WHITE PAPER

Is Your Email Security Working? A Survey of the State of Ransomware, Phishing, and Business Email Compromise

An Osterman Research White Paper

Published January 2017

CYREN

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

EXECUTIVE SUMMARY

Ransomware, phishing, and Business Email Compromise (BEC) represent a group of critical email-delivered security threats that every organization will encounter at some point. This white paper gives background on why these threats are proliferating, shares the perspective of IT professionals on related questions, and provides a list of best practices to minimize an organization's risk.

These threats are not necessarily new, but have recently escalated dramatically in scope. Phishing started in the 1995-1996 time frame, became a recognized problem in the mid-2000s, and has now become the top threat risk facing businesses. Logical extensions of phishing, spearphishing (targeted against a group, a company or individuals within that company) and BEC activity (which targets senior executives within a single company, also referred to as whaling) are increasing rapidly and costing organizations hundreds of millions of dollars each year. Cyber extortion via ransomware, which is primarily e-mail delivered and has been enabled by the advent of Bitcoin as a payment vehicle, is reaching epidemic proportions, growing from payouts of $24 million in 2015 to $209 million in Q1 2016 and on pace for $1 billion in 2016,[i] according to an FBI tally from reported incidents, which doesn't take into account unreported incidents nor lost productivity and other costs.

ABOUT THIS WHITE PAPER

A primary research survey of business IT managers and decision-makers was conducted in the U.S. during the first week of January 2017 specifically for this white paper, some of the results of which are included herein. The complete set of survey results will be published in a separate Osterman Research survey report. This white paper was sponsored by Cyren – information about the company is provided at the end of this paper.

KEY TAKEAWAYS IN THIS PAPER

- The vast majority of IT decision makers are highly concerned about phishing, malware infiltration, spearphishing and ransomware, and for good reason: 75 percent of organizations report they have been the victim of these types of attacks and exploits during the last 12 months.
- Users continue to be the weak link in most organizations' security infrastructure.
- IT decision makers' confidence in their users' ability to deal with phishing, spearphishing, whaling/BEC and ransomware is low, in part because of the lack of training their users receive, but mostly because organizations are not preparing adequately and putting in the necessary systems to address these problems.
- The security solutions that are in place today are somewhat effective, but a significant proportion of decision makers report that their problems with phishing, spearphishing, whaling/BEC and ransomware are getting worse over time. For most of the security capabilities that organizations have deployed to combat these threats, the majority of decision makers report they are not highly effective.
- Problems with phishing, spearphishing, BEC and ransomware are getting worse as cyber criminals become more sophisticated, better funded and are outpacing many prospective victims' spending on new security solutions and security awareness training.
- Despite the escalating threat level, there are a number of steps that organizations can take to significantly improve their defenses against phishing, spearphishing, whaling/BEC and ransomware that will dramatically reduce their chances of falling victim to these attacks.

The vast majority of IT decision makers are highly concerned about phishing, malware infiltration, spearphishing and ransomware and for good reason.

LEADING SECURITY CONCERNS

The research conducted for this white paper found that a wide range of security problems have occurred within the organizations surveyed. As shown in Figure 1, 37 percent of organizations have been the victim of an email phishing attack that successfully infected systems with malware, 24 percent of have been the victim of a successful ransomware infection, and 22 percent have had sensitive or confidential information leaked through email. In fact, only 25 percent of the organizations we surveyed have not been the victim of at least one of the security incidents shown.

Figure 1
Security Problems That Have Occurred During the Previous 12 Months

Incident	% of Organizations
An email phishing attack was successful in infecting systems on our network with malware	37%
One or more of our endpoints had files encrypted because of a successful ransomware attack	24%
Malware has infiltrated our internal systems, but we are uncertain through which channel	22%
Sensitive / confidential info was accidentally leaked through email	22%
One or more of our systems were successfully infiltrated through a drive-by attack from employee web surfing	21%
An email as part of a whaling/BEC attack successfully tricked one or more senior executives in our organization	12%
An email spearphishing attack was successful in infecting one or more of our senior executives' systems with malware	10%
Sensitive / confidential info was maliciously leaked through email	7%
Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	6%
Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application	2%
Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain	2%
None of the above has occurred	25%

Source: Osterman Research, Inc.

RECENT PHISHING, SPEARPHISHING, WHALING/BEC AND RANSOMWARE EXAMPLES

Here are some recent examples of the types of attacks discussed in this white paper:

- The GoldenEye ransomware is targeting German speakers in HR departments using a two-part attack. The first attachment is a PDF file delivered in email that contains a cover letter, while the second attachment is an Excel file that uses malicious macros to load ransomware by asking the victim to click a link[ii].

