A CISO's guide to

Phishing and Malware

Joel Rosenblatt

Brought to you by Proofpoint

securitycurrent

Security Current is an information and collaboration community. It improves the way security, privacy and risk executives collaborate to protect their organizations and their information. Its CISO-driven proprietary content and events provide insight, actionable advice and analysis giving executives the latest information to make knowledgeable decisions.

Copyright © 2016 Security Current

All Rights Reserved. For reprint permission contact:
201-835-9205 or write info@securitycurrent.com

securitycurrent

A
CISO's
guide to

Phishing and Malware

Joel Rosenblatt

Table of Contents

About the Author

Joel Rosenblatt is the Director of Computer and Network Security, Columbia Information Security Office. Joel oversees the computer security for all systems connected to the Columbia University Network.

Joel serves as the chairperson of the Security Metrics subcommittee of the Security Effective Practices committee of Educause. He is a member of Infragard and the NYECTF and active in other organizations that he can neither confirm nor deny the existence of.

Introduction

Chief information security officers (CISOs) face a gauntlet of evolving challenges to secure their enterprises. From complex infrastructure with legacy hardware and software to a lack of resources and a changing threat environment, a CISO's challenges are constant and ever present.

Hackers need to find only one vulnerability to exploit; the defender must defend against all possible threats. Regulations and litigation are increasing the stakes for companies and their CISOs, with data breaches becoming costly and fireable offenses.

The traditional perimeter defense model is ill-suited to the modern environment. Attackers no longer limit themselves to breaking into systems by compromising servers. They are now targeting employees, contractors, partners, and vendors directly with sophisticated scams. These attacks turn the everyday materials of the digital workplace — emails, files, and links to social posts and mobile apps — into weapons.

To protect against these attacks, CISOs must fortify the weakest link: their people. That means deploying practical tools to ensure users authorized to access networks or data become an organization's first line of defense, rather than a vector for attack.

A recent FBI analysis(1) shows that business email compromises rose 270 percent between January and August of 2015. Although the danger for enterprises has never been greater, users are demanding greater access, increased mobility, and less interference. The CISO must balance the opportunities provided by mobile computing and payments, the Internet of Things (or Internet of Everything), and cloud and infrastructure diversity with the additional security risks they pose.

Threats have become more significant, sophisticated and impactful. Many organizations continue to rely on legacy defenses, such as email security solutions that lean on anti-spam and antivirus (AV). These signature-based solutions have few, if any, controls for employee use of social media.

Threats introduced by social media, combined with a permissive approach to the countless apps downloaded onto employee smartphones and tablets, increase the likelihood that sensitive corporate data will be exposed far outside an organization's controls.

Furthermore, current malware largely slips past traditional defenses. Even the latest generation of commodity malware (like Dridex and Dyre) can evade the leading antivirus solutions more than 99% of the time. In a targeted attack with customized malware, the evasion can be close to 100% successful.

Many CISOs do not have adequate plans to deal with incidents and breaches. Disaster recovery, business continuity, and incident response planning are not always within their purview. Even when the CISO does have experience in these areas, it all too often takes a crisis to truly appreciate the importance of remaining proactive in terms of incident response.

About This Book

Today, cybercrime is very much a B2B affair with surging returns on investment. From a business perspective, there is always a number associated with a breach. For example, Columbia University calculates every exposed Social Security number costs organizations $195. This number represents only a fraction of the total cost; losses to the breached companies, the people whose data has been stolen, and to society as a whole aren't easily measured.

This book explores real-world examples of advanced targeted attacks via email and social media to show how these evolving threats are increasing an organization's business risks. It is written with the CISO in mind. More specifically, it explores attack vectors such as email that are being exploited as never before and presents ways CISOs can confront those increasing risks.

TRADITIONAL

MALWARE

SECURITY

Traditional Security

Understanding Today's Changing Malware Environment

Malware has come a long way since 1983, when Fred Cohen, then a student at the University of California, developed the first computer virus.

The first mass attack by computer malware occurred in 1988 when Cornell University graduate student Robert T. Morris, son of the chief scientist of the NSA's National Computer Security Center, launched what is known as the "Morris Worm." The worm broke into thousands of Internet-connected machines and replicated itself, slowing these machines down.

Malware has since developed from a hacker "proof of concept" to an annoyance to a major source of fraud, intellectual property theft, and espionage. Today, it is the bane of every CISO.

