getting better is that they tend to be very well funded, criminal enterprises – in short, they have the financial and technical resources to improve their wares.

- Cybercriminals are developing new and better variants of ransomware, as well as improved methods for communication to infected systems. Moving from the more basic, locker-type ransomware that was the norm a few years ago, more sophisticated, crypto-based variants have emerged, such as CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas (2016), Locky (2016) and Zepto (2016). Moreover, ransomware-as-a-service is becoming more common – the Cerber service, for example, had infected 150,000 endpoints as of July 2016 and is pulling in profits of nearly $200,000 per month[xiv].

- Many users share too much information through social media, which provides cybercriminals with information they can use to create personalized and more believable/harder-to-detect email messages.

- Some anti-phishing and anti-ransomware solutions are not backed up with a sufficiently robust database of real-time messaging intelligence, and so can fail to detect the latest techniques used by phishers and ransomware authors.

- Many users receive inadequate training about phishing and ransomware, as well as best practices in dealing with unknown threats. Related to this is the fact that many users simply are not sufficiently skeptical when it comes to receiving requests to do things like transfer funds, open attachments or provide sensitive information.

- Exploit kits, such as those that are used to infect victims with ransomware, can be used by cyber criminals that possess only a minimal skill set. These kits, which exploit vulnerabilities in a wide range of commercially available software, include various options, such as using the cyber criminals' own malware or using distribution channels offered by the criminal organization selling or renting the exploit kit. While exploit kits can be expensive to purchase outright, they can be rented for as little as $500 per month[xv].

- Ransomware has evolved from a focus on blocking/locking technologies that prevent users from gaining access to their files, to crypto technologies that actually encrypt files. The former are comparatively easy from which to recover because of the availability of tools that will unlock infected computers. The latter, however, are nearly impossible to defeat once infected because the cryptography normally cannot be broken and ransomware victims are normally given only a short period in which to pay the ransom.

Add to this the fact that phishing and ransomware authors are becoming better at accomplishing their goal of stealing financial or other data. For example:

Cybercriminals are developing new and better variants of ransomware, as well as improved methods for communication to infected systems.

- Some threats can remain dormant for an extended period and are less likely to be detected by many traditional anti-phishing and anti-malware solutions.
- Some types of malware can detect when they have been placed into a sandbox and so will not execute until after having been released from the sandbox.
- Some cyber criminals coordinate their attacks among various delivery venues, including email, social media, Web browsers, files, etc.
- One piece of malware can operate another that appears to be innocuous.
- Some malware requires user interaction, such as clicking on a button in a dialog box, before going into action and will not be "fooled" by the simulation of user clicks in a sandbox.

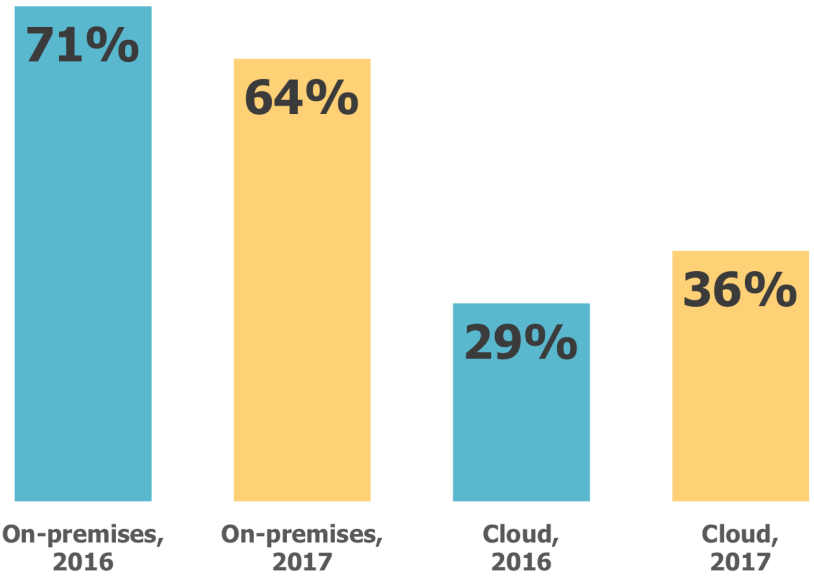
SECURITY SPENDING IN 2016 AND 2017

Decision makers clearly understand the threat of phishing, ransomware and other security risks and are spending significantly to address them. Our research found that the total security budget at the organizations surveyed will average $425 per employee in 2016, increasing 10.1 percent in 2017 to $468. Moreover, our research indicates that smaller organizations (up to 999 employees) will spend 51 percent more per employee on security-related expenditures than larger (1,000+ employees) organizations, underscoring the economies of scale that the latter enjoy in the context of IT spending in general, and security spending in particular.