- In early 2017, organizations with MongoDB databases in which access control had not been configured properly were deleted and were being held for ransom. On January 2nd, 200 databases had been deleted, but by January 6th the number of deleted databases reached 10,500[iii].

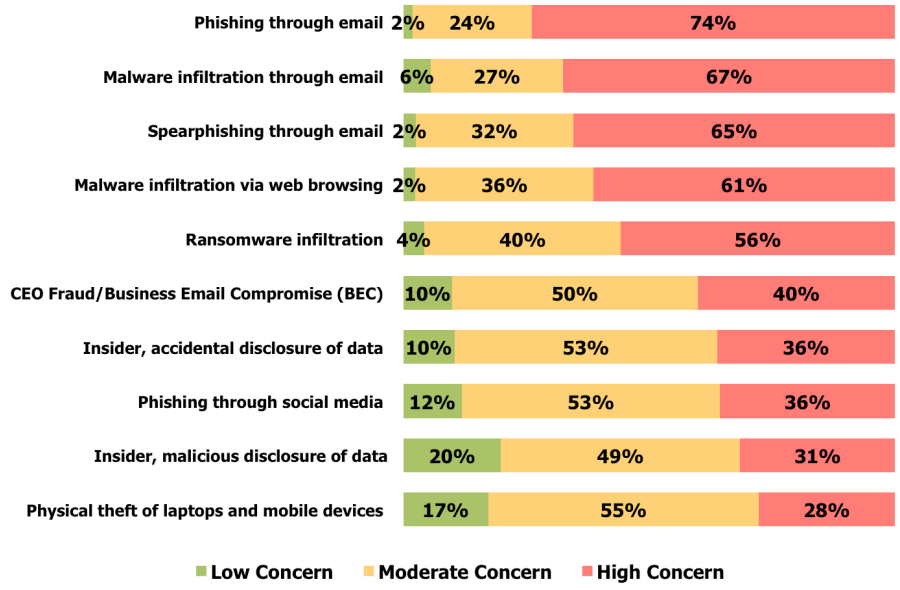
- A new ransomware technique employs a twist on social engineering by offering free decryption for victims' files if they send a link to their contacts and if at least two of these new victims pay the ransom of one Bitcoin[iv].

- Some notable victims of whaling or BEC over the past couple of years include Crelan Bank in Belgium (victimized for $75.8 million); FACC, an Austrian manufacturer of aircraft components, which ($54 million); Mattel, ($3 million); The Scoular Company, a commodities trading firm, ($17.2 million); Ubiquiti Networks, ($46.7 million); and the Romanian factor of German firm Leoni AG ($44 million).

PROBLEMS THAT CONCERN DECISION MAKERS MOST

Not surprisingly, there is a wide range of security issues about which IT decision makers and influencers are concerned. As shown in Figure 2, the top three issues of concern are focused on email as the primary threat vector: phishing, malware infiltration and spearphishing. However, a number of other security threats are also of significant concern, including malware infiltration through Web browsing, ransomware, and whaling/BEC.

Figure 2
Level of Concern Over Various Types of Security Threats



Source: Osterman Research, Inc.

The top three issues of concern are focused on email as the primary threat vector: phishing, malware infiltration and spear-phishing.

SECURITY SPENDING IN 2016 AND 2017

To address these security issues, organizations are spending significantly on security. Our research found that the median expenditure in 2016 focused on phishing, malware, ransomware and related types of threats was $58.33 per employee, increasing slightly to $58.85 per employee in 2017. More significantly, while 36 percent of organizations planned to spend the same amount in 2017 addressing these issues as they did in 2016, 62 percent will increase their security budget, while only two percent will spend less.

WHY ARE PHISHING, SPEARPHISHING, WHALING AND RANSOMWARE SUCCESSFUL?

Phishing, spearphishing, whaling/BEC, ransomware and other security threats have proven to be highly successful in stealing funds and causing other problems. Consider the following:

- The World Economic Forum places the global cost of cyber crime at $445 billion in 2016[v].
- The Ponemon Institute estimates that the typical 10,000-employee company spends $3.7 million per year dealing with just phishing attacks[vi].
- Vade Secure estimates that the cost of one spearphishing attack against a company with $100 million in revenue that suffers a breach of 50,000 records will be $7.2 million[vii].
- The FBI estimates that for the two years ended June 2016, whaling/BEC attacks have cost the more than 22,000 businesses that have fallen victim to it a total of $3.09 billion[viii].
- Ransomware attacks netted cyber criminals approximately $1 billion in 2016[ix].

