WHITE PAPER

Best Practices for Protecting Against Phishing, Ransomware and Email Fraud

An Osterman Research White Paper
Published April 2018

Malwarebytes

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

Executive Summary

- **Various types of security threats are increasing in number and severity at a rapid pace, most notably cryptojacking malware that is focused on mining coins for the roughly 1,400 cryptocurrencies currently in use.**

- **Organizations have been victimized by a wide range of threats and exploits, most notably phishing attacks that have penetrated corporate defenses, targeted email attacks launched from compromised accounts, and sensitive or confidential information accidentally leaked through email.**

- **Threats are becoming more sophisticated as well-financed cybercriminal gangs develop improved variants of malware and social engineering attacks. The result is that the perceived effectiveness of current security solutions is not improving – or is actually getting worse – for many organizations.**

- **Decision makers are most concerned about endpoints getting infected with malware through email or web browsing, user credentials being stolen through email-based phishing, and senior executives' credentials being stolen through email-based spearphishing.**

- **Four of the five leading concerns expressed by decision makers focus on email as the primary threat vector for cybercriminal activity, and nearly one-half of attacks are focused on account takeovers.**

- **Most decision makers have little confidence that their security infrastructure can adequately address infections on mobile devices, CEO Fraud/BEC, and preventing users personal devices from introducing malware into the corporate network.**

- **Many organizations are not exercising proper due diligence on a number of fronts in the context of their security posture, including security awareness training, data backup processes, strong internal control processes, implementation of technologies in-depth, and establishment of adequate processes.**

- **To address the worsening threat landscape, security spending at mid-sized and large organizations will increase by an average of seven percent in 2018 compared to 2017.**

- **There are a number of best practices that organizations should seriously consider as they attempt to bolster their security defenses. These include conducting a thorough audit of the current security and compliance environment, establishing detailed and thorough policies, implementing best practices for users to follow, provide adequate security awareness training that is commensurate with the risk associated with each role, and deploy alternatives to employee-managed tools and services.**

Many organizations are not exercising proper due diligence on a number of fronts in the context of their security posture.

ABOUT THIS WHITE PAPER

A survey was conducted specifically for this white paper, some of the results of which are included here. However, a full survey report will be published shortly after publication of this white paper.

This white paper was sponsored by Malwarebytes; information about the company is provided at the end of this white paper.

Overview

Security teams and the organizations they support live in difficult times: they increasingly are the targets of sophisticated threats developed by a shadowy and very well financed cybercrime industry that has demonstrated it can often outsmart even the most robust security defenses. Cybercriminals are aided by the fact that security teams often lack the human and financial resources necessary to keep pace, and so often cannot defend against the latest threats that are directed against them. Add to this the fact that security teams often support users who unwittingly aid cybercriminals (or occasionally become them) through mistakes or intentional acts that can result in the loss of sensitive data or corporate funds. Consider what security teams are up against:

- Cryptocurrency mining on endpoints increased by 8,500 percent during 2017[i] and the trend is accelerating: one vendor found that the deployment of illicit cryptomining scripts grew by 725 percent during a four month period ending in January 2018[ii].
- The practice of injecting malware into software updates increased by 200 percent during 2017[iii].
- The number of web application vulnerabilities increased by 212 percent in 2017, and more than one-half of these vulnerabilities have a public exploit that hackers can use[iv].
- There was a 54 percent increase in mobile malware during 2017[v].
- In February 2018, there was one phishing attempt in every 3,331 emails and one piece of malware for every 645 emails[vi]. That means that in an organization of 500 email users who receive a median of 100 emails per day, the security infrastructure will receive 15 phishing attempts and 77 pieces of malware each day.
- While the massive ransomware campaigns we saw in 2015 and 2016 have abated to some extent, we continue to see targeted ransomware campaigns focused on specific industries like healthcare and government, among others. Moreover, the number of ransomware variants continues to increase: one source found a 74 percent increase during the 13 months ended February 2018[vii].
- While spam is today less of a problem than it was several years ago, the one-year period that ended in March 2018 saw an overall increase in the volume of spam traversing the Internet, with enormous spikes occurring in early 2018[viii].
- Security teams must deal with all of these issues, in addition to the everyday problems of rootkits, bootkits, adware, overwriting viruses, bots, software bugs, keyloggers, password-stealing Trojans, backdoors, and dumb user mistakes.

We discovered a wide range of security incidents that have occurred to survey respondents' organizations over the past year.

What Concerns Decision Makers?

What types of security threats could compromise an organization's data assets and, in some cases, even put it out of business? We discovered a wide range of security incidents that have occurred to survey respondents' organizations over the past year, most notably successful phishing attacks that infected one or more systems with malware (28 percent of organizations), targeted email attacks from a compromised account that had the same result (25 percent) and the loss of sensitive or confidential information that was successfully leaked through email (25 percent), as shown in Figure 1.

Figure 1
Percentage of Organizations That Have Been the Victim of a Security Incident During the Period March 2017 to March 2018

Incident	% of Orgs
A phishing attack was successful in infecting systems on our network with malware	27.9%
A targeted email attack launched from a compromised account successfully infected an endpoint with malware	25.0%
Sensitive / confidential info was accidentally leaked through email	25.0%
A targeted email attack launched from a compromised account successfully stole a user's account credentials	23.1%
One or more of our endpoints had files encrypted because of a successful ransomware attack	22.1%
Malware has infiltrated our internal systems, but we are uncertain through which channel	21.2%
One or more of our systems were successfully infiltrated through a drive-by malware attack from employee web surfing	19.2%
An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization	17.3%
A fileless/malwareless attack reached an endpoint	17.3%
An account takeover-based email attack was successful	15.4%
Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	8.7%
A targeted email attack was successful in infecting one or more of our senior executives' systems with malware	7.7%
Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application	5.8%
Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain	5.8%
Sensitive / confidential info was maliciously leaked through email	4.8%
None of the above	34.6%

Source: Osterman Research, Inc.