The vast majority of successful attacks originate with self-replicating malware (like Morris) or malware injected through phishing, email-based attacks that trick users into helping infect their own machines by opening bad attachments or clicking a malicious link.

Malware is becoming increasingly difficult to prevent and detect. In its initial "worm" phase, it was a hacker's hobby, an intellectual exercise. Worms such as I LOVE YOU, Code Red and SQL Slammer had the ability to crawl through networks and reproduce, wreaking havoc in a very short time. But for the most part, they did not steal information or defraud organizations or people.

As world commerce became more digital and online exploits became increasingly profitable, attackers became more sophisticated and "professional."

For this reason, with the exception of pointedly targeted attacks, more dangerous forms of malware have largely supplanted network-based worms.

Today's malware of choice has changed. They're delivered using slick marketing techniques and advanced, multi-stage design. Call it Madison Avenue meets M.I.T.

Operating system vendors have been trying to fix systemic bugs, and the network layer has been hardened. But problems persist. Malware authors have turned their attacks on other entry points, such as active web content and ubiquitous media players, as demonstrated by the bug discovered in the Android OS in July 2015 that could take over a handset and let attackers steal anything on it.

Today's malware of choice has changed. Viruses and Trojans are nuggets of nastiness packaged to look like something that you or your employee really want. They're delivered using slick marketing techniques and advanced, multi-stage design. Call it Madison Avenue meets M.I.T. — this very complexity makes it so effective.

For attackers, the beauty of the multi-stage attack is that malicious entry is authorized. Apparently innocent offers entice the user to authorize attackers' access to the system. Once that authorized access is granted, the malware can do its dirty work in the background and often below the radar of anti-malware software.

Examining Current Threat Protection

Traditional antivirus programs at the core of many current AV solutions, such as McAfee, Kaspersky, and Norton, depend on a pre-defined signature, a sequence of bytes meant to be unique to a particular program, to find the virus and block it from running. These programs are plagued by false positives and the ease with which signatures can be invalidated.

As commercial AV programs became ubiquitous, the next phase of the cyber war started. Attackers adapted malware to be polymorphic — its code constantly changing to stay a step ahead of AV signatures. In addition, simple phishing attacks grew more sophisticated and began installing malware as the second stage of the attack, where the malicious nature of the code isn't as easily detected. These advances have made phishing one of today's most effective attacks.

One Phish, Two Phish…

Phishing comes in three major forms: regular, spear, and whale.

Some anti-spam tools can block up to 70 percent of regular phishing attacks. Specially crafted spear phishing messages, however, often make it through commercial spam tools. That's because they contain information specific to the organization and include names, graphics, and text that an employee would recognize.

Whale phishing involves highly targeted emails sent to management. These attacks, which are becoming more prominent, are refined, highly customized with personal information, and almost impossible to automatically discover and block.

Phishing email can be more dangerous than simple viruses because it often captures the credentials of the targeted person, giving the attackers broad and unfettered access to an organization's systems and applications.

Determining the Business Impact of Cyberattacks Resulting from Advanced Threat Campaigns

Willie Sutton's famous (and probably apocryphal) answer to the question "Why do you rob banks?" now applies to attackers: "Because that's where the money is."

When the goal of virus malware was simply to infect and spread, estimating damage was simple: count the number of infected machines and multiply that by the cost to restore the system. Today's advanced attacks are more lucrative, and the losses are more difficult to calculate.

Attackers do not even need to steal information to make money from it. They just need to control access to it.

Most users are unaware of the amount of vulnerable data they possess: financial credentials, medical identities, access to their employer's networks and accounts, and more. Email used to share business strategies, product designs, and merger or acquisition plans can be easily pilfered. Even an administrative assistant's contact list can be a roadmap to a successful spear phishing attack.

With today's powerful data-mining tools, hackers can steal data "wholesale" and then sell the gems they uncover "retail." Attackers do not even need to steal information to make money from it. They just need to control access to it. Popular programs such as CryptoLocker or CryptoWall hold data hostage for ransom — often in the form of untraceable Bitcoins — in exchange for the key to unencrypt the data.

Tallying the losses in this case is simple multiplication. If you have backups, it is the cost of a simple rebuild and restore, multiplied by the number of infected systems. If you do not have a backup, as is

often the case, then you need to pay the ransom and hope the keys provided actually work.