Our research also revealed that security capabilities are migrating to the cloud. As shown in Figure 3, 71 percent of security-related budgets are spent for on-premises solutions in 2016, while 29 percent are spent on cloud-based solutions. However, in 2017, decision makers anticipate that the on-premises component of their security budget will drop to 64 percent, while the proportion devoted to the cloud will increase to 36 percent. Underscoring the increasing importance of the cloud in the context of security, our research found that in 2016 only 12.0 percent of organizations have budgets for cloud-based security that exceed their spending for on-premises solutions, but this figure is expected to increase to 18.5 percent in 2017.

Our research found that for many organizations, key security solutions are either not improving over time or their performance is actually deteriorating.

Figure 3
Distribution of Security Budgets Devoted to On-Premises and Cloud Solutions, 2016 and 2017



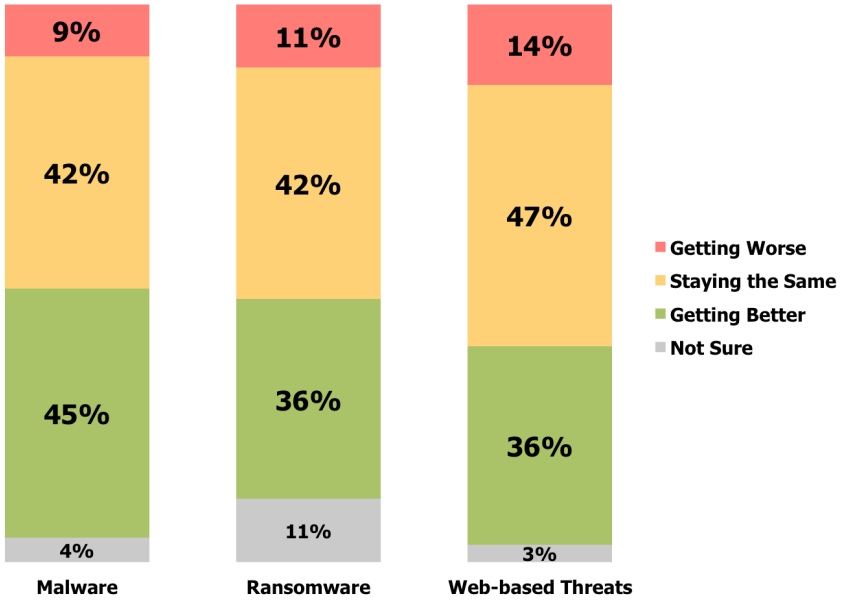
Source: Osterman Research, Inc.

SECURITY NEEDS SIGNIFICANT IMPROVEMENT

IMPROVEMENTS ARE MODEST

Our research found that for many organizations, key security solutions are either not improving over time or their performance is actually deteriorating. For example, as shown in Figure 4, 42 percent of organizations report that their solutions designed to block malware are not improving over time, while nine percent report that these solutions are actually getting worse. The problem of either static or degrading performance is even more pronounced for solutions designed to block ransomware and Web-based threats.