These are staggering figures that cost organizations of all sizes enormous amounts of money in direct costs, but also lost employee productivity, lost revenue, lost goodwill with customers, and damage to their corporate reputations.

So, why are these attacks so successful?

USERS ARE THE WEAK LINK IN THE CHAIN

One of the fundamental problems with security – and the primary reason that these attacks are so successful – is users themselves. Most users are not adequately trained about how to recognize phishing, spearphishing, whaling/BEC, or ransomware attempts, and even those that are can still fall prey to them, induced by carelessness or succumbing to seemingly innocuous links or attachments in sophisticated emails. Our research found that six percent of users never receive any security awareness training, while 52 percent receive training no more than twice per year. The result is that users are not trained to be sufficiently skeptical of suspicious emails or other potential threats, such as short URLs in Twitter or Facebook advertisements. Moreover, organizations frequently do not provide the infrastructure that would adequately support better user-driven security, such as notifications, reminders, opportunities for users easily to query IT about suspicious emails or attachments, or effective automated email and web security.

The result is that IT is not at all confident in their users' ability to recognize incoming threats or in their organizations' ability to stop phishing and related incursions. For example, as shown in Figure 3, fewer than one in five IT decision makers or influencers is "confident" or "very confident" that their employees are adequately trained to recognize ransomware attacks. And, in any event, only 14% believe they can consistently stop phishing attacks and network intrusions.

Figure 3
Confidence in End User Training and the Ability to Stop Security Threats
Percentage Responding "Confident" or "Very Confident"

Source: Osterman Research, Inc.

ORGANIZATIONS ARE NOT PERFORMING SUFFICIENT DUE DILIGENCE AND HAVE INADEQUATE PROCESSES AND SECURITY SYSTEMS

Further complicating the problem – and enabling cyber criminals to be successful – is that organizations are not performing enough due diligence and making specific preparations to address the problems of phishing, spearphishing, whaling/BEC and ransomware. For example:

- Many organizations have insufficient backup processes that would enable them to rapidly revert content on servers, user workstations and other endpoints to a known good state following a ransomware attack or other incursion.
- Most organizations do not adequately test their users to determine which are most susceptible to interacting with malicious emails.
- Many organizations lack strong internal control processes that require checks and balances in an effort to prevent whaling/BEC attacks. For example, many organizations do not require that a wire transfer request from a senior executive delivered through email be verified through some sort of "back channel", such as a text message or voice call.
- Many organizations have not implemented email and web security technologies that are sufficiently sophisticated to reduce the threats that they face.
- Many organizations have not adequately addressed the "Bring Your Own" phenomenon in the context of the devices, mobile apps and cloud applications that users employ, allowing corporate data and system resources to be accessed through insecure means.

CRIMINAL ORGANIZATIONS ARE WELL FUNDED

The criminal organizations that are perpetrating cyber crime are generally very well funded and they have the technical resources to publish new and increasingly more capable variants of their malware. For example, ransomware has evolved from locker-

Organizations are not performing enough due diligence and making specific preparations to address the problems of phishing, spear-phishing, whaling/BEC and ransomware.

type variants that were the norm just a few years ago to more sophisticated, crypto-based variants like CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas (2016), Locky (2016) and Zepto (2016). Add to this the fact that ransomware-as-a-service is becoming more commonplace – as just one example, the Cerber service had infected 150,000 endpoints as of July 2016 and is generating profits of nearly $200,000 per month[x]. Because of their robust funding, criminal organizations can readily adapt to changing requirements in an effort to stay ahead of less capable security solutions and processes.

CYBER CRIMINALS ARE SHIFTING THEIR FOCUS

Cyber crime has been so successful over the past few years, data breaches have been so numerous, and the number of sellers on the "Dark Web" and in underground hacking forums have increased so much, that stolen credentials, credit card numbers, health records and other content are no longer as valuable as they once were. For example, the price of a payment card record in 2016 was $6, down from $13 in 2014 and $25 in 2011[xi]. The cost of a health record on the black market dropped from $75 to $100 in 2015 to just $20 to $50 in 2016[xii].

In effect, cyber criminals have flooded the market with so much stolen data that supply is exceeding demand, resulting in a significant drop in prices for this information. This means that cyber criminals will need to steal more data in order to generate the same level of revenue as they did in the past. Moreover, there is now a shift in emphasis from stealing information that then needs to be sold on the black market, where prices are declining, to stealing information directly from information-holders themselves. Cyber criminals will more frequently use phishing and spearphishing that will install malware like keyloggers that can enable them to transfer money out of corporate financial accounts, ransomware that will extort money from victims, and whaling/BEC that will trick senior managers into making large wire transfers directly to cyber criminals' accounts. This will effectively reduce the need to steal and sell something of value, and instead the funds directly.