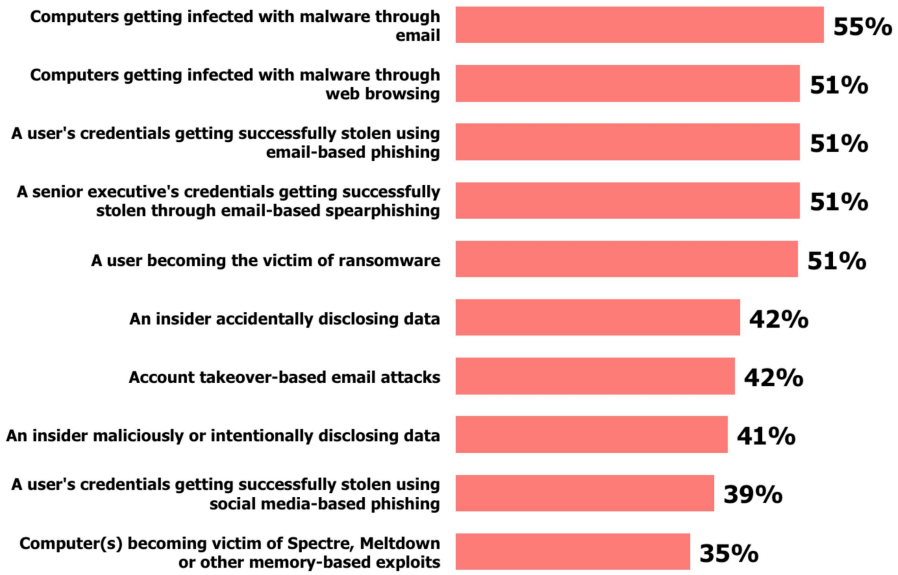
It's important to note that account takeover-based and related types of attacks constitute a major source of threats that organizations face. Our research showed that these types of attacks account for 44 percent of the attacks that organizations encounter.

It's also important to note that 35 percent of respondents who reported no security incidents over the past year may be a bit low. It's likely that some survey respondents may be less than completely forthcoming about all of the security problems that have occurred, either because it's corporate policy not to divulge security incidents publicly, they might be reluctant to share their security department's shortcomings, or they might not be aware of all of the incidents that have occurred.

ISSUES THAT CONCERN DECISION MAKERS MOST

There are a number of cybersecurity issues about which IT decision makers and influencers are concerned or very concerned. As shown in Figure 2, four of the top five issues of concern – all of which were an important issue for more than one-half of respondents – are focused on email as a key threat vector: phishing, malware infiltration and spearphishing. That said, a number of other cybersecurity threats are also of concern, including malware infiltration through Web browsing, data breaches, and account takeover-based email attacks.

Figure 2
Security Issues That Concern Organizations Most
Percentage Responding a "Concern" or "Major Concern"



Source: Osterman Research, Inc.

TARGETED ATTACKS ARE DIFFERENT FROM OTHER TYPES OF ATTACKS

Unlike a traditional phishing attack in which a cybercriminal is going after an individual's bank account login credentials or their credit card number, a targeted email attack is designed to bypass an organization's security defenses using sophisticated malware to gain access to endpoints or other resources. The goal of such an attack might include stealing intellectual property, stealing login credentials for corporate financial accounts so that funds can be transferred out, or simply gaining access for purposes of reconnaissance in anticipation of a future attack. Fundamentally, the goal is to locate, exfiltrate and monetize stolen data and intellectual property without the victim finding out before it happens.

THE POTENTIAL FOR THE CLOUD TO INCREASE SECURITY THREATS

Cloud providers generally offer very good security defenses, but they are vulnerable to attack because they aggregate such a large volume of their customers' valuable information. Although these providers normally have better security capabilities than most of their customers and suffer fewer data breaches than the typical enterprise customer, a successful breach of cloud-based data can expose customers to regulatory fines, other financial penalties, loss of customer confidence, and declining competitive market position, among other consequences. For example, consider the perception of companies like Uber, Yahoo!, Dropbox, eBay, Adult Friend Finder, Equifax and others that store data in the cloud and that have been the victims of major security breaches. To be sure, data breaches in the cloud are less common than those of organizations that maintain their data largely on-premises, but the breaches tend to be enormous when they do happen.

A cloud provider that suffers a breach and loses its customers' data must follow mandatory data breach notification laws in almost every US state and a growing number of countries. For example, Europe's General Data Protection Regulation (GDPR) will come into force in May 2018, continuing the data breach notification requirements of the earlier Data Protection Directive, while introducing major

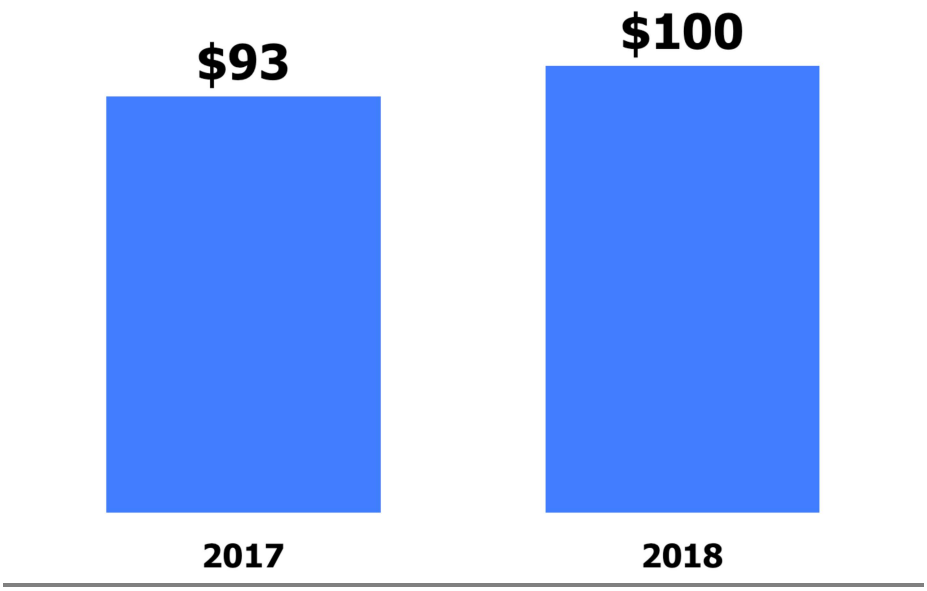
Cloud providers generally offer very good security defenses, but they are vulnerable to attack because they aggregate such a large volume of their customers' valuable information.

financial penalties for failure to protect customer data adequately. The Australian government has passed a data breach notification extension to its Privacy Act. Japan is focused heavily on protecting data privacy and has imposed strict rules about penalizing those who do not adequately protect customer and other data.

SECURITY SPENDING IN 2018 VERSUS 2017

The survey conducted for this white paper found that the average security budget will be increasing in 2018 compared to 2017, and that most organizations are increasing their security budgets in 2018. As shown in Figure 3, the typical security budget will increase from $93 per employee in 2017 to $100 in 2018. Moreover, 67 percent of the organizations surveyed will increase their security budgets in 2018, 30 percent will keep their budget constant, and only two percent will decrease it.

Figure 3
Median Security Budget per Employee, 2017 to 2018



Source: Osterman Research, Inc.