Figure 4
Perceptions About Changes in Performance of Key Solutions



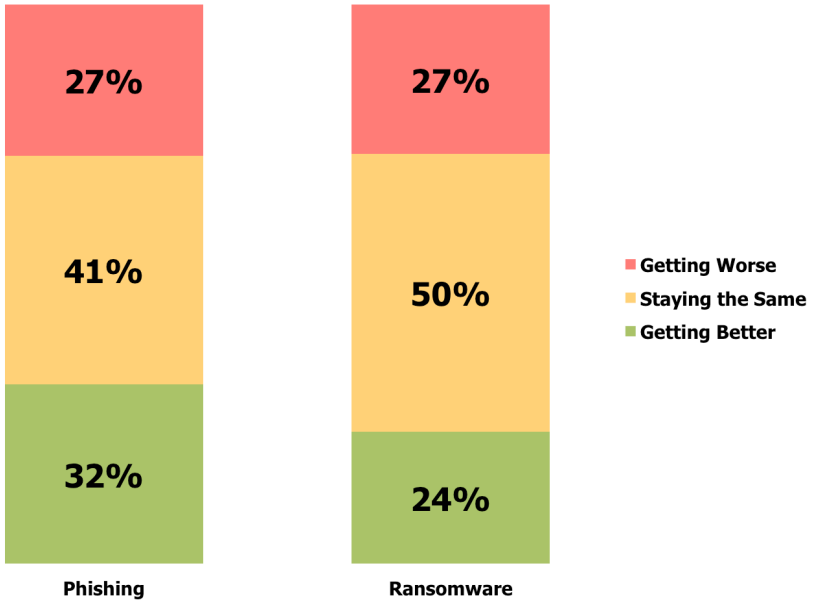
Source: Osterman Research, Inc.

PHISHING AND RANSOMWARE ARE GETTING WORSE

We also discovered that for most organizations, the problems they have experienced with both phishing and ransomware over the past 12 months are either getting worse or not improving. As shown in Figure 5, more than one in four organizations report that both phishing and ransomware are getting worse, while phishing and ransomware are as bad as they were a year ago for 41 percent and 50 percent of organizations, respectively.

….for most organizations, the problems they have experienced with both phishing and ransomware over the past 12 months are either getting worse or not improving.

Figure 5
Changes in Phishing and Ransomware Problems Over the Past 12 Months



Note: Totals may not equal 100% due to rounding error.
Source: Osterman Research, Inc.

HOW EFFECTIVE ARE CURRENT SOLUTIONS?

Our research also focused on determining how effective current security capabilities and solutions are in protecting organizations from the growing variety of threats that they face. As shown in Figure 6, one-third or fewer of organizations consider their end user training practices in the context of ransomware, Web surfing and CEO Fraud/BEC to be "excellent". The only areas in which a majority of IT decision makers believe they are doing an excellent job is in eliminating malware and spam before it can reach end users.

….one-third or fewer of organizations consider their end user training practices in the context of ransomware, Web surfing and CEO Fraud/BEC to be "excellent".

Figure 6
Perceived Effectiveness of Current Security Capabilities

Capability	Excellent	Moderate	Poor
Training end users on detecting and dealing with ransomware	27%	61%	13%
Training end users on best practices when surfing the Web	28%	63%	9%
Training end users on detecting and dealing with CEO Fraud/Business Email Compromise	33%	58%	9%
Preventing data loss via email or the Web	36%	57%	8%
Training end users on detecting and dealing with phishing threats	37%	55%	9%
Preventing users' personally owned mobile devices from introducing malware into the corporate network	43%	48%	9%
Eliminating ransomware before it reaches end users	50%	49%	1%
Eliminating malware before it reaches end users	56%	44%	0%

Figure 6 (concluded)
Perceived Effectiveness of Current Security Capabilities

Capability	Excellent	Moderate	Poor
Eliminating spam before it reaches end users	58%	43%	0%
AVERAGE	**41%**	**53%**	**6%**

Note: Totals may not equal 100% due to rounding error.
Source: Osterman Research, Inc.