WIDESPREAD AVAILABILITY OF LOW-COST PHISHING AND RANSOMWARE TOOLS

There is a growing number of tools designed to help amateurs with minimal knowledge of IT to become "hobbyist" phishers and ransomware authors. As noted in a FraudWatch International blog post from September 2016, "Gone are the days where only the most skilled hackers could develop a phishing site and scam users into divulging their personal information. Nowadays, any Joe Shmo can create one, and they do it with the help of a Phishing Kit.[xiii]" The result has been an explosion of ransomware and other exploits coming from a large and growing assortment of amateurs, adding to the problem from professional cyber criminal organizations.

MALWARE IS BECOMING MORE SOPHISTICATED AND HARDER TO DETECT

Over time, phishing and malware have become more sophisticated. For example, the early days of crude phishing attempts that tried to trick gullible users into clicking on a malicious link or open a malicious attachment have evolved into sophisticated BEC attacks in which hackers infiltrate an organization's network and learn business processes with the goal of crafting potentially lucrative attacks aimed at specific senior executives. Ransomware has evolved from variants that simply prevented an individual from accessing his or her files to those that use sophisticated encryption capabilities. Jonathan Whitley of WatchGuard Technologies believes that 2017 will see the development of even more sophisticated threats, such as self-propagating ransomware (what he dubs "ransomworms"), as well as the use of machine learning to get around security solutions that also rely on machine learning[xiv].

In short, the problems of phishing, spearphishing, whaling/BEC and ransomware are simply going to get worse without appropriate solutions and processes to defend against them.

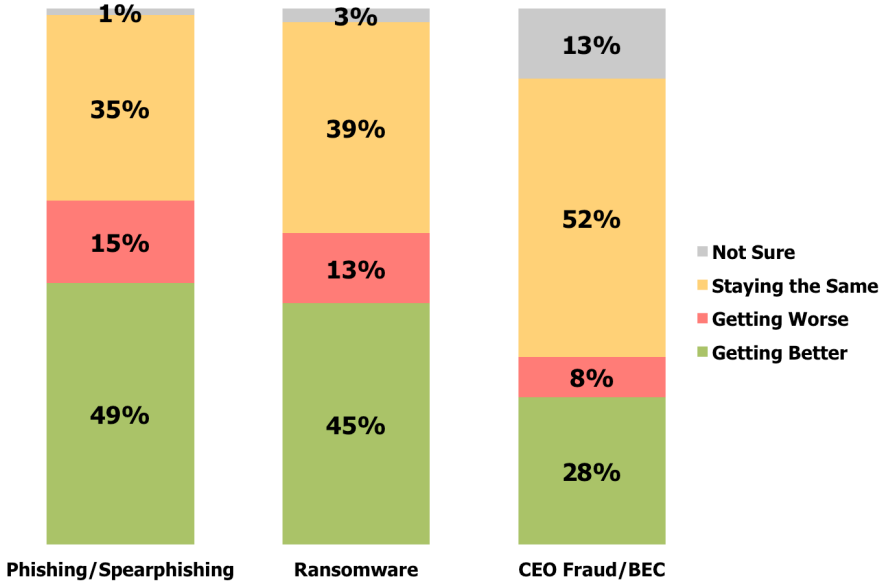
SECURITY MUST GET BETTER

The simple answer to the problem of increasingly sophisticated phishing, spearphishing, whaling/BEC and ransomware is that practices, processes, solutions and the overall mindset toward security must improve. However, our research found that while there are some improvements in security, they are not keeping pace with security threats.

SECURITY SOLUTIONS ARE IMPROVING ONLY SLIGHTLY IN SOME AREAS AND GETTING WORSE IN OTHERS

Our research found that nearly half of organizations perceive that their phishing/spearphishing and ransomware defenses are improving, by being better able to detect and thwart these threats before they can reach end users or have an impact on an organization. However, as shown in Figure 4, across all threat categories considered here, a majority of organizations report that their security solutions either are not improving or are getting worse, while many are simply unsure whether or not they are seeing any change.