The Growing Success of Cyberthreats

ORGANIZATIONS ARE NOT PERFORMING ADEQUATE DUE DILIGENCE

One of the several reasons that cybercriminals are achieving success is because many organizations are not exercising adequate due diligence in addressing the problems of phishing, spearphishing, CEO fraud/business email compromise (BEC) and ransomware. For example:

- Most organizations do not sufficiently test their users' security awareness to determine which are most susceptible to interacting with malicious content.
- Many have inadequate backup processes that would enable them to rapidly recover from a ransomware attack.
- Many lack strong the internal control processes that would enable them to prevent CEO Fraud/BEC attacks. For example, many have not set up an adequate process for wire transfers that would require the recipient of a funds-transfer request, such as the CFO, to contact the requestor, such as the CEO,

through an out-of-band mechanism, or "backchannel", to verify the request.

- Many have not implemented technologies that are sophisticated enough to reduce the number of incoming phishing, spearphishing and other threats that are sent to them.

- Some organizations don't perform the basic types of due diligence that would enable them to identify problems before they start. As just one example is the case of Hannah Robert, who operated as a defense contractor out of her home. In October 2010, Ms. Robert used her church's password-protected web site to transmit sensitive military drawings to India where she owned a company that manufactured defense-related hardware, and which submitted defense contracting bids to foreign entities. Ms. Robert's action resulted in the grounding of 47 F-15 Eagle fighters operated by the US Air Force and she was subsequently sentenced to 57 months in prison[ix].

- Finally, many IT and security departments have not properly addressed the "Bring Your Own" devices/cloud/apps phenomenon, allowing corporate data and system resources to be accessed through insecure means.

CRIMINAL ORGANIZATIONS ARE CAPABLE

Another reason for the success of cybercrime is that criminal organizations are generally well funded, they have the technical resources to create new and increasingly more capable attack methods, and they often are highly collaborative in nature. Looking at just the evolution of ransomware, which actually dates back to 1989 (the AIDS Trojan malware was mailed to victims on a floppy disk[x]), we have seen the evolution of locker-type variants that were commonplace just a few years ago to more sophisticated, crypto-based variants like:

- 2013: CryptoLocker
- 2014: CryptoWall, CTB-Locker and SimpLocker
- 2015: TeslaCrypt, Encoder, Chimera, Fusob and Small
- 2016: Samas, Locky, Zepto, KeRanger, Mamba and ZCryptor
- 2017: WannaCry, NotPetya and Bad Rabbit
- 2018: GandCrab

The robust capabilities of cybercriminal organizations in creating ransomware has led to significant profits for these organizations. For example, CryptoLocker generated more than $3 million in revenue between September and December 2013 after infecting more than 250,000 endpoints[xi], and CryptoWall had generated $18 million in revenue through mid-2015[xii]. All told, the FBI estimated that ransomware generated revenue of $24 million in 2015 and $1 billion in 2016[xiii], and Cybersecurity Ventures estimated the figure to be $5 billion in 2017[xiv].

Some organizations don't perform the basic types of due diligence that would enable them to identify problems before they start.

THE GROWTH OF CRYPTOCURRENCY MINING

While ransomware will continue to be a threat, it is now being supplanted by the growth of cryptocurrency mining (or cryptojacking) that can be more profitable than ransomware, and which can create its own set of threats for security teams to address. Underscoring the growing threat of cryptomining:

- Malwarebytes reported that malicious cryptomining has been leading their detection of endpoint threats since September 2017[xv].

- Imperva reported that as of December 2017, 88 percent of remote code execution attacks were related to cryptomining malware, a jump from just 55 percent in September 2017[xvi].

- Symantec reported that cryptocurrency mining increased by 8,500 percent during 2017 – the company logged 1.7 million detections on endpoint computers just in December 2017[xvii].

- Cyren monitored 500,000 web sites during the period September 2017 to January 2018 and found that 7,281 web site servers were running cryptomining scripts, an increase of 725 percent during that four-month period[xviii].

Cryptocurrencies are managed via a "blockchain", a peer-to-peer network that serves as a distributed ledger of cryptocurrency transactions that will register and validate the creation of these currencies. The 1,400+ cryptocurrencies that exist today are generated through "mining", a process of solving complex calculations. The problem of cryptocurrency, from a security perspective, is that the mining process requires enormous amounts of computing power. Cryptocurrency miners can obtain the necessary software for the mining process for a modest fee, but they need massive amounts of computing power to process the algorithms necessary to generate cryptocoins. For those miners and mining organizations (some of which are state-sponsored, such as North Korea's suspected involvement in the practice) that don't want to make the investments in hardware and electricity necessary to conduct lucrative mining operations, they can turn to malware that will help them to create an army of cryptomining bots. While cybercriminal cryptominers can illegally exploit the massive computing resources of a supercomputer or high-speed internal network without malware, as was the case for a dogecoin-mining operation at Harvard University in 2014[xix], they are increasingly using malware to create highly distributed networks of bots that they develop through fairly traditional means like malvertising, phishing and even Facebook Messenger[xx].

While cryptomining malware represents a serious security threat, it's actually less of a direct threat than other types of malware, such as ransomware. For example, while ransomware is "noisy" in that it announces itself after encrypting a victim's files in an attempt to extort a payment, cryptomining malware is intentionally quiet because the miners want to exploit the infected computing resource for as long as possible without being detected. However, an endpoint infected with cryptomining malware will significantly impact the computing power available on that endpoint, since the compute-intensive nature of cryptomining draws down most of the available CPU (or GPU) power. More sophisticated types of cryptomining malware will actually stop working to avoid detection when a victim plays a game that requires the GPU, but will consume virtually all of the available computing resources of infected endpoints.

CYBERCRIMINALS ARE CHANGING THEIR FOCUS

Cybercriminal activity has been so successful over the past few years, data breaches have been growing so quickly, and the number of vendors on the "Dark Web" have increased so much, that "traditional" cybercrime is no longer as lucrative. For example, stolen credit card numbers, passport information, login credentials, files, healthcare records and other sensitive or confidential information have been falling in price over the past several years simply because of the laws of supply and demand: the supply of this stolen content has grown faster than demand, and so prices have gone down. For example, Facebook login credentials can be purchased on the Dark Web for as little as $5.20, Costco account information goes for $5.00 and Uber credentials sell for only $7.00. On the other hand, PayPal credentials for accounts with significant balances go for nearly $250[xxi].

To more efficiently generate revenue, cybercriminals turned to ransomware and activities like CEO Fraud/BEC that enable them to steal directly from victims rather than stealing something of value that then has to be sold to someone else. However, while these activities will definitely continue for some time to come, more organizations are becoming aware of how to either block ransomware or recover from it (or they just refuse to pay), and more decision makers are becoming aware of the methods they can use not to fall victim to CEO Fraud/BEC attacks.

The result is that activities like cryptomining will increase in popularity because they can be more lucrative and are not currently as subject to the same level of awareness from prospective victims as more traditional threats.