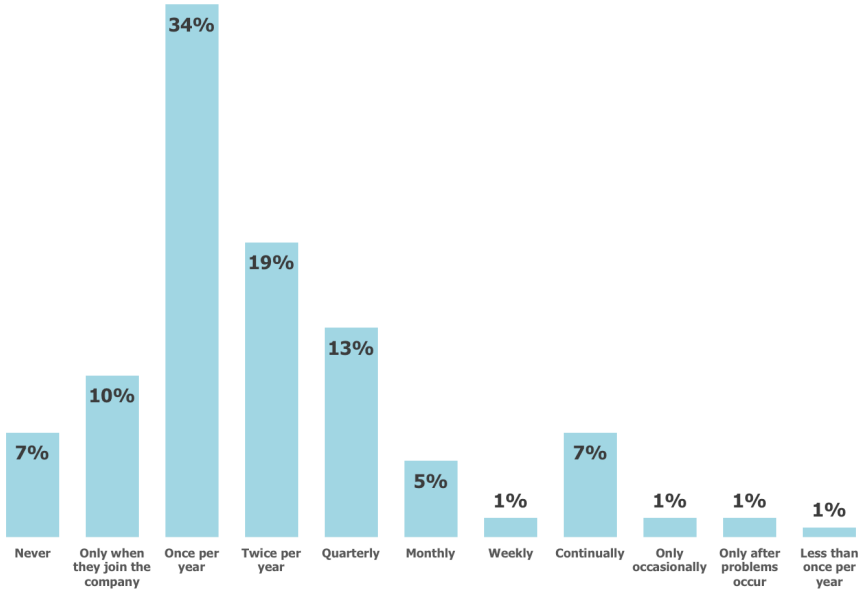
TRAINING NEEDS IMPROVEMENT

Our research further explored the confidence that organizations have (or don't have) with regard to how well employees are trained to deal with phishing and ransomware attacks. When decision makers were asked to rate their organizations on a scale of 1 (no confidence) to 100 (very confident), we found that only 13.6 percent of organizations scored a "90" or above in the context of phishing training preparedness, while only 11.1 percent scored this highly with regard to ransomware training preparedness. Moreover, we found that 17.6 percent of organizations are either "not too confident" or "not confident at all" that they can stop phishing attacks, while 23.8 percent feel this way about stopping ransomware attacks.

The relatively low marks for training preparedness are related to the minimal amount of security awareness training that many employees receive. For example, as shown in Figure 7, 52 percent of employees receive security awareness training (if they receive it at all) a maximum of once per year.

….52 percent of employees receive security awareness training (if they receive it at all) a maximum of once per year.

Figure 7
Frequency With Which Employees Receive Security Awareness Training



Source: Osterman Research, Inc.

This self-assessment reveals three important points:

- Not surprisingly, we found a relationship between the number of attacks that organizations have experienced during the past 12 months and their self-

assessment ratings for security: organizations that reported encountering no ransomware, malware, hacking or other security problems during the previous 12 months gave themselves a seven percent higher rating on the perceived effectiveness of their security capabilities than organizations that had experienced at least one security problem.

- With an across-the-board 41 percent "excellent" rating, organizations clearly still have a long way to go in protecting their users, networks and data assets from phishing, ransomware, other forms of malware infiltration, data loss and other security-related threats. Even in those areas for which decision makers give their organizations relatively high marks, the data reveals that significant improvements need to be made to provide more adequate protection.

- Improvement in phishing and ransomware protection is needed across the board, and additional security awareness training is needed to help reduce the infection rate of phishing and ransomware attacks. While training is just one component of a successful strategy to deal with phishing and ransomware, it can be effective: our survey found that organizations in which users receive security awareness training only once per year or less experience an average of 18.5 security attacks per year. However, among organizations whose employees are trained more than once per year, there is an average of 4.3 attacks.

WHERE ARE THINGS GOING FROM HERE?

Osterman Research anticipates that both phishing and ransomware attacks will continue to increase as they have for the past several years. Specifically, we anticipate that:

- The number of phishing emails that contain links or attachments intended to distribute ransomware or other types of malware will increase at a significant pace throughout the rest of 2016 and into 2017. Underscoring the rapid pace of just ransomware development, a Symantec study found that between 2005 and 2014, about 16 ransomware families were discovered in the wild. However, 27 were discovered in 2015 alone and another 15 were discovered in just the first quarter of 2016[xvi].

- A growing proportion of phishing attempts will be designed to install ransomware on victims' computers. One security company has determined that 93 percent of phishing emails as of mid-2016 are focused on distributing ransomware[xvii].

- While the overall spam problem has been on the decline for the past several years, spam is still an effective method to distribute malware, including ransomware. For example, Trustwave found that during a seven-day period in March 2016, 18 percent of the total volume of spam it detected contained malware or malware links[xviii]. We anticipate that spam will continue to be used as a secondary method to distribute ransomware and other forms of malware.

- Moreover, we believe that the market for ransomware and other forms of malware may be bifurcating to some extent. Because of the ease with which non-technical cybercriminals can enter the market, we anticipate a growing trend toward two distinct focus areas for ransomware criminals: a) "low-end" ransomware that demands a few hundred dollars in ransom that is sent by amateurs and other low-level criminals using basic phishing techniques; and b) "high-end" ransomware sent by more sophisticated cybercriminals and focused on high value targets in the healthcare, financial services, insurance and other industries that are more likely to pay significant sums to recover their encrypted data. We anticipate the latter will use more sophisticated spearphishing techniques in their attempts to infect high value endpoints.