The loss calculation gets more complicated if the keys do not work or if you try to retrieve the information from versions saved on other machines and users' memories. Some organizations just write off the value of the data on an infected machine and move on. But this is not always possible and depends largely on what data attackers are holding ransom.

Organizations should ask themselves how much it would cost to recreate lost work — if they could do it at all. In some cases, an entire company could be irreparably damaged if its data cannot be recovered.

In other attacks, the goal is exfiltrating corporate data. High profile attacks for this purpose have been reported, including the hack of the U.S. government's Office of Personnel Management (OPM)(2), which exposed more than 20 million records and is believed to have started as a phishing attack.

THE NEW

PHISHING

PARADIGM

Chapter 2

The New Paradigm

Today's attackers are highly motivated, sophisticated "businesses" that employ highly skilled computer professionals to break into enterprises. Bad actors range from organized crime to terrorist organizations to foreign governments, sometimes working in tandem.

The economics of these campaigns have also evolved. Instead of regular phishing attack, trying to steal information in small units (e.g. an ID/password), each yielding a few hundred to a few thousand dollars, the objective today is to extract millions and scale up the damage done to hundreds of millions. What's more, hacking has become sensationalized with some attackers now seeking fame along with the cash.

As the return on investment has increased, the bad guys can spend a lot of money to create the perfect attack. They have the means to hire a team of programmers to build custom malware. Because this malware has never been used before, signature-based defenses such as AV don't catch it.

Writing even the most malicious software is not illegal; only using it is. Many exploits have been identified when the attacker is "testing it out" prior to launching a full-scale campaign.

Attackers' "research and development" is also becoming more sophisticated. Gathering intelligence for a complex whale phishing attack includes hiring researchers to study the "mark" using social media and even surveillance. The goal: crafting a detailed and believable phish.

Another kind of attack known as "business email compromise (BEC)," or impostor email threats, has dramatically increased in recent months. In these attacks, threat actors research the financial and organizational structure of the business. Then they send the CFO, treasurer, or anyone else who can transfer company funds an email from the CEO or president requesting an emergency wire transfer.

Other times, the attacker asks for the wire transfer details over the email rather than instruct the recipient to initiate it; no malware or links are generally involved.

The BEC scam continues to grow and evolve and it targets businesses of all sizes. According to the FBI(3), from October 2013 to August 2015 the total U.S. exposed dollar loss was more than $747 million.

These totals, combined with those identified by international law enforcement agencies during this same time period, bring BEC-related losses to over $1.2 billion.

The following BEC statistics were reported to the Internet Crime Complaint Center from **October 2013 to August 2015:**

Total U.S. Victims:	**7,066**
Total U.S. exposed[1] dollar loss:	$747,659,840.63
Total non-U.S. Victims:	**1,113**
Total non-U.S. exposed dollar loss:	$51,238,118.62
Combined Victims:	**8,179**
Combined exposed dollar loss:	$798,897,959.25

1. Exposed dollar loss includes actual and attempted loss in United States dollars

How Social Engineering Is a Game Changer

The social engineer, the digital con artist, is a most worrisome attacker. Kevin Mitnick, a reformed computer hacker and social engineer, says it is much easier to trick someone into giving up his or her password than to hack into the computer system.[1]

Social engineering is the art of using psychology to create an almost irresistible urge on the part of the recipient to open the mail and do what it says, despite any latent suspicions.

One well-known and effective method to elicit passwords and login IDs involves calling the target and pretending to be the IT repair technician. While highly effective, this technique is labor intensive and ill-suited to the size of most email attack campaigns.

To compromise hundreds, if not thousands, of machines, con artists developed mass mail spamming, eventually using botnets as the sending service to ratchet up effectiveness. Botnets are used to send the mail to confuse anti-spam systems, as the sending IP address is only used to send a few messages, not allowing the system to recognize the threat.

1 http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

REAL WORLD

CHALLENGES

EXAMPLE

Chapter 3

Real World Example

The following case study features a real Proofpoint user and illustrates how advanced email protection can help stop and mitigate email attacks.

Case Study: Leading University and Medical Center

Business Challenge

Universities often pose a unique challenge for email administrators. Many have both a university environment and a medical environment. And within these entities, sub-departments may not be universally managed.

At our university, we act in many ways as an ISP. While we host a central email system for both our university and medical center, we also provide Mail Exchange (MX services) record services for over a hundred other entities. Many of these are small departments with their own mail systems, while others are simply domains for which we provide address-rewriting services.