Figure 4
Perceptions About Changes in the Effectiveness of Security Solutions



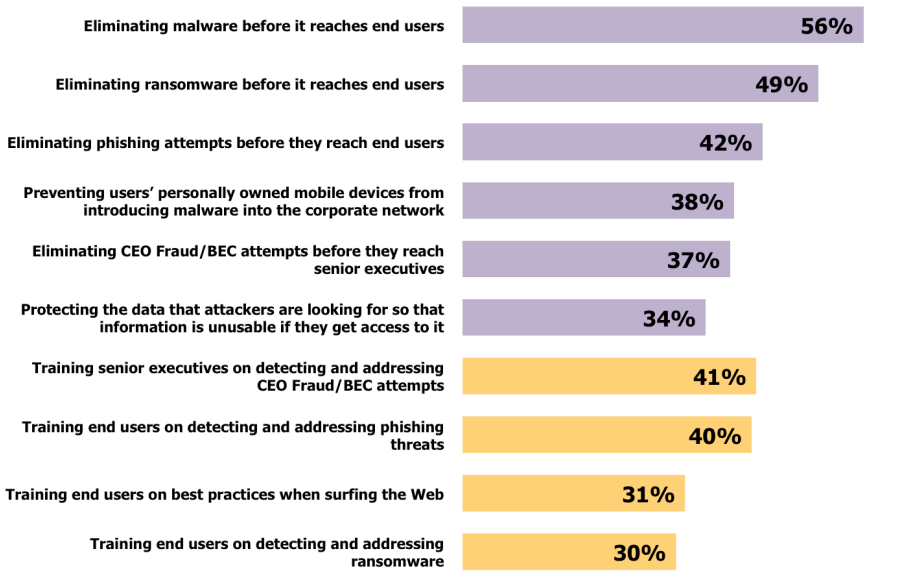
Source: Osterman Research, Inc.

HOW EFFECTIVE ARE CURRENT SOLUTIONS?

Our research also asked organizations to rate the effectiveness of their various security solutions and training practices. As shown in Figure 5, 56 percent of those surveyed believe that their current solutions to eliminate malware before it reaches end users are either "very good" or "excellent", but things deteriorate from there: fewer than one-half of respondents indicated that their solutions against ransomware, phishing or mobile device threats rate this highly. Even worse, the effectiveness of current end user training practices was considered "very good" or "excellent" by only a minority of organizations.

Our research found that while there are some improvements in cyber security, they are not keeping pace with threats.

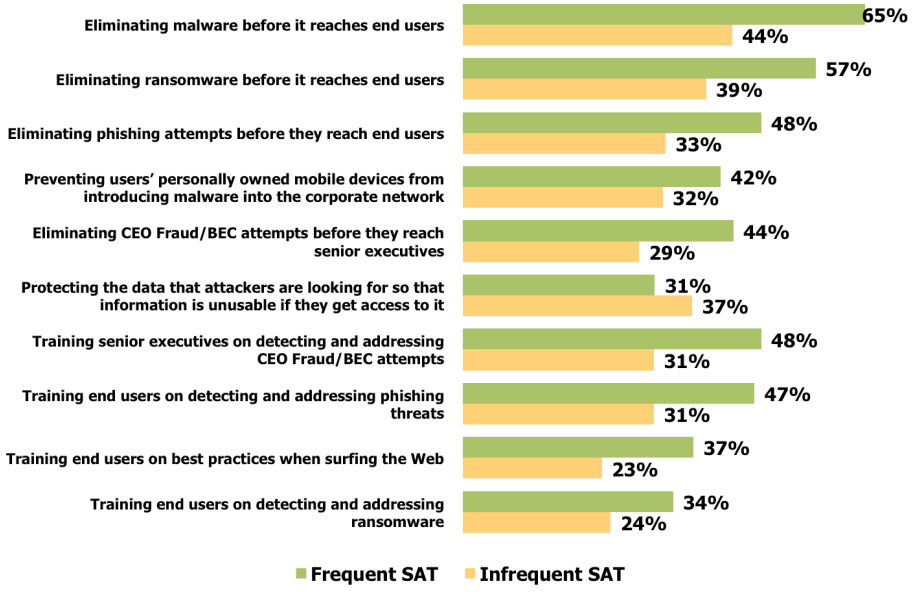
Figure 5
Perceptions About Capabilities in Training Users and Preventing Threats
Percentage Indicating that Effectiveness is "Very Good" or "Excellent"



Source: Osterman Research, Inc.

We found that organizations with more frequent security awareness training (where employees are trained at least twice per year) rate their security effectiveness more highly than organizations in which security awareness training is either less frequent or non-existent, as shown in Figure 6.

Figure 6
Perceptions About Organizational Capabilities in Training Users and Preventing Threats Based on Frequency of Security Awareness Training



Source: Osterman Research, Inc.

