WHITE PAPER

Techniques for Dealing with Ransomware, Business Email Compromise and Spearphishing

An Osterman Research White Paper

Published January 2017

KnowBe4
Human error. Conquered.

OSTERMANRESEARCH

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

Phishing, spearphishing, CEO Fraud/Business Email Compromise (BEC) and ransomware represent a group of critical security threats that virtually every organization will encounter at some point – and most already have. While phishing actually started in the 1995-1996 time frame, it became a much more serious problem in the mid-2000s. The logical evolution of phishing – spearphishing (targeted against a group, a company or individuals within that company) and CEO Fraud/BEC (which targets senior executives within a single company) – are increasing rapidly and costing organizations hundreds of millions of dollars each year. Add to this the fact that ransomware is reaching epidemic proportions and increasing at an even faster pace, growing from an impact of "just" $24 million in 2015, but increasing to approximately $1 billion in 2016[i].

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: most organizations have been the victim of these types of attacks and exploits, as well as others, during the last 12 months.

- The cyber security solutions that are in place today are somewhat effective, but a significant proportion of decision makers report that their problems with phishing, spearphishing, CEO Fraud/BEC and ransomware are getting worse over time (although the proportion reporting that their ransomware problem is staying the same or getter better increased from our 2016 survey). For most of the cyber security capabilities that organizations have deployed to combat these threats, the majority of decision makers report they are not highly effective.

- Users continue to be the weak link in most organizations' cyber security infrastructure because they have not been adequately trained to deal with phishing, spearphishing and CEO Fraud/BEC attempts.

- IT decision makers' confidence in their users' ability to deal with phishing, spearphishing, CEO Fraud/BEC and ransomware is low, in part because of the lack of training their users receive, but also because organizations are not performing sufficient due diligence to address these problems.

- Problems with phishing, spearphishing, CEO Fraud/BEC and ransomware are getting worse as cyber criminals become more sophisticated, better funded and are outpacing many prospective victims' spending on new cyber 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, CEO Fraud/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 ransom-ware…and for good reason.

ABOUT THIS WHITE PAPER

A primary research survey was conducted 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 KnowBe4 – information about the company is provided at the end of this paper.

LEADING CYBER SECURITY CONCERNS

The research conducted for this white paper found that a wide range of cyber 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 victims 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 cyber security incidents shown or, more importantly, are not aware they are victims.

Figure 1
Cyber 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 CEO Fraud/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 or are aware it has occurred	25%

Source: Osterman Research, Inc.

RECENT PHISHING, SPEARPHISHING, CEO FRAUD/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].

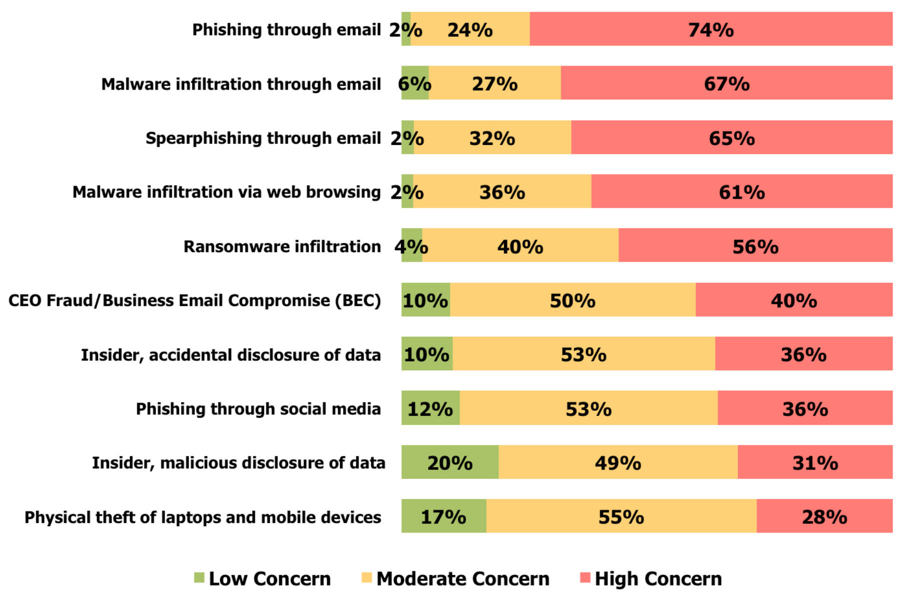
- A new ransomware technique employs a twist on social engineering by offering free decryption for victims' files if they send a link to their contacts and if at least two of these new victims pay the ransom of one Bitcoin[iv].