It's important to note that we are not saying that data breaches, ransomware, CEO Fraud/BEC and the host of other threats that organizations face are going away – they most definitely are not. However, it is important to understand the cybercrime is an industry, and like any industry that wants to thrive over the long term, its methods adapt to changing market conditions and "customer" behaviors.

LOW-COST TOOLS ARE EASY TO ACQUIRE

Amateurs and hobbyists can become cybercriminals with minimal knowledge of their "craft" by acquiring any of the growing number of ransomware and phishing tools available at low cost. As just one example, the Karmen Cryptolocker ransomware variant that can be traced to ransomware infections as early as December 2016 is a ransomware-as-a-service offering and can be purchased for just $175[xxii]. Karmen has some sophisticated features, such as the ability to delete its decryptor if it detects analysis software or a sandbox on a prospective victim's computer, a decent interface that allows non-technical perpetrators to modify it, and a "Clients" page that permits cybercriminals to track the number of infected computers and the status of victims' ransom payments.

The result of tools like Karmen has been an increase in ransomware and other exploits coming from a large group of amateur cybercriminals, adding to the already significant problem from professional cybercriminal organizations.

THREATS ARE BECOMING MORE SOPHISTICATED

Phishing, spearphishing and other threats have become more sophisticated over time. From the relatively crude phishing attempts that tried to trick gullible users into clicking on a malicious link or open a malicious attachment, there has evolved sophisticated CEO Fraud/BEC attacks in which hackers will infiltrate an organization's network, study their business processes, and then launch attacks aimed at specific senior executives. For example, a cybercriminal can infiltrate a corporate network undetected; search for things like wire transfer timing, amounts of these transfers and their recipients; executives' travel schedules; etc. and then craft a whaling attempt against a CFO with the goal of tricking him or her into transferring a large sum directly to the cybercriminal. These types of malware-less threats are becoming more common and are more difficult to detect using conventional security technologies – a SANS survey from mid-2017 found that nearly one-third of the organizations it surveyed have experienced some type of malware-less threat[xxiii].

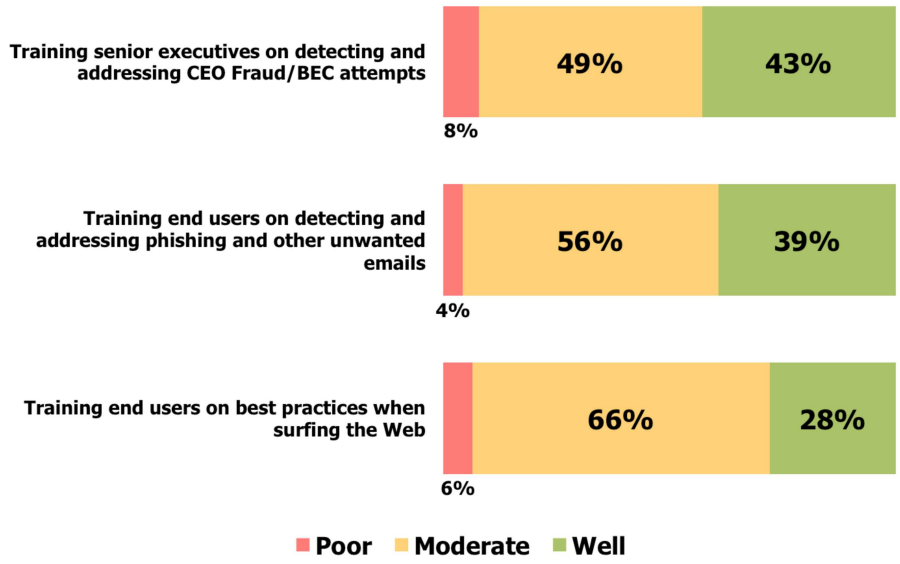
In short, the potential damage associated with phishing, spearphishing, CEO Fraud/BEC and ransomware are going to get worse without appropriate solutions and processes to defend against them.

USERS ARE A WEAK LINK IN THE SECURITY CHAIN

A key problem with cybersecurity – and an important reason that these attacks are successful – is the victims themselves. A large proportion of users are not properly trained about how to recognize threats like phishing, spearphishing, CEO Fraud/BEC, or ransomware attempts, and so they commonly fall for attacks by clicking on links or opening attachments in emails without thinking about the potential for harm that can result. For example, the survey conducted for this white paper found that six percent of users never receive any type of security awareness training, while another 33 percent receive this type of training only once per year or when they join the company. Even among those that do receive more frequent security awareness training, the results are fairly unimpressive: as shown in Figure 4, a minority of security-focused decision makers and influencers don't believe that their current training regimen is all that effective.

....the potential damage associated with phishing, spearphishing, CEO Fraud/BEC and ransom-ware are going to get worse without appropriate solutions and processes to defend against them.

Figure 4
Organizations' Effectiveness With Regard to Employee Training



Source: Osterman Research, Inc.

It's important to note that the fairly low effectiveness of security awareness training should not be interpreted as a knock on the concept of this training, but rather the way that many organizations implement it. For example, our research found that 65 percent of organizations will occasionally or commonly use the "Break-Room Approach" or the "Monthly Security Video Approach" to security awareness training, neither of which are as effective as the more sophisticated types of training that are available from a number of specialist providers.

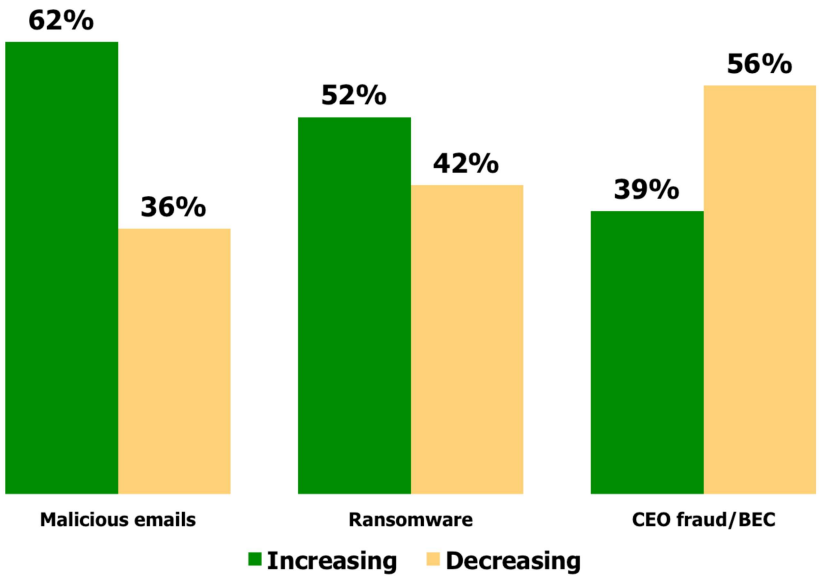
Without adequate training, many users will not be sufficiently skeptical of potential threats, particularly if these are delivered through social media channels, web advertising or text messaging that are implicitly assumed to be more trustworthy (or at least less suspect) than email or the web. At its core, the result of poor or inadequate training is that IT and security lack confidence in their users' ability to recognize incoming threats or in their organizations' ability to stop phishing and related incursions. For example, the survey conducted for this white paper asked respondents how confident they are that their organizations' users are well trained to recognize phishing and targeted email attacks that attempt to steal credentials: only 32 percent responded that they have relatively high or high confidence in their users in this regard.