Our business challenge when selecting a mail security vendor was to find a product that would effectively filter our spam, protect us from phishing, keep us relatively free from threats entering via email, and be customizable to the needs of our robust environment. We needed to meet these challenges at a price that made sense.

Technology Challenge

Our technical challenges mostly stemmed from a lack of structure once email enters our environment. Our main domain is not authoritative on any single mail system and, as such, email directed to it could eventually deliver to a handful of systems. This caused us to create a routing layer in our perimeter that is used for address translation. Likewise, we have a large number of mail servers that are not directly reachable even from our main mail servers. This creates a situation where we have comprehensive routing tables on the perimeter.

A second technical challenge was being able to apply policy to a subset of users. Our medical center users are required to have their mail route through a data loss prevention (DLP) solution, while university users are not bound by this policy. As we continued to merge email domains, identification via sender domain is becoming a method we could no longer rely upon.

Finally, a third and important challenge we faced was the continued phishing campaigns against our users. The reasons for attempting credential compromise are many; however, we found that most often phishing messages would come in and credentials would be compromised -- so accounts could then be used to send outbound phishing mail to other organizations. This is not unique to us. But the ease with which the phishing messages were entering our environment and the inability to stop them from going out continued to be a problem and provided an environment for spam/phishers to continue their abuse.

Solution

We trialed two other vendor solutions prior to selecting Proofpoint. Due to the structure of our organization, we were able to demo these products in a live environment. We configured the trial solution to complement our existing environment and added a handful of hosts into our load-balanced environment. This allowed us to demo live traffic and see the results side by side. It also allowed for a good comparison between vendors.

Proofpoint did the best job of blocking based on message analysis and was competitive in blocking based on sender reputation. The interesting comparisons came with the phishing messages that entered the environment during this time. Due to the way we distributed messages, we found that the Proofpoint scanners blocked phishing messages that made it through our existing environment.

We took care of the routing challenge, for the most part, using the existing supported configurations. Our medical environment, as noted earlier has access to some hosts that our university environment does not. Additionally, there are numerous aliases that exist only within that environment. For this, we setup a unique cluster. The medical center had a number of web forms that were used for management of these aliases and routing tables. Through a root access agreement, we were able to write a few custom scripts that allowed us to push these configurations from our existing web management tools to our cluster.

We chose Proofpoint's Email Protection solution. Proofpoint did the best job of blocking based on message analysis...

Business Value

We chose Proofpoint's Email Protection solution. The licensing agreement allowed us to run as many virtual appliances as we needed. Proofpoint was realistic, and very conservative, in helping us determine the sizing for our environment. In the end we deployed double their recommendation so that we could support our full load in a single datacenter if we were to lose connectivity to our second active datacenter. Additionally, as previously mentioned we deployed a second small cluster to handle primarily MTA (Message Transfer Agent) services in our medical center. A third cluster was installed as a test environment.

Once we were fully setup and deployed, adding agents became a trivial procedure for us that certainly adds value to the product. We are able to build and deploy additional servers from scratch in approximately 60-90 minutes. Being able to respond fairly quickly like this is a great benefit to us.

Since deployment of Proofpoint, our phishing messages have dropped considerably. We now rarely respond to a phishing threat because the number that makes it through has dropped to almost nothing. When one of these messages has made it through, Proofpoint has been quick to respond and teach their filters so these messages are stopped going forward.

Furthermore, we have seen very good results in spam detection with a minimum number of false positives. While we have reported several false positives, support has been quick to respond and correct on the fly. Subsequent scoring of these messages would allow them through without issue.

Based on the results we are seeing in spam/phishing protection, I believe Proofpoint is the leader in this protection dollar-for-dollar. We paid approximately the same amount for our previous product and received more phishing and spam emails with less features and inferior support.

Technology Benefits

The phishing and credential compromise issue was aided in a second way due to Proofpoint technology. Due to its better scanning capabilities, Proofpoint also began detecting the outbound emails following a compromise as spam/phish. This created an environment where less of the garbage left our environment.

The built-in rate limiting based on quality of the messages kicked in. This technology looks at things such as spam scores and bounced messages due to invalid recipients. The outbound spam behavior

consisted of both of these. Many messages were considered spam and also attempted deliveries to invalid recipients. Due to this, the outbound messages were throttled, which created an environment that is not very productive to a spammer; therefore, our target as an inbound threat was lowered because the ability to capitalize on compromised credentials for spam has also been lowered.