- Businesses, not individuals, will increasingly be the primary target for phishing and ransomware, particularly the latter. Because businesses are more likely to have critical data that must be recovered, will have the wherewithal to obtain

….significant improvements need to be made to provide more adequate protection.

Bitcoin or other digital currencies with which to pay the ransom, and are more likely to pay larger ransom demands, cybercriminals will focus the bulk of their efforts on infecting these higher value targets.

RECOMMENDED BEST PRACTICES

Osterman Research recommends that decision makers undertake a variety of steps in order to deal more effectively with phishing and ransomware attacks.

UNDERSTAND THE RISKS YOU FACE

While it may seem trite to offer a recommendation simply to understand the risks that your organization faces, we cannot overstate the importance of doing just that. Decision makers must understand that they face threats not only from phishing and ransomware attacks, but also a growing variety of threats across all of their communication and collaboration systems, the personal devices that their users employ, and even users themselves. Cybercrime is an industry with significant technical expertise, extensive funding, and a rich target environment.

DEVELOP ADEQUATE POLICIES

Many organizations have not yet developed and published detailed and thorough policies for the various types of email, Web, collaboration, social media and other tools that their IT departments have deployed or that they allow to be used as part of "shadow IT". As a result, we recommend that an early step for any organization should be the development of detailed and thorough policies that are focused on all of the tools that are or probably will be used in the foreseeable future. These policies should focus on legal, regulatory and other obligations to encrypt emails and other content if they contain sensitive or confidential data; monitor all communication for malware that is sent to blogs, social media, and other venues; and control the use of personal devices that access corporate systems.

Establishing robust policies will not provide security protection per se, but it can be useful in limiting the number of tools that employees use when accessing corporate resources. In turn, these limitations can be helpful in reducing the number of ingress points for ransomware, other forms of malware, phishing attempts, and other content that could pose a security risk.

KEEP SYSTEMS UP-TO-DATE

Application, OS and system vulnerabilities can allow cybercriminals to successfully infiltrate corporate defenses. Every application and system should be inspected for vulnerabilities and brought up-to-date using the latest patches from vendors.

ENSURE YOU HAVE GOOD AND RECENT BACKUPS

A useful method for recovering from a ransomware attack, as well as from other types of malware infections, is to restore from a known, good backup taken as close as possible to the point before the infection occurred. Using a recent backup, an endpoint can be reimaged and its data restored to a known, good state with as little data loss as possible. While this strategy will likely result in some level of data loss because there will normally be a gap between the most recent backup and the time of reimaging, recent backups will minimize data loss if no other remedy can be found.

DEPLOY ANTI-PHISHING AND ANTI-RANSOMWARE SOLUTIONS

There are good solutions available that can be deployed on-premises or in the cloud that can detect phishing attempts, ransomware and a variety of other threats. Every organization should implement solutions that are appropriate to its security infrastructure requirements, but with specific emphasis on the ability to detect, isolate and remediate phishing and ransomware threats.

While the overall spam problem has been on the decline for the past several years, spam is still an effective method to distribute malware, including ransomware.

IMPLEMENT BEST PRACTICES FOR USER BEHAVIOR

Next, implement a variety of best practices to address whatever security gaps may exist in the organization. For example:

- Employees should employ passwords that correspond to the sensitivity and risk associated with the corporate data assets they are accessing. These passwords should be changed on an enforced schedule under the direction of IT.

- Implement a program of robust security awareness training that will help users to make better judgments about the content they receive through email, what they view or click on in social media, how they access the Web, and so forth. The goal of security awareness training is simply to help users to be more careful about what they view, what they open and the links on which they click. While security awareness training by itself will not completely solve an organization's security-related problems, it will bolster the ability for users – the first line of defense in any security infrastructure – to be more aware of security issues and to be less likely to respond to phishing and ransomware attempts. It is essential to invest sufficiently in employee training so that the "human "firewall" can provide an adequate first line of defense against increasingly sophisticated phishing and other social engineering attacks.