Security Needs to Improve

SECURITY IS NOT IMPROVING AS IT SHOULD

Our research discovered some good news and some bad news with regard to the effectiveness of security solutions that have been deployed. As shown in Figure 5, 62 percent of organizations responded that their current security solutions are getting better at blocking malicious emails, 52 percent said that their anti-ransomware solutions are improving, but only 39 percent told us that their ability to block CEO Fraud/BEC attempts is improving. By contrast, the proportion of organizations that reported their security solutions are getting worse or not improving increases with the severity of the threat.

Figure 5
Perceived Effectiveness of Current Security Solutions
Percentage Responding "Very Good" or "Excellent"



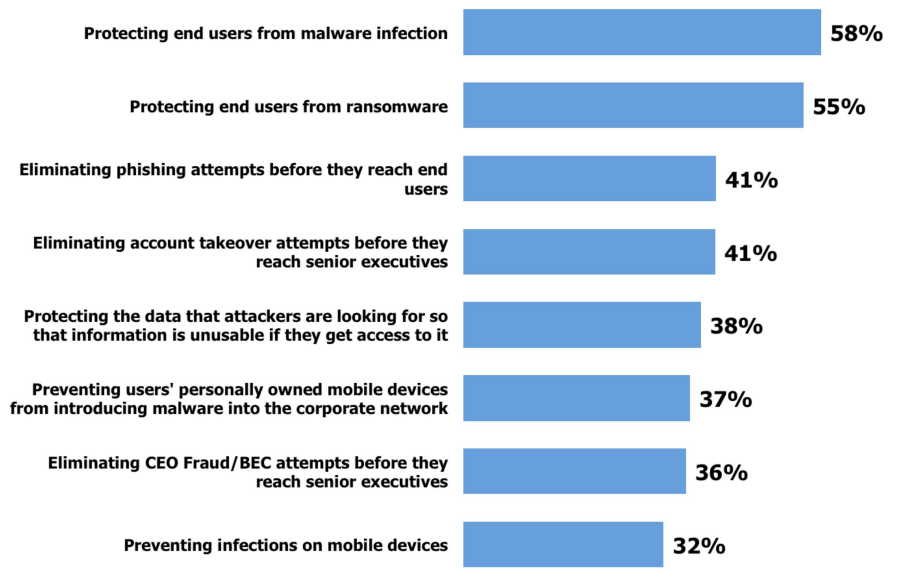
Source: Osterman Research, Inc.

HOW EFFECTIVE ARE CURRENT SOLUTIONS?

Our survey also asked respondents to rate the effectiveness of their various cybersecurity solutions and training practices. As shown in Figure 6, 58 percent of those surveyed believe that their current solutions to eliminate malware before it reaches end users are either "very good" or "excellent", and 55 percent believe that their ability to protect users from ransomware are this effective. Unfortunately, things get worse from there: fewer than one-half of respondents believe their ability to block phishing attempts from end users, eliminate account takeover attempts before they reach senior executives, and protect sensitive data is either "very good" or "excellent".

....fewer than one-half of respondents believe their ability to...eliminate account takeover attempts before they reach senior executives...is either "very good" or "excellent".

Figure 6
Perceived Effectiveness of Current Security Solutions
Percentage Responding "Very Good" or "Excellent"



Source: Osterman Research, Inc.

PREVENTING ADVANCED ATTACKS IS ESSENTIAL

There are serious consequences that can result from targeted email attacks: direct financial losses and loss of intellectual property like trade secrets or proprietary plans, among other problems, as per the examples below:

- During the last week of April 2017, Southern Oregon University sent a wire payment of $1.9 million to what it thought was its contractor, Andersen Construction, for the latter's work on the university's new pavilion and student recreation center project. Three business days after the payment was sent, the construction company reported that it never received the funds. An investigation revealed that the university was the victim of a CEO Fraud/BEC attack.

- France-based Etna Industrie, a 50-person industrial equipment manufacturer, fell victim to CEO Fraud/BEC using a combination of telephone calls and emails during a one-hour period in early 2016. In the attack, a cybercriminal telephoned the company's accountant indicating that she would receive instructions about a highly confidential transaction in which Etna was to acquire a company in Cyprus. Shortly thereafter, the accountant received an email purportedly from the company's CEO with additional information. All told, the accountant received about 10 emails and several phone calls during a one-hour period and eventually transferred €500,000 to bank accounts outside of France[xxiv].

- In March 2016, an employee of Alpha Payroll received an email supposedly from the company's CEO, requesting copies of every W-2 form that the company had created for its customers for the 2015 tax year. The cybercriminal's email contained embedded commands that rerouted the victim's response containing the W-2 forms. The company discovered the breach after one its customers reported that a fraudulent tax return had been filed using its information. Alpha Payroll investigated the incident and the employee who sent the information was subsequently fired[xxv].

- In December 2016, three hackers targeted seven New York-based law firms in an attempt to install malware within their networks, and successfully did so in

two of them. Their goal was to obtain confidential information on planned mergers from these firms' web and email servers, which they would then use to purchase stocks in the affected companies. They were successful in doing so and earned more than $4 million from their insider trading activities. The Securities and Exchange Commission charged the three hackers, and a judgment handed down by the Southern District Court of New York in May 2017 fined the three $8.8 million, required them to return their illegal gains, and required the mother of one of the defendant's to return $900,000 in funds she was holding for her son. As of this writing, the three cybercriminals may also face prison time[xxvi].

- China's J-20 stealth fighter is markedly similar to the Lockheed Martin F-22 Raptor and for good reason: a Chinese national worked with two Chinese military officers to install malware on the computers of Boeing and Lockheed Martin employees, using the malware to exfiltrate sensitive and confidential files that were then sold to Chinese companies. The individual who worked with the Chinese military was apprehended and in 2016 was sentenced to four years in prison after being charged with theft of trade secrets for the F-22, the Lockheed Martin F-35 Lightning II, and the Boeing C-17[xxvii].