The ability to use SAML2 as an authentication method for both administrators and end-users keeps our IT Security office happy.

The email firewall rules are very configurable and can come in quite handy for auditing your environment as well as protecting it. For example, we were encouraged to implement a rule which looks for email coming inbound from senders using our domain name in the From address or as the envelope sender. This rule simply captures a copy of this message as a potential spoofed message so we can evaluate it later, if desired. We included a whitelist for known outside senders — think marketing mailers — but now have greater visibility into the messages purportedly sent by us from external sources.

Another benefit is Proofpoint's willingness to help you configure the environment for your specific use cases. Even at the support level, if you are trying to do something a bit out of the ordinary, they are willing to help. For instance, I was having trouble getting a configuration synchronization working properly when initiated via a script from the command line. This is something they typically do not support. But the tech support person was willing, and able, to find the proper command for me to run to accomplish what I was after. The alternative I have seen with other vendors is simply a response of, "That is not a supported method." This willingness to function like a partner and help us accomplish our goals is of great value to us.


TODAY'S
PROTECT
ENTERPRISE

Chapter 4

What is Needed to Protect Today's Enterprise

In the mainframe days, computer security and physical security were closely related. Securing physical access to servers and workstations went a long way toward preventing data theft.

In the network age, attackers can steal data without ever stepping foot in the same state or even the same country.

Initially, network-enabled system break-ins worked because the underlying network architecture and operating system had vulnerabilities. This let attackers use specially crafted network packets to compromise systems and create an administrative account giving them access to data.

In today's world, a mature OS is not easily hacked through a network connection without the help of a vulnerable application.

This leaves two major types of potential entry points: vulnerabilities in the network-facing applications and exploits from compromised credentials.

An example of the first case would be a web-based form that is open to an SQL injection attack because of inadequate secure coding and applications testing.

Exploits from compromised credentials are much more complicated. To the system, the access appears to be legitimate. The credentials are indeed valid; it is the attacker who is not.

Innovations in Advanced Threat Protection

Detecting advanced threats requires information that cannot be gathered solely from the local enterprise, such as identifying machines that are part of a botnet. Without the address of the command-and-control (C&C) node, traffic from an individual machine going to a remote location cannot be deemed suspicious.

Many advanced defenses benefit from threat information collected and shared by similar systems deployed over a large number of sites. By pooling and correlating information collected over a large number of systems, such defenses can find patterns in messages and block malicious emails that less intelligent tools miss.

Any high-end threat analysis tool will be able to collect and share information and use that collective intelligence to prevent attacks.

Staying Ahead of Attackers

The first step in preventing an attack is recognizing that one is occurring. This sounds obvious, but a modern attacker can breach your system and steal data before you are aware that anything is amiss. That means you must monitor the network constantly, including collecting and monitoring logs for evidence of abnormal activity and follow-up to rule out breaches and/or successful exploits.

Some attacks against your enterprise are easily spotted, such as distributed denial-of-service attacks (DDoS), ransomware, or any other attack that prevents the organization from functioning. Today's attack of choice, via social engineering, is less obvious.

Theft-of-information attacks hurt the company and the customers whose information is compromised. They often start in the email system of the company or one of its partners.

In the Target breach, a simple phishing scheme enabled the attacker to penetrate one of the nation's largest retailers. The HVAC vendor had access to the Target network, giving attackers the ability to exploit a vulnerability of the contractor's system to escalate network privileges and gain access to the system that Target used to distribute updates to their point-of-sale (POS) systems. Once the POS terminals were compromised, the attackers could steal crucial information from millions of credit cards.

Any high-end threat analysis tool will be able to collect and share information and use that collective intelligence to prevent attacks.

The lesson: a company must look not only at its own systems, but at the systems of critical vendors to ensure their access is restricted specifically to what they require. Your security is only as strong as theirs.

Attacks using email to target corporate officers depend on the fact that most executives are busy people, often unable to verify the authenticity of an email or link. While CISOs must educate their users (often not an easy process), combining education with today's existing tools is business-critical. Automated controls that can detect these attacks and prevent that fatal click or block that URL have never been more crucial.