- Some notable victims of CEO Fraud/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 cyber 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 cyber security threats are also of significant concern, including malware infiltration through Web browsing, ransomware, and CEO Fraud/Business Email Compromise (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.

CYBER SECURITY SPENDING IN 2016 AND 2017

To address these cyber 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 for the year, increasing slightly to $58.85 per employee for 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 cyber security budget, while only two percent will spend less.

However, we found that larger enterprises (more than 1,000 employees) are actually planning to spend slightly less on cyber security in 2017 than they did in 2016, dropping from $23.86 per employee in 2016 to $21.53 per employee in 2017. Smaller organizations, on the other hand will see an increase from $66.67 per employee in 2016 to $70.00 per employee in 2017.

The significant difference in per-employee spending between larger and smaller organizations highlights one of the perennial problems of the latter: they lack the economies of scale to drive down the costs of cyber security, resulting in significantly higher per-employee costs simply because they have fewer employees over which to spread the costs of their cyber security infrastructure.

WHY ARE PHISHING, SPEARPHISHING, BEC AND RANSOMWARE SUCCESSFUL?

Phishing, spearphishing, CEO Fraud/BEC, ransomware and other cyber 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, CEO Fraud/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.

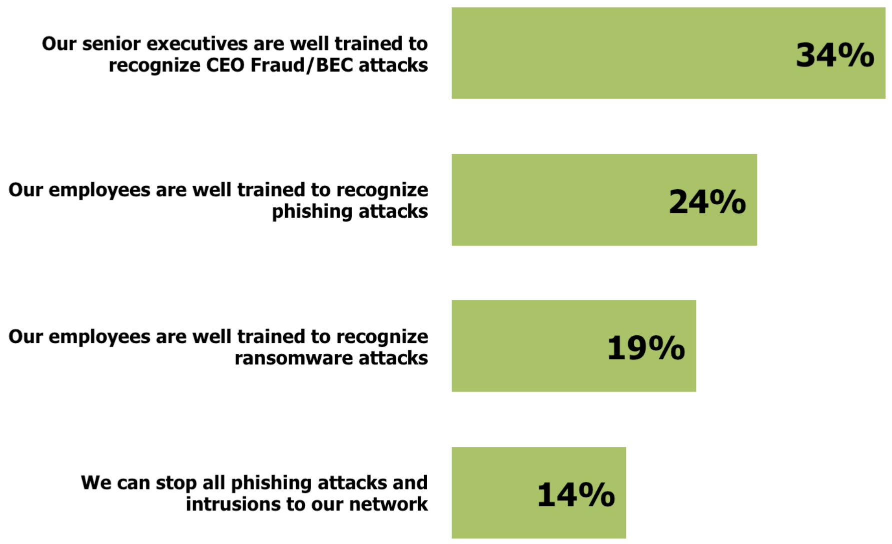
So, why are these attacks so successful?

USERS ARE THE WEAK LINK IN THE CHAIN

One of the fundamental problems with cyber 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, CEO Fraud/BEC, or ransomware attempts, and so often fall prey to them by clicking on links or opening attachments in emails that they receive without considering the potential for harm that can result. For example, 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, primarily because they have never been trained to be skeptical about these threat venues. Moreover, organizations do not provide the infrastructure that would adequately support better user-focused security, such as notifications, reminders, or opportunities for users easily to query IT about suspicious emails or attachments.

The result of this poor training 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.