- In April 2017, a systems administrator was charged by the FBI with creating malware that was designed to steal the encryption keys and source code of KCG Holdings, a San Jose, California-based company that develops trading algorithms for predicting stock market changes. The defendant stands accused of stealing more than three million sensitive and confidential files from his employer, and was discovered only accidentally after four months of his alleged activity[xxviii].

POST-DELIVERY PROTECTION IS ESSENTIAL

While the emphasis on security tends to focus on preventing phishing attempts, spearphishing attempts, malware and other threats from reaching end users, security must also focus on post-delivery protection because of the high likelihood that something bad will eventually get through even the most robust defenses. For example, frequent backups and snapshots should be used to rapidly recover from endpoints that become infected with various types of malware or ransomware, solutions must be implemented that will prevent detonated ransomware from encrypting backups, access control solutions should be implemented that will prevent the execution of malware, sandboxing should be used to evaluate suspicious file types, firewalls should be used to limit the ability of malware to connect to command-and-control servers, and so forth.

NATIVE SECURITY IS OFTEN NOT ADEQUATE

Many organizations rely on the native security that is included with their email system or other applications. However, these security capabilities often do not provide the same level of protection as third party solutions that are more specifically focused on threat detection and remediation. Let's use Microsoft Office 365, the most popular business-grade email and collaboration platform, as an example:

- Some customers report poor recognition of phishing attempts using Exchange Online Protection (EOP), Office 365's native security capability, including attacks that impersonate Microsoft products like Office 365, Outlook and SharePoint that contain links leading to dangerous payloads.

- EOP offers no specific whaling detection tool, so first stage-baiting messages are often delivered to end users who may answer them, thereby allowing the spammer to go to the next step.

- The default EOP configuration allows users to easily access their Office 365 junk folder and release any message. Once a message has been released, the user can then click on any dangerous link or open any dangerous attachment it may contain.

....security must also focus on post-delivery protection because of the high likelihood that something bad will eventually get through even the most robust defenses.

- Microsoft's more capable offering, Advanced Threat Protection (ATP), does not enable checking attachments and links for unknown and emerging threats by default – instead, an administrator must set up these capabiltiies.

- While ATP newly supports content at rest in SharePoint Online, OneDrive for Business and Microsoft Teams, not all content is actively scanned in place for embedded threats.

- ATP does not offer a whitelist or other integrated ability to mark particular domains as clear or safe.

The point in this section is not to criticize Microsoft's security-related shortcomings, but merely to illustrate that native security capabilities sometimes will not be adequate.

INCIDENT RESPONSE IS ESSENTIAL

Incident response is a critical component of any security capability, but these efforts can be time-consuming and difficult. Osterman Research has found that security teams spend the largest single share of time on identifying potential security threats, followed by gathering information about incidents and then resolving the security threats they introduce. Our research also found that:

- A typical security incident takes 10 hours to resolve, but for a large proportion of organization the process takes 16+ to resolve.

- We have found that when a typical security incident requires escalation to the next level of incident response, it takes 45 minutes for security analysts to process the incident.

A large and growing proportion of IT and security decision makers would like to adopt automated capabilities into the incident response process to shorten the resolution and escalation time required to manage security incidents, and to handle the more mundane and routine alarms they encounter.

THE NEED FOR DETAILED AND THOROUGH COMPLIANCE POLICIES AND REQUIREMENTS

Every organization needs detailed and thorough policies and procedures for protecting sensitive data and other assets. For example, these policies should include:

- Acceptable use policies for every communication, collaboration and file-sharing tool that will be used, including personally managed/owned devices, applications and services. This includes non-business tools, such as personal social media accounts.

- How employees should handle and share sensitive and confidential data, including encrypting and classifying this data, as well as the tools they can use to send and store this information.

- Password-management best practices, including password requirements, frequency of password changes, how passwords are stored, and so forth.

- Use of passphrases instead of passwords. For example, "MangoHawaii99" can be bruteforced using a typical home computer in about seven months, whereas "I ate mangos in Hawaii in 1999" would take 10,000+ centuries to crack[xxix].

- How frequently every system is backed up, including backup testing procedures.

- Implementation of dual-control procedures to ensure that a single employee cannot steal or delete highly sensitive data assets.

- Requirements for the use of at-rest and in-use encryption for every device, particularly mobile devices and laptops, and the ability to wipe them if they are lost or stolen – including personally owned devices.

- How and why sensitive data assets are made available via the corporate network and which should be air-gapped.

EXPECTATIONS FOR THE NEXT THREE YEARS

Osterman Research believes that sophisticated attacks will continue to increase as they have for the past several years, but that cryptomining exploits now represent a new and dangerous threat vector moving forward. Specifically, we anticipate that:

- Email will continue to be the primary threat vector for attacks on the enterprise.

- The number of phishing emails that contain links or attachments intended to distribute malware will continue to increase, but we will see significant growth in the use of malware-less threats.

- Spam will continue to be an effective tool for cybercriminals to distribute malware and social engineering attacks, and their use of spam will increase. For example, Trend Micro data shows that for the 17 months ending in late March 2018, there were worldwide spikes in spam volumes of up to 320 billion messages per day in September 2017[xxx].

- Cryptomining malware will see a rapid increase in 2018 as cybercriminals exploit corporate computing resources to mine for cryptocurrencies.

- Businesses, not individuals, will increasingly be the key target for phishing, ransomware and cryptomining malware because they have critical data that must be protected, they will have the resources to obtain cryptocurrencies to pay ransom demands, and they will be motivated to recover data assets that might fall victim to ransomware.

Best Practices to Consider

Osterman Research recommends a number of important security-related best practices that decision makers should seriously consider.

UNDERSTAND THE RISKS

Decision makers must understand the risks that their organizations face from phishing, spearphishing, CEO Fraud/BEC, ransomware, traditional malware, cryptomining malware, other threats and just dumb mistakes, and address them as a high priority. That seems obvious, but many decision makers give intellectual assent to the risks they face without taking them to heart. As just one example, in mid-2017 a developer with Tata Consultancy Services in Kolkata, India uploaded an enormous volume of internal reports, web banking code development plans, telephone records and other sensitive information for 10 financial services customers – including six Canadian banks and two US financial institutions – to a public GitHub repository[xxxi]. Tata's management clearly knew about the technologies and process that could have been put in place to prevent this occurrence, but did not implement the appropriate controls necessary to ensure that this was caught before it happened.

Decision makers must understand the risks that their organizations face...and address them as a high priority.

CONDUCT A THOROUGH AUDIT OF THE CURRENT SECURITY INFRASTRUCTURE, TRAINING PRACTICES AND CORPORATE AND COMPLIANCE POLICIES

Decision makers should conduct a complete audit of their current security infrastructure, including their security awareness training programs, the security solutions they have in place, and the processes they have implemented to remediate

security incidents. This is a key element in identifying the deficiencies that may (and probably do) exist, and it can be used to prioritize spending to fix the problems it finds.