THREATS ARE GETTING WORSE

Compounding the problem of ineffective security solutions and inadequate training is the fact that phishing, spearphishing, whaling/BEC and ransomware are getting worse. For example:

- The Anti-Phishing Working Group reports that the number of unique phishing sites it detected grew from 0.39 million in 2014 to 0.79 million in 2015 to 1.49 million[xv] in 2016.
- Cyren reports that the number of phishing URL's its GlobalView™ security cloud is actively monitoring increased from
- The FBI reported that identified, exposed losses from whaling/BEC increased by 1,300 percent from January 2015 to June 2016[xvi].
- Symantec reports that the average ransom amount has increased from $294 in 2015 to $679 in 2016[xvii].
- The FBI reported that ransomware victims paid $24 million in ransom in 2015, but $209 million in just the first quarter of 2016.
- The Identify Theft Resource Center reported that the number of data breaches increased from 614 in 2013 to 783 in 2014 and dropped only slightly to 781 in 2015.

Osterman Research anticipates that phishing, spearphishing, whaling/BEC and ransomware – and the resulting data breaches and financial losses they can cause – will continue to get worse over the next few years in several key ways:

- Businesses will increasingly be the target for phishing and ransomware, not individuals. Because businesses are more likely to have mission-critical data that must be recovered, will have the means to purchase Bitcoin or other digital currencies to pay the ransom, and are more likely to pay higher ransom amounts, cybercriminals will focus more of their efforts on infecting these higher value targets. The increasing emphasis on businesses as targets of ransomware is borne out by data from Kaspersky, which found that corporate users comprised 6.8 percent of ransomware victims in the 2014-2015 timeframe, but 13.1 percent of victims in 2015-2016[xviii].
- The healthcare industry will be a key target for ransomware because of the success that cyber criminals have enjoyed so far in 2016 targeting hospitals and other healthcare facilities, and because healthcare organizations have demonstrated that they will pay significant amounts to recover their data. Among the healthcare organizations successfully attacked in 2016 were the Chino Medical Center (Chino, CA), Ottawa Hospital (Ottawa, ON), University of Southern California's Keck and Norris Hospitals (Los Angeles, CA), the New Jersey Spine Center (Chatham, NJ), Alvarado Medical Center (San Diego, CA), Professional Dermatology Care (Reston, VA), Hollywood Presbyterian Medical Center (Los Angeles, CA), Marin Healthcare District (Greenbrae, CA), King's Daughters' Health (Madison, IN), Urgent Care Clinic of Oxford (Oxford, MS), Kansas Heart Hospital (Wichita, KS), MedStar Health (Washington, DC), Desert Valley Hospital (Victorville, CA) and Methodist Hospital (Henderson, KY)[xix].
- Whaling/BEC will become a primary focus area for cyber criminals because of the lucrative nature of this activity. While these types of attacks require significantly more effort than, for example, ransomware attacks because of the need to determine key staff members in the target companies, the victims' suppliers, their payment practices, and so forth, the payoff is much larger. Trend Micro has determined that the typical whaling/BEC exploit results in a net payoff of $140,000 per incident compared to $30,000 from a successful ransomware

Businesses will increas-ingly be the target for phishing and ransomware, not individuals.

attack on an enterprise[xx].

FOURTEEN BEST PRACTICES AND TECHNIQUES TO CONSIDER

Osterman Research recommends that decision makers consider the following 11 steps that will help to improve an organization's security posture in the context of protecting against phishing, spearphishing, whaling/BEC and ransomware.

1. **Appreciate the risks that your organization faces**
   Decision makers must understand the risks that their organizations face from phishing, spearphishing, whaling/BEC and ransomware and address them as a high priority. While that may seem like an obvious recommendation, many decision makers understand problems intellectually, but they fail to put that understanding into action by training users appropriately and implementing the right security infrastructure. Cyber crime is an industry with sophisticated technical expertise, huge funding, and a rich target environment of potential victims and it must be dealt with as such.

2. **Conduct a complete audit of current security tools, training and practices**
   Organizations should conduct a thorough audit of their current security infrastructure, including their security awareness training regimen, the security solutions they have in place, and the processes they have implemented to remediate security incidents. This is an essential element in identifying the deficiencies that may (and probably do) exist, and it can be used to prioritize spending to address problems.

3. **Establish policies**
   It is important to develop policies for all of the email, Web, collaboration, social media, mobile and other solutions that IT departments have deployed or that are allowed for use as part of "shadow IT". As a result, Osterman Research recommends that a key step should be the development of detailed and thorough policies focused on the tools that are or probably will be used in the future. Policies should focus on legal, regulatory and other obligations to encrypt emails 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 that contain business content.

   Policies, in and of themselves, will not provide security per se, but they can be useful in limiting the number of solutions that employees use when accessing corporate systems. These limitations can be helpful in reducing the number of ingress points for ransomware, other forms of malware, phishing and spearphishing attempts, and other content that might pose a security risk.