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

Further complicating the problem – and enabling cyber criminals to be successful – is that organizations are not performing enough due diligence to address the problems of phishing, spearphishing, CEO Fraud/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 CEO Fraud/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 "backchannel", such as a text message or voice call.

- Many organizations have not implemented 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-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

Further complicating the problem is that organizations are not performing enough due diligence to address the problems of phishing, spearphishing, CEO Fraud/BEC and ransomware.

(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 cyber 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 CEO Fraud/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 is moving cyber criminals to steal 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 amateur cyber criminals, adding to the problem from professional cyber criminal organizations driven by the onset of Ransomware-as-a-Service (RaaS)[xiv].

MALWARE IS BECOMING MORE SOPHISTICATED

Over time, phishing and various types of 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 CEO Fraud/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 cyber security solutions that also rely on machine learning[xv].

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

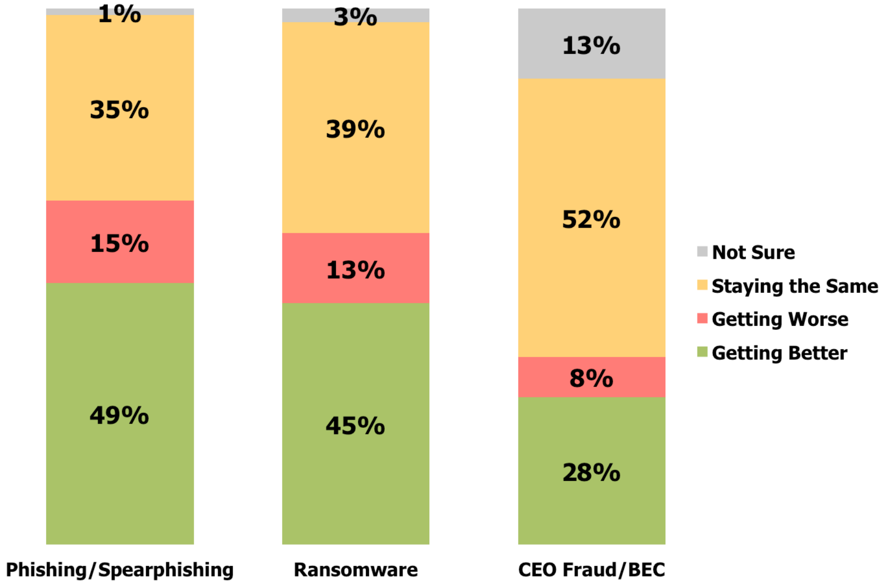
CYBER SECURITY MUST GET BETTER

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

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

Our research found that for many organizations, phishing/spearphishing, ransomware and CEO Fraud/BEC solutions actually 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, the majority of organizations report that their cyber 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 Cyber Security Solutions



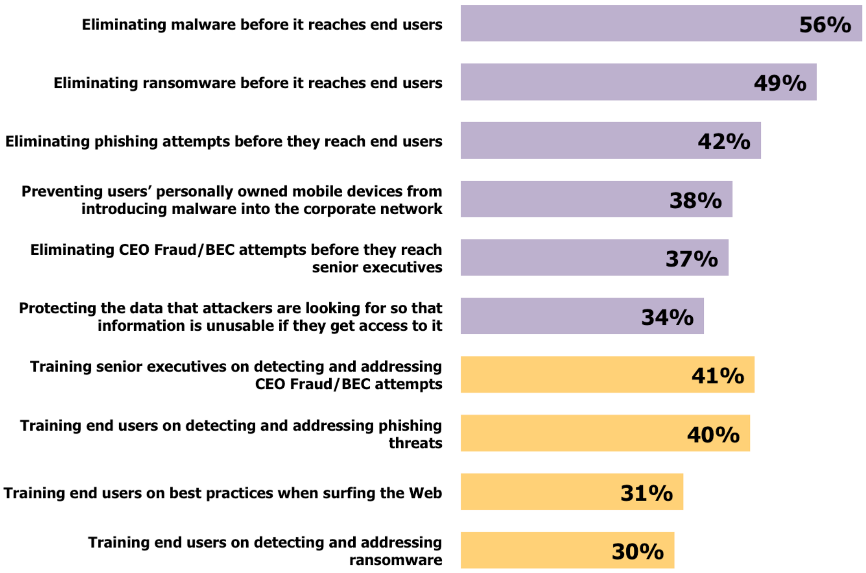
Source: Osterman Research, Inc.