CONSIDER A MULTI-LAYER APPROACH FOR EMAIL SECURITY

It is important to note that security solutions need advanced threat protection features because security is no longer simply about just spam and phishing campaigns. Advanced threats like ransomware, cryptojacking, zero-days, CEO Fraud/BEC, etc. are sophisticated, advanced threats that need advanced capabilities. These capabilities include attachment sandboxing and time-of-click URL analysis to complement the incumbent anti-spam and anti-malware for email hygiene.

VIEW SECURITY HOLISTICALLY

Security should be viewed as a holistic exercise, from the cloud services that are employed to detect and remediate threats all the way down to every endpoint solution. This doesn't mean single sourcing of a security infrastructure, but it does require that appropriate reporting and monitoring mechanisms be in place so that security teams can have a full understanding of their organizations' security posture in as close to real time as possible.

ESTABLISH DETAILED AND THOROUGH POLICIES

It is essential to develop policies for all of the email, Web, collaboration, social media, mobile and other solutions that IT departments have deployed or that they permit to be used by employees. Osterman Research recommends that an important step should be the establishment of detailed and thorough policies focused on the tools that are or will be used in the future. These policies should focus on the regulatory, legal, industry and other obligations to encrypt emails if they contain sensitive or confidential data; monitor all communication for malware that is sent to social media, blogs, and other venues; and control the use of personally owned devices that access corporate systems that house any kind of business content.

By themselves, policies will not ensure robust cybersecurity, but they can be a useful tool in limiting the number of tools that employees use when accessing corporate systems. These restrictions can be helpful in reducing the number of ingress points for malware, phishing and spearphishing attempts, as well as other content that might pose a risk.

IMPLEMENT AND REVISE COMPANY PROCEDURES

All organizations should implement and regularly update their company procedures about how sensitive and confidential data assets, as well as business-critical systems, are accessed and protected. For example, all organizations need an effective set of backup, restoration and testing procedures for their sensitive data assets so that they can recover quickly from a ransomware or other malware infection. Further, dual-control procedures should be implemented for access to critical data assets, especially those focused on financial transactions, so that a single, rogue employee cannot create a data breach or breach of cybersecurity.

IMPLEMENT BEST PRACTICES FOR USER BEHAVIOR

There are a number of best practices to address the cybersecurity gaps that might exist in the organization. For example:

- All employees, but especially senior executives who are more likely to be the target of a CEO Fraud/BEC attack, should be reminded regularly about the risks associated with oversharing information on social media. For example, sharing one's travel itinerary and business-class upgrades might impress a senior executive's friends, but it also provides cybercriminals with the opportunity to know they are more likely to be successful with a CEO Fraud/BEC or other attack.

- Any employee who deals with finances or sensitive data assets should have pre-established "backchannels", or out-of-band communication methods, provided to them for verifying sensitive requests. For example, if an accountant receives a request from the CEO to transfer money, as in the example of Etna Industrie discussed earlier, he or she should have an alternative method of contacting the CEO to verify the request. This might be a number that can be used to send a text message or make a phone call even if the CEO is on vacation, or it could be a designated person in the office who can verify the CEO's request.

- Employees should be required to use passwords that match the sensitivity and risk associated with the corporate assets they are accessing, and these passwords should be changed on a regular schedule enforced by IT.

- Software and operating systems should be kept 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 employees.

- Ensure that every employee maintains good endpoint defenses on their personal devices if there is any chance that these devices will access corporate resources like corporate email or databases with sensitive information. That includes employees' personally owned computers and devices if they access corporate resources while traveling or at home.

TRAIN ALL USERS, INCLUDING SENIOR EXECUTIVES

Every organization should have a robust security awareness training program that will enable users to make better judgments about the emails they receive, how they surf the web, how they use social media, and so forth. The goal of any security awareness training program is to help users to be more aware and more skeptical about what they receive in email, what they view on social media, and what they consider to be safe to access.

Every organization should have a robust security awareness training program that will enable users to make better judgments...

Security awareness training alone will not completely address an organization's cybersecurity threats, but it will improve the ability for users to be more aware of cybersecurity issues and make the organization less susceptible to ransomware, other malware attacks, phishing, spearphishing and CEO Fraud/BEC. It is essential to invest adequately in employee training so that the "human firewall" can provide a solid 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 cybercriminals and the consequences of their failure can be much greater.

It's important to note that security awareness training by itself will not be adequate to prevent all security threats, but it is an important component to protect against users clicking on phishing links, downloading malicious content, being tricked by CEO Fraud/BEC attacks, and the like.

CONSIDER THE GDPR AS A SECURITY ISSUE

The European Union's General Data Protection Regulation (GDPR) has two tiers of administrative fines for non-compliance (Article 83), which can be levied by a supervisory authority based on the type of infringement, rather than on a first, second, and subsequent infraction basis:

- The fine for lower level infringements is up to €10 million or up to two percent of the total worldwide annual turnover from the preceding financial year, whichever is higher. Infringements at this level include failing to enact data protection by design and by default (Article 25), failing to keep adequate records of processing activities (Article 30), and not ensuring appropriate security of processing (Article 32), among others.

- The higher level of fines is up to €20 million or four percent of total worldwide annual turnover, whichever is higher, and is for infringements such as failing to comply with the basic principles for processing, including conditions for consent (Article 5-7, and 9), not providing data subjects with their rights (Articles 12-22), and unauthorized or inappropriate transfers outside of the EU (Articles 44-49), among others.

Because data protection in the GDPR must be by "design and default", security will play prominently in any organization's approach to protecting their data assets.

DEPLOY ALTERNATIVES TO "SHADOW IT"

Most organizations permit employees to use their own smartphones, tablets, file-sharing accounts and cloud storage services. While this alleviates the burden on IT from having to provide all of these tools to users (or incur their wrath if they don't), it can create enormous security holes. As a result, it's important for IT to offer robust alternatives to the solutions that employees have deployed, or might want to deploy. This includes solutions for file-sync-and-share, voice-over-IP, cloud storage, real-time communications and other capabilities that employees use because they don't have an equivalent capability from IT, or because IT-provided solutions are not as good as the free or freemium solution that employees use. Providing an IT-approved solution that is as good as the solutions that employees have deployed on their own can enhance cybersecurity and give IT more control over corporate content.

OTHER ISSUES TO CONSIDER

1. **Keep systems up-to-date**
   All corporate systems are buggy and the vulnerabilities in applications, operating systems, plug-ins, devices and systems can allow cybercriminals to successfully infiltrate most corporate defenses. As a result, every application and system should be inspected for vulnerabilities and brought up-to-date using the latest patches from vendors. For example, just about every PC and Mac is (or was recently) vulnerable to Meltdown and Spectre[xxxii].