What Staying Ahead of the Attackers Means to Your Enterprise

Today's businesses face many challenges. Technology is ubiquitous, and your customers expect you to use it effectively to serve them. The ease of use and 24/7 availability is practically a requirement before the first product rolls out the door.

In the rush to get to market, some organizations overlook or minimize the need to secure their essential systems. They treat security as an afterthought, something you add after everything is up and running. They shouldn't.

Security is not a zero sum game. There is no perfect security. The name of the game is assessing business risk and mitigating it relative to your environment.

The pressure that enterprises are under to provide more Internet-based services is palpable. Attackers know this. Though they are clever and leverage advanced threats, they seek the easiest link to penetrate an organization. In most cases, that link is people through social engineering and phishing attacks.

Organizations shouldn't wait until they are breached to act — in most cases, cyber-attacks aren't discovered for months, long after the damage is done. To protect their people, data, and brand, executives and boards of directors need to provide CISOs the tools they need to build in security from the outset. When that is not possible, they should assess the weakest links and secure them.

Security is not a zero sum game. There is no perfect security. The name of the game is assessing business risk and mitigating it relative to your environment.


REDUCING
PROOFPOINT
THE THREAT

Chapter 5

Reducing the Threat with Proofpoint

Email-borne attacks — in the form of weaponized file attachments, malicious links, wire-transfer fraud and credential phishing — are the No. 1 threat vector for most organizations.

Today's sophisticated email attacks require a full-lifecycle strategy that includes real-time threat intelligence, automated threat response, dynamic malware analysis, and sophisticated email filtering. Powered by its patented Proofpoint MLX machine learning technology, Proofpoint's anti-spam and anti-phishing technology efficiently filters millions of possible attributes in every email. This advanced-level scanning protection accurately filters emails by examining envelope headers and structure, content, email sender reputation, images and more, to prevent spam emails, malware, other malicious email and attachment-based spam from reaching inboxes.

New Defense for a New Generation of Attacks

Threats come in two major types: known and unknown. Known threats, while easier to detect, can still cripple organizations not properly prepared to block and contain the attacks before they can infect machines or compromise credentials.

Email systems, which are a key attack vector, must have the most advanced phishing protection and anti-spam capabilities or the business will be open to a vast array of infiltrators and dangerous files.

Unknown threats — those that have never been seen before — can pass undetected through conventional filters. In many cases, the phish has been crafted to either bypass detection or instill enough

confidence that the recipient is willing to click on the included link or answer with the requested information.

Proofpoint Enterprise Protection uses signature-based antivirus and behavioral-based zero-hour detection technologies to protect against all types of malware, known and unknown. It detects and responds to threats in their earliest stages to keep email users safe from all types of malicious code.

Next-Generation Cloud-Based Cybersecurity

The ability to leverage the cloud is becoming an essential component of today's advanced threat detection models. The power to correlate data from many different sources around the world is a necessary advantage, especially when processing email. Spam and phishing email often come from botnets, making it hard to block the IP addresses used to send them.

Proofpoint enterprise applications are delivered on a cloud infrastructure. As such, they can be deployed as secure, cloud-only solutions, or as hybrid email services that combine SaaS with optional physical or virtual points-of-presence installed behind the enterprise firewall for customers looking to keep certain functions inside their security perimeter.

These options give customers heightened security of all customer data and processing capabilities, while leveraging the lower total cost-of-ownership and efficiency benefits of cloud computing.

Securing Big Data and Advanced Threat Intelligence

Advanced threat analytics are another essential feature of a state-of-the-art malware protection system. Using the cloud to look for similar attacks against multiple locations (statistical analysis or "big data") and advanced sandboxing, Proofpoint can detect zero-day malware and stop it before it gets to vulnerable workstations.

Built from the ground up on the latest cloud and big data technologies, Proofpoint solutions offer:

- Innovation that keeps pace with the latest advanced threats
- The ability to scale up to even the largest, most complex global organizations
- Compelling time to value and total cost of ownership

Dynamic Malware Analysis

A favored technique of malware creators is polymorphic code. This introduces small changes that don't affect the code's behavior but do give it a new software "fingerprint" to throw off traditional signature-based antivirus and common blocking and detection solutions.

Zero-day threats, so named because they are so new that organizations have "zero days" to patch vulnerable systems, evade traditional systems equally well. To reduce these risks, an advanced detection system must employ technologies that discover malware based on its behavior — not just its signature — using advanced sandboxing, static analysis, and statistical analysis. Other techniques such as heuristic scanning discover and protect against currently unknown threats providing enhanced security and reassurance.