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

HOW EFFECTIVE ARE CURRENT SOLUTIONS?

Our research also asked organizations to rate the effectiveness of their various cyber 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.

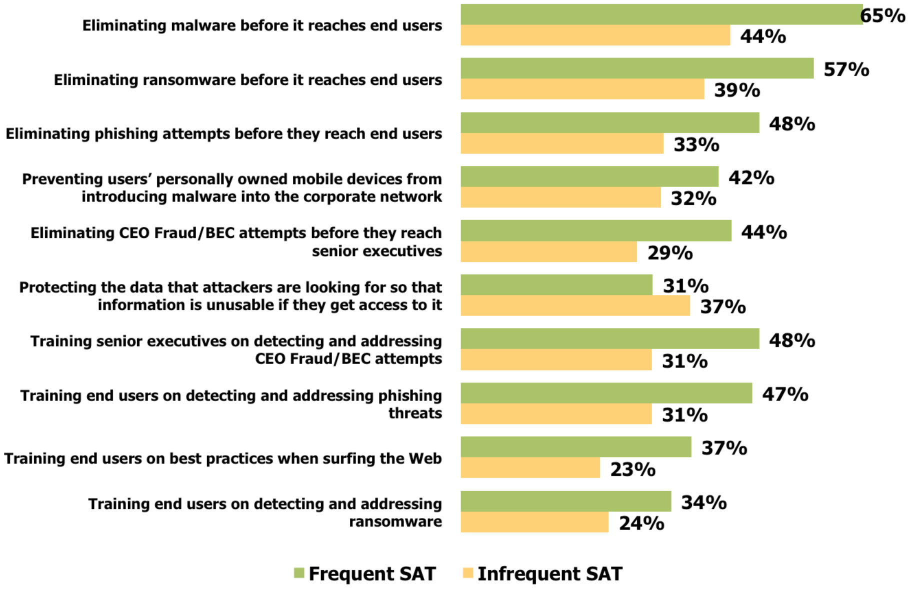
Figure 5
Perceptions About Capabilities in Training Users and Preventing Threats
Percentage Indicating that Effectiveness is "Very Good" or "Excellent"



Source: Osterman Research, Inc.

However, we found that organizations with more frequent security awareness training (where employees are trained at least twice per year) rate their cyber 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

WHAT DO WE MEAN BY "GETTING WORSE"?

Cyber security threats are getting worse, but what exactly does that mean? In short, it means that while cyber criminals are becoming more adept at their craft, many cyber security solutions and the level of security awareness training are not keeping pace. For example:

- Cyber criminals are shifting from consumer to corporate victims with very targeted strategies aimed at the latter, as noted below.

- Phishing, spearphishing and related types of attacks are becoming more advanced, making it harder for intrusion prevention systems, DLP and other defenses to detect a breach.

- The cost of data breaches, ransomware demands, and threat remediation continue to climb.

STATISTICS TO PROVE THE POINT

Compounding the problem of ineffective cyber security solutions and inadequate training is the fact that phishing, spearphishing, CEO Fraud/BEC and ransomware are becoming more common threats than they already are. 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[xvi] in 2016.

- The FBI reported that identified, exposed losses from CEO Fraud/BEC increased by 1,300 percent from January 2015 to June 2016[xvii].

- Symantec reports that the average ransom amount has increased from $294 in 2015 to $679 in 2016[xviii].

- The FBI reported that ransomware victims paid $24 million in ransom in 2015, but $209 million in just the first quarter of 2016 and was on-pace to be a $1 billion problem for all of 2016[xix].

- 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.

A GROWING VARIETY OF THREAT VECTORS

Osterman Research anticipates that phishing, spearphishing, CEO Fraud/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.

- 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[xx].