4. **Deploy alternatives to the solutions that employees use as part of "Shadow IT"**
   It is important for IT to offer good alternatives to the solutions that employees have deployed, or might want to deploy, to be more effective in their work. This includes solutions for file-sync-and-share, voice-over-IP, cloud storage, real-time communications and other capabilities that employees download and install because they do not have an equivalent capability from IT, or because the IT-provided solution is not as good as the free or freemium solution they have chosen. Providing an IT-approved solution that is as good as the solutions that employees have deployed on their own can significantly enhance security and give IT control over corporate content. Look for tools or services, which provide Shadow IT discovery and control capabilities.

5. **Implement and/or update company procedures**
Every organization should implement, and periodically update, their company procedures with regard to how sensitive and confidential data, as well as business-critical systems, are protected and accessed. For example, every organization needs an effective set of backup, restoration and testing procedures for all of its data assets so that it can quickly recover from a ransomware infection. Moreover, dual-control procedures should be implemented for access to critical data assets, particularly those focused on financial transactions, so that a single, rogue employee cannot create a data breach or breach of security.

6. **Implement best practices for user behavior**
Organizations should establish a number of best practices to address whatever security gaps may exist in the organization. For example:

   - Employees should be tested on a regular basis to determine if their security awareness training has been effective, and to identify those employees that might need additional training.

   - Employees should use passwords that match the sensitivity and risk associated with the corporate assets they are accessing. These passwords should be changed on an enforced schedule established by IT.

   - Create communication "backchannels" for staff members that will be involved with corporate finances or sensitive information. For example, if a CEO sends a request to his CFO to transfer funds to an established vendor, the CFO should have a means of verifying the authenticity of the CEO's request before initiating the transfer, such as texting or calling the CEO's smartphone.

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

   - Employees, particularly senior executives who are more likely to be the target of a whaling/BEC attack, should be reminded regularly about the dangers of oversharing information on social media. Employees' friends might be interested in the latest personal information that gets posted on social media, but this information might give cybercriminals the information they need to create a believable spearphishing email.

   - Make sure that every employee maintains good anti-malware defenses on their personal devices if there is any chance that these devices will access corporate resources like corporate email or databases with sensitive corporate information.

7. **Train all users and senior executives**
Develop a good security awareness training program that will help users to make better judgments about the emails they receive, how they use the Web, the links they click in social media, and so forth. The goal of security awareness training is to help users to be more skeptical about what they view and what they consider to be safe to open. While security awareness training alone will not completely address an organization's security problems, it will bolster the ability for users to be more aware of security issues and make the organization less susceptible to phishing, spearphishing, whaling/BEC and ransomware attacks. It is critical to invest adequately in employee training so that this "human "firewall" can provide a solid first line of defense against increasingly sophisticated phishing and other social engineering attacks. Senior executives should have additional training to deal with spearphishing and whaling/BEC, since they are higher value targets to cyber criminals and the consequences of their failure can be dramatically greater.

Organizations should establish a number of best practices to address whatever cyber security gaps may exist in the organization.

8. **Keep systems up-to-date**
   Vulnerabilities in applications, operating systems, plug-ins and systems 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, a key mitigation technique to reduce the effectiveness of exploit kits. One source estimates that 99 percent of computers are vulnerable to exploit kits because almost all computers runs Oracle Java, Adobe Flash and/or Adobe Reader[xxi].

9. **Ensure there are good and recent backups**
   An effective way to recover from a ransomware attack, as well as from other types of malware infections, is to restore the infected endpoint(s) from a known, good backup taken as close as possible to the point before the infection occurred. With a recent backup, an endpoint can be reimaged and its data restored to a pre-infection state with minimal data loss. While this strategy will probably result in some 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.

10. **Deploy anti-phishing and anti-ransomware solutions**
    There are very good email security and web security solutions that can be deployed on-premises or in the cloud that can detect phishing and spearphishing attempts, ransomware and a variety of other threats. Every organization should implement solutions that are appropriate to its security infrastructure requirements, but with an emphasis on the ability to detect, isolate and remediate phishing, spearphishing, whaling/BEC and ransomware threats.

11. **Use good threat intelligence**
    The use of historical and real-time threat intelligence to reduce the potential for infection can be an effective way to reduce the likelihood of an attack or infection. Real-time threat intelligence can offer a strong defense to protect against access to domains that are known to have a poor reputation and so are more likely to be used by cyber criminals for phishing, spearphishing, ransomware and other forms of attack. Threat intelligence can also be used proactively by security analysts to investigate recent attacks and discover previously unknown threat sources. Plus, historical threat intelligence – such as a record of Whois data that includes information on who has owned domains in the past – can be of use in conducting cyber crime investigations.