Proofpoint employs these advanced techniques as part of its Targeted Attack Protection (TAP) platform.

Key Technology Benefits

By reducing or preventing malicious email from reaching employees, organizations greatly reduce the potential attack surface. Almost all current breaches can be traced back to an email received by an employee that was used to install a backdoor into the network.

Securing your organization means protecting your employees; many of them are gateways to critical business information. Email is not just a means to transmit information but, without proper protection, a way to gain unfettered access to your critical data.

Proofpoint is used by thousands of the world's most successful organizations, including more than half of the Fortune 100.

Proofpoint:

- Blocks mass email attacks to detect targeted attacks, which are indicators of more serious compromises by a knowledgeable foe
- Identifies high-value human targets based on their role and the applications and data they have access to
- Identifies people in your organizations who click things they shouldn't
- Intelligently responds to specific targeted attacks, including:
    - Scanning the actual URLs to determine whether the website is hosting malicious content before a user is granted access
    - Predictive sandboxing suspect URLs and attachments to test their payloads before users are allowed to access
- Employs a heuristic approach including the ability to automatically update email security and malware detection systems to include new signatures
- Continuously improves the collection of threat intelligence and data analysis

Key Business Benefits

Phishing attacks via email, social media and file sharing are on the rise, with attackers focused on end-user accounts and sensitive data. New laws, industry standards, and litigation means the stakes have never been higher. For companies, CISOs and even CEOs, breaches are becoming fireable offenses.

The Proofpoint solution:

- Provides peace of mind and guaranteed performance allowing users to focus on their business
- Saves time, costs, and resources normally wasted on unwanted email
- Protects corporate bandwidth for web, VoIP, and other critical systems
- Delivers effective defense from threats and manages threats away from your network with no hardware or software required
- Updates in real time to protect against new and emerging threats

1. "Internet Crime Complaint Center (IC3) | Business Email Compromise. "*Internet Crime Complaint Center (IC3) | Business Email Compromise*. Department of Justice, 27 Aug. 2015. Web. 01 Feb. 2016. https://www.ic3.gov/media/2015/150827-1.aspx.

2. Gallagher, Sean. "Why the "biggest Government Hack Ever" Got past the Feds." *Ars Technica*. Condé Nast, 8 June 2015. Web. 01 Feb. 2016. http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

3. "Internet Crime Complaint Center (IC3) | Business Email Compromise. "*Internet Crime Complaint Center (IC3) | Business Email Compromise*. Department of Justice, 27 Aug. 2015. Web. 01 Feb. 2016. https://www.ic3.gov/media/2015/150827-1.aspx.

A CISO's view...

Napa County CISO Gary Coverdale:

"As a CISO and participant in cyber-knowledge sharing and collaboration at the local, regional, and national levels, I fully understand the need for deploying aggressive cyber hygiene. The adage of count, configure, protect, and patch all technology assets in your organization represents the really low-hanging fruit when it comes to protecting your organization from security breaches.

"In addition to these best practices, email hygiene is a must for safeguarding your organization from both external and internal threats.

"As CISO for Napa County, I led my team's evaluation of several different solutions. And in the end, we selected and implemented Proofpoint as our mail hygiene product. Using Proofpoint has minimized our threat "opportunities" by reviewing and stripping any potentially suspect package, or link loaded or contained, within the email. This includes phishing attempts on our staff.

"Because of Proofpoint we have not had any ransomware or CryptoLocker breaches on our systems while other public agencies surrounding Napa have been targeted and successfully compromised with these types of phishing attacks. Those breaches were quite costly to resolve and/or resulted in a loss of important data.

"As all security and privacy executives know , all the security-awareness programs in the world are not going to prevent that one staff member from falling victim to an aggressive phish. That is why Proofpoint is so important as part of Napa County's security quiver of tools. It is beneficial to prevent loaded malware packages from being delivered to our users, but equally as important, Proofpoint prevents any of our staff from having the ability to be persuaded to click that one link that might compromise the organization."

"This ebook provides valuable insight regarding the importance of the risk to the Human Element, as phishing is the gateway to many compromises that cripple organizations internally and damage the brand."

-Brian Lozada, Duff & Phelps CISO

securitycurrent