- 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), the National Health Service's (NHS') Lincolnshire and Goole Trust (three locations in England), 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), Lukas Hospital (Neuss, Germany), 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)[xxi].

Underscoring the tremendous vulnerability of the healthcare industry to cyber attack, one firm found that, as of mid-2016, 88 percent of ransomware attacks had been in the healthcare industry[xxii]. Many healthcare organizations have been hit with malware multiple times, such as Leeds Teaching Hospital (Leeds, England) that suffered five attacks during 2016[xxiii], part of the NHS' growing problem in which 30 percent of NHS Trusts have been hit with ransomware[xxiv].

- CEO Fraud/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 CEO Fraud/BEC exploit results in a net payoff of $140,000 per incident compared to $30,000 from a successful ransomware attack on an enterprise[xxv].

FOURTEEN BEST PRACTICES AND TECHNIQUES TO CONSIDER

Osterman Research recommends that decision makers consider the following 14 steps that will help to improve an organization's cyber security posture in the context of protecting against phishing, spearphishing, CEO Fraud/BEC and ransomware.

1. **Appreciate the risks that your organization faces**
   Decision makers must understand the risks that their organizations face from phishing, spearphishing, CEO Fraud/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 cyber 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 cyber security tools, training and practices**
   Organizations should conduct a thorough audit of their current cyber 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 cyber 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 cyber 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 cyber security and give IT control over corporate content.

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 cyber security.

6. **Implement best practices for user behavior**
   Organizations should establish a number of best practices to address whatever cyber 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. IT can help through management and enforcement on behalf of users.

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

- Employees, particularly senior executives who are more likely to be the target of a CEO Fraud/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 cyber security problems, it will bolster the ability for users to be more aware of cyber security issues and make the organization less susceptible to phishing, spearphishing, CEO Fraud/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 CEO Fraud/BEC, since they are higher value targets to cyber criminals and the consequences of their failure can be dramatically greater.

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[xxvi].

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 solutions that can be deployed on-premises or in the cloud that can detect phishing and spearphishing attempts, ransomware, data exfiltration and a variety of other threats. Every organization should implement solutions that are appropriate to its cyber security infrastructure requirements, but with an emphasis on the ability to detect, isolate and remediate phishing, spearphishing, CEO Fraud/BEC and ransomware threats. DLP is a key element in any cyber security infrastructure because of its ability to reduce or prevent data breaches.

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 cyber 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.

Corporations should broadly leverage email encryption for protection of all internal and external emails.

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, CEO Fraud/BEC and ransomware represent serious threats to any organization because they can be used to steal finances, 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 cyber 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 cyber security solutions and best practices that can be implement to reduce dramatically the chance that a phishing, spearphishing, CEO Fraud/BEC or ransomware attack will be successful. Deploying these solutions and implementing best practices must be a high priority for every organization.

SPONSOR OF THIS WHITE PAPER

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach. This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind. Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilized their end users as a first line of defense. Learn more at www.KnowBe4.com.

KnowBe4
Human error. Conquered.

www.knowbe4.com

@KnowBe4

info@knowbe4.com

+1 855 815 9494

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

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] https://www.enterprisetimes.co.uk/2016/05/20/clever-cerber-ransomware-attack-spotted/

[xv] http://www.itproportal.com/features/7-security-predictions-for-2017/

[xvi] Osterman Research extrapolation based on January-September 2016 APWG data

[xvii] https://www.ic3.gov/media/2016/160614.aspx

[xviii] Source: *An ISTR Special Report: Ransomware and Businesses 2016*

[xix] http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[xx] https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

[xxi] http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1

[xxii] https://www.helpnetsecurity.com/2016/07/27/ransomware-healthcare-industry/

[xxiii] https://www.infosecurity-magazine.com/news/30-of-nhs-trusts-hit-by-ransomware/

[xxiv] http://betanews.com/2017/01/17/uk-health-ransomware/

[xxv] http://www.trendmicro.co.uk/vinfo/uk/security/research-and-analysis/predictions/2017

[xxvi] https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/