12. **Implement data-centric protection of all high value data**
    At the end, no matter the cyber security precautions taken by an organization to stop an intrusion, a sophisticated cyber attack may get through cyber defenses. Organizations should implement data-centric protection of their most valuable data so that if attackers get through, the information captured will be unusable. New encryption technologies such as Format-Preserving Encryption (FPE) are easy to use and simple to maintain and can protect high value data at rest, in-use or in-motion, ensuring protection in all use cases. Recently, FPE was standardized by the National Institute of Standards and Technology (NIST) of the US Department of Commerce.

13. **Encrypt sensitive email communications**
    The disclosure of sensitive email communications has been central to some of the most high-profile data breaches in recent memory. Corporations should broadly leverage email encryption for protection of all internal and external emails. Either by the automated trigger of a DLP or by user initiation, email encryption should be added as a standard tool for fighting phishing by making sensitive data useless to the attackers. Look for a solution that encrypts email end-to-end, from originator to recipient on any desktop or mobile device. Some email encryption solutions can also be used to encrypt all data flowing into a cloud-office application provider, including files used in collaboration.

14. **Consider the use of behavior analytics**
    Behavior analytics examines the normal behavior patterns of employees across an organization and, when a divergence is noted – for example, when the user account accesses applications not previously accessed, accesses data at unusual times of the day or night or from foreign locations, or there is an increase in some other unusual activity – an exception is raised for further investigation, or access is immediately blocked. Unusual behavior could signal an employee going rogue, a malware attack, the presence of compromised credentials or some other problem, thereby enabling early detection and risk mitigation.

SUMMARY

Phishing, spearphishing, whaling/BEC and ransomware represent serious threats to any organization because they can be used to steal funds, extort ransom payments, exfiltrate intellectual property, disrupt business operations and, in extreme cases, actually put a company out of business. These problems are getting worse over time, because cyber criminals can easily exploit organizations that have not deployed appropriate security solutions and that have not adequately trained their users about best practices for dealing with email, social media and other business systems. However, there are robust security solutions and best practices that can be implemented to reduce dramatically the chance that a phishing, spearphishing, whaling/BEC or ransomware attack will be successful. Deploying these solutions and implementing best practices must be a high priority for every organization.

SPONSORS OF THIS WHITE PAPER

Cyren (NASDAQ and TASE: CYRN) protects more than 600 million users against cyber attacks and data breaches through its cloud-based web security, email security, DNS security and cloud sandboxing solutions. Relied upon by many of the world's largest technology companies such as Dell, Google, McAfee and Microsoft, Cyren offers enterprise-focused security-as-a-service solutions as well as embedded solutions for software and security providers. Cyren's global cloud security platform processes more than 17 billion daily transactions and uses innovative zero-day protection technology to proactively block over 130 million threats each day. Learn more at www.cyren.com.

www.cyren.com
@CYREN_IR
info@cyren.com
+1 703 760 3320

REFERENCES

[i] http://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/
[ii] http://www.techrepublic.com/article/hr-managers-beware-ransomware-could-be-your-next-job-applicant/
[iii] http://arstechnica.com/security/2017/01/more-than-10000-online-databases-taken-hostage-by-ransomware-attackers/
[iv] http://www.information-age.com/new-ransomware-offers-victims-free-decryption-key-123463585/
[v] https://www.weforum.org/reports/the-global-risks-report-2016
[vi] http://www.csoonline.com/article/2975807/cyber-attacks-espionage/phishing-is-a-37-million-annual-cost-for-average-large-company.html
[vii] http://blog.vadesecure.com/en/spear-phishing-cost/
[viii] https://www.ic3.gov/media/2016/160614.aspx
[ix] http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html
[x] http://www.itworldcanada.com/article/largest-ransomware-as-service-scheme-pulls-in-us195000-a-month-report/385700
[xi] Source: Intel Security as noted in the Verizon 2016 Data Breach Investigation Report
[xii] http://www.healthcareitnews.com/news/cybercriminals-poised-launch-more-ransomware-attacks-black-market-price-health-data-drops
[xiii] http://fraudwatchinternational.com/all/what-are-phishing-kits/
[xiv] http://www.itproportal.com/features/7-security-predictions-for-2017/
[xv] Osterman Research extrapolation based on January-September 2016 APWG data
[xvi] https://www.ic3.gov/media/2016/160614.aspx
[xvii] Source: *An ISTR Special Report: Ransomware and Businesses 2016*
[xviii] https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf
[xix] http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1
[xx] http://www.trendmicro.co.uk/vinfo/uk/security/research-and-analysis/predictions/2017
[xxi] https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/