- Establish communication "backchannels" for key staff members that might be called upon to deal with corporate finances or sensitive information. For example, if a traveling CEO sends a request to her CFO to transfer funds to a supplier, the CFO should have an independent means of verifying the authenticity of the request, such as texting or calling to the CEO's smartphone.

- Employees should be tested periodically to determine if their security awareness training is effective.
- Employees should be reminded continually about the dangers of oversharing content on social media. Employees' friends might be interested in the latest breakfast, vacation or restaurant visit that gets posted on social media – but this information could give cybercriminals the information they need to craft a spearphishing email.

- Ensure that every employee maintains robust anti-malware defenses on their personally managed platforms if there is any chance that these employee-owned devices will access corporate resources.

- Employees should be reminded and required to keep software and operating systems up-to-date to minimize the potential for a known exploit to infect a system with malware.

USE ROBUST THREAT INTELLIGENCE

Every organization should use historical and real-time threat intelligence to minimize the potential for infection. Real-time threat intelligence can provide a strong defense to protect against access to domains that have a poor reputation and, therefore, are likely to be used by cybercriminals for spearphishing, ransomware and other forms of attack. Threat intelligence can also be used proactively by security analysts and others to investigate recent attacks and discover previously unknown threat sources. Moreover, historical threat intelligence – such as a record of Whois data that includes information on who has owned domains in the past – can be useful in conducting cybercrime investigations.

Using both real-time and historical domain and IP-based threat intelligence is an important adjunct for any security infrastructure because it offers protection in several ways:

There are good solutions available that can be deployed on-premises or in the cloud that can detect phishing attempts, ransomware and a variety of other threats.

- Organizations can remain compliant with the variety of regulatory obligations they face to protect employee data, customer data and other information they own or manage.

- Good threat intelligence helps to monitor both intentional and inadvertent use of corporate brands so that these brands can be protected.

- Threat intelligence provides forensics researchers with deep insight into how attacks began, how cybercriminals carried out their attacks, and ways in which future attacks can be detected early on and thwarted before they can do damage.

SUMMARY

Phishing and ransomware are very serious threats that can cause enormous damage to an organization's finances, data assets and reputation. They can cause vast disruption to an organization's employees and IT department, cause an organization to run afoul of industry and governmental regulations, can result in lawsuits, and – in extreme cases – put an organization out of business. However, there are steps that any organization can take to address phishing and ransomware so that the chances of infection – and the consequences that will arise from it – can be mitigated.

SPONSOR OF THIS WHITE PAPER

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit www.trustwave.com.

www.trustwave.com
@Trustwave
info@trustwave.com
+1 888 878 7817

REFERENCES

[i] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

[ii] Crypto ransomware is a more recent type of ransomware that will encrypt users' files as compared to blocking ransomware that simply prevented access to them. However, the goal of both types of ransomware is to prevent access to files until and unless a ransom is paid by the victim.

[iii] Source: Phishing Activity Trends Report, APWG, May 23, 2016

[iv] Source: McAfee Labs Threats Report, June 2016

[v] http://www.securityweek.com/history-and-statistics-ransomware

[vi] https://www.justice.gov/criminal-ccips/file/872771/download

[vii] http://www.bbc.com/news/technology-37166545

[viii] https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/; https://blog.knowbe4.com/cyberheist-nets-44-million-in-single-ceo-fraud-attack

[ix] http://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomware-attack/

[x] https://oag.ca.gov/system/files/Snapchat%20Inc%20updated%20Sample%20of%20Employee%20Notice%20of%20Data%20Breach_Redacted_0.pdf?

[xi] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[xii] http://resources.infosecinstitute.com/spear-phishing-real-life-examples/

[xiii] Results of an End User Survey About Communications Practices, Osterman Research, Inc.

[xiv] http://www.itworldcanada.com/article/largest-ransomware-as-service-scheme-pulls-in-us195000-a-month-report/385700

[xv] Source: Infosec Institute

[xvi] https://blog.malwarebytes.com/cybercrime/2016/06/ransomware-dominates-the threat-landscape/

[xvii] http://www.digitaltrends.com/computing/93-percent-phishing-emails-ransomware/

[xviii] https://www.trustwave.com/Resources/SpiderLabs-Blog/Massive-Volume-of-Ransomware-Downloaders-being-Spammed/