2. **Keep recent backups and verify them**
   The most effective way to recover from a ransomware attack, as well as from other types of malware infections, is to restore the infected endpoint(s) to a known good state, preferably as close to the most recent pre-infection state as possible. With a recent backup, an endpoint can be reimaged and its data restored with minimal data loss. While this strategy will probably result in some level of data loss because there will usually be a gap between the most recent backup and the time of reimaging, recent backups will minimize data loss if no other recovery solution can be found.

3. **Deploy good endpoint solutions**
   A number of good endpoint solutions can be deployed that can detect ransomware, other malware, phishing attempts, spearphishing attempts, data exfiltration and a variety of other threats. Every organization should deploy solutions that are appropriate to its cybersecurity 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 cybersecurity infrastructure because of its ability to reduce or prevent data breaches.

   In addition to good threat detection and remediation solutions at the endpoint, decision makers should also consider the use of virtual web browsers to largely eliminate the risks associated with standard browsers. A virtual browser prevents the execution of web code when users are using the web, and can eliminate exposure to a significant proportion of the threats that could impact a corporate network.

4. **Consider the risks inherent in the Internet of Things**
   The growing number of Internet of Things (IoT) devices pose a growing threat to any organization that has deployed these devices, or that has business partners that have deployed them. Decision makers may not want to give IoT security a high priority, but they need to have a well-considered security strategy to mitigate against malware infiltration and other consequences of unsecured IoT devices in their ecosystem. In the United States, the Federal Trade Commission and the Department of Homeland Security have plans to mandate that IoT devices have a security stack, but the time frame for implementation is not known as of this writing.

5. **Use adequate threat intelligence**
   Using historical and real-time threat intelligence to reduce the potential for infection can be a good way to reduce the likelihood of an attack or infection. Real-time threat intelligence can offer a good defense to protect against access to domains that are known to have a poor reputation and so are more likely to be used by cybercriminals for phishing, ransomware, spearphishing and other types of attack. Threat intelligence can also be used by cybersecurity analysts to investigate recent attacks and discover previously unknown threat sources. Moreover, historical threat intelligence can be useful in conducting cybercrime investigations.

6. **Protect all high value data**
   A sophisticated cyberattack always has the potential to penetrate even the best cyberdefenses. Consequently, organizations should protect their most valuable data so that if attackers get through, the information captured will be unusable. New encryption technologies like Format-Preserving Encryption (FPE) are easy to use, simple to maintain and can protect high value data at rest, in-use or in-motion, ensuring protection in all use cases. FPE has been standardized by the National Institute of Standards and Technology (NIST) of the US Department of Commerce.

7. **Encrypt sensitive and confidential email communications**
   The revelation of sensitive or confidential email communications has been key to some of the most high-profile data breaches. Organizations should broadly leverage email encryption for protection of all internal and external emails. Email encryption should be a standard tool for fighting phishing and other threats by making sensitive data useless to the attackers. A solution that encrypts email end-to-end, from originator to recipient on any desktop or mobile device, should be a key priority. Some email encryption solutions can also be used to encrypt all data flowing into a cloud-office application provider, including files used in collaboration.

8. **Consider using behavior analytics**
   Behavior analytics solutions examine the normal behavior patterns of employees across an organization and, when a divergence is noted an exception is raised for further investigation or access is immediately blocked. Unusual behavior could signal an employee about to leave the organization, a malware attack, the presence of compromised credentials or some other problem, thereby enabling early detection and risk mitigation.

Sponsor of This White Paper

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts. For more information, please visit us at http://www.malwarebytes.com/.

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. Marcin was recently named "CEO of the Year" in the Global Excellence awards and has been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and the Silicon Valley Business Journal's 40 Under 40 award, adding those to an Ernst & Young Entrepreneur of the Year Award.

www.malwarebytes.com
@Malwarebytes
info@malwarebytes.com

REFERENCES

[i] https://www.symantec.com/security-center/threat-report
[ii] https://www.darkreading.com/attacks-breaches/number-of-sites-hosting-cryptocurrency-miners-surges-725--in-4-months/d/d-id/1331176
[iii] https://www.symantec.com/security-center/threat-report
[iv] https://www.imperva.com/blog/2017/12/the-state-of-web-application-vulnerabilities-in-2017/
[v] https://www.symantec.com/security-center/threat-report
[vi] https://www.symantec.com/security_response/publications/monthlythreatreport.jsp
[vii] https://www.recordedfuture.com/ransomware-trends-2018/
[viii] https://www.spamcop.net/spamgraph.shtml?spamyear
[ix] https://www.justice.gov/opa/pr/former-owner-defense-contracting-businesses-sentenced-57-months-prison-illegally-exporting
[x] https://www.carbonite.com/blog/article/2017/08/the-evolution-of-a-cybercrime-a-timeline-of-ransomware-advances/
[xi] https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
[xii] https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
[xiii] https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
[xiv] https://www.helpnetsecurity.com/2017/11/02/ransomware-ransom/
[xv] https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/
[xvi] https://www.imperva.com/blog/2018/02/new-research-crypto-mining-drives-almost-90-remote-code-execution-attacks/
[xvii] https://www.symantec.com/security-center/threat-report
[xviii] https://www.darkreading.com/attacks-breaches/number-of-sites-hosting-cryptocurrency-miners-surges-725--in-4-months/d/d-id/1331176
[xix] http://www.thecrimson.com/article/2014/2/20/harvard-odyssey-dogecoin/
[xx] https://news.bitcoin.com/new-cryptocurrency-mining-bot-is-infesting-facebook-messenger/
[xxi] https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20
[xxii] https://www.recordedfuture.com/karmen-ransomware-variant/
[xxiii] https://www.prnewswire.com/news-releases/playing-whack-a-mole-results-of-the-2017-sans-threat-landscape-survey-300500286.html
[xxiv] http://www.bbc.com/news/business-35250678
[xxv] https://www.tripwire.com/state-of-security/latest-security-news/employee-terminated-after-falling-for-w-2-phishing-scam/
[xxvi] http://www.bbc.com/news/technology-39883224
[xxvii] https://world.wng.org/2018/01/copycat_crimes
[xxviii] https://www.cyberscoop.com/rogue-insider-charged-writing-malware-steal-wall-street-firms-crown-jewel-algorithms/
[xxix] Source: Kaspersky Secure Password Check (https://password.kaspersky.com)
[xxx] https://www.ers.trendmicro.com
[xxxi] https://www.theregister.co.uk/2017/06/12/tata_bank_code_github/
[xxxii] https://meltdownattack.com