Phishing Incident Response

How to Eliminate Noise Leveraging Internal Attack Intelligence

ISMG
INFORMATION SECURITY
MEDIA GROUP

PHISHME

Executive Summary

This white paper will address the importance of implementing an incident response process that directly tackles phishing attacks and show how technologies designed specifically for phishing incidents can collect, organize and prioritize phishing intelligence from other systems, as well as from human reporting, to dramatically improve detection, prevention and mitigation of these types of attacks.

Introduction

Phishing attacks arguably are the most persistent—and pernicious—cyberattacks that organizations face.

In 2015, security solutions provider Trend Micro wrote that three-quarters of targeted attack attempts use email as an attack vector,[1] while the number of unique phishing websites increased 250 percent just between the final quarter of 2015 and the first quarter of 2016, according to the APWG (Anti-Phishing Working Group).[2] The Symantec 2016 Internet Security Threat Report revealed that spear-phishing campaigns targeting employees increased 55 percent.

More troubling to security practitioners, phishing attacks have grown more targeted and dangerous, as the variety of attack methods continue to evolve and the number of threat actors proliferate. In its latest Internet Security Threat Report,[3] Symantec also points out that a thriving criminal marketplace has made phishing campaigns easier to run:

> Attackers will cooperate, with some specializing in phishing kits, and others selling them on to other scammers who want to conduct phishing campaigns. These kits often trade for between US$2 and $10, and their users do not require much in the way of technical skills to operate them or customize their webpages to suit their needs. Scammers may use the data stolen from these attacks for their own purposes, or sell it on underground marketplaces for a profit.

Meanwhile, styles of phishing continue to metamorphose from scattershot emails sent to thousands of people at once to more targeted, effective methods like spear phishing, business email compromise and so-called "soft targeting," all of which leverage social engineering techniques to trick people to click on malware, send money or take a host of other actions that imperil the organization. And attackers have dramatically increased the malware payloads used in phishing attacks just in the last several months. As of March 31, 2016, PhishMe found that 93 percent of all phishing emails analyzed contained encryption ransomware,[4] up from 56 percent only three months earlier.[5]

The bottom line is that incident responders face constantly evolving challenges in preventing and mitigating phishing attacks. This paper explores those challenges and how to gather, organize, prioritize and ultimately leverage internal attack intelligence to stay ahead of attacks.

---

[1] Trend Micro. Spear Phishing 101: What Is Spear Phishing? (Trend Micro, September 24, 2015)

[2] APWG. Phishing Activity Trends Report, 1st Quarter 2016. (APWG, 2016)

[3] Symantec, Internet Security Threat Report, Volume 21. (Symantec, April 2016, 33)

[4] PhishMe. Q1 2016 Malware Review. (PhishMe, June 2016)

[5] Korolov, Maria. "93% of phishing emails are now ransomware." (CSO, June 1, 2016)

The Problem: Too Much Information, Not Enough Intelligence

Unlike other security challenges, phishing doesn't suffer from an awareness problem. Instead the problem incident responders face more has to do with the fact that phishing attacks get lost among a deluge of suspicious emails and system alerts that incident responders receive from multiple sources, including:

- Alerts from numerous technology sources, including perimeter, internal, and network-based systems within an enterprise environment; and
- Reports from employees and to a lesser extent, customers, partners and third-party vendors.

Although the alerts that are relayed from these multiple sources oftentimes report similar activity, incident responders too often find themselves chasing down a host of different symptoms because they don't have the tools to correlate the source of these alerts to a discrete phishing email. No single system captures all the information. An anti-virus alert that goes off on someone's machine may have already tripped an alert on the proxy from where that file came from, but ensuring that incident responders receive those alerts, let alone organize and prioritize them once they are gathered, is difficult without putting in place technologies that can manage them.

Meanwhile, each new sensor or blocking tool means more attack data, which necessitates more correlation, leads to additional complexity, and requires more staff, all of which adds to the overall cost of defeating phishing threats. Although these systems in a perfect world would work together in sequence, getting to that perfect world is difficult.[6]

Employees, assuming they have been properly trained and conditioned to look for suspicious emails that contain phishing attack indicators have the potential to significantly improve phishing detection and response. (See sidebar "Employee Phishing Boot Camp: 3 Key Process Elements" on page 8 for information on how to enlist users in the fight against phishing.)

However, most organizations lack a clear, repeatable process that they may use to report suspicious activity directly to the incident response team. Sometimes the activity is routed to a help desk, while other times it is sent to an unmonitored mailbox that is oftentimes ignored. None of these processes are efficient, let alone scale, for effective phishing prevention.[7]

[6] Galway, Will. "ISMG Interview with Will Galway, Director of Product Management, Triage, at PhishMe." (Phone Interview, June 2016)

[7] MacKinnon, Dave. "ISMG Interview with Dave MacKinnon, Director of Research at PhishMe." (Phone Interview, June 2016)

Most organizations have a limited number of incident responders to apply to the many security issues these organizations regularly face.

Top Challenges for Incident Responders

A 2016 survey co-produced by consultancy ESG (Enterprise Security Group) and security automation and orchestration company Phantom reports that more than two-thirds of respondents have found it increasingly difficult to handle incident response over the past two years. Among the main factors are the workload from additional security management and incident detection technologies, a growing number of security alerts, and increased difficulty in prioritizing them. The report also shows 74 percent of large enterprises regularly ignore some security alerts as they seek to prioritize investigations and manage their security workload.[8]

There are several reasons behind this challenge:

Limited number of incident responders: Most organizations have a limited number of incident responders to apply to the many security issues these organizations regularly face. Given the increased workload—and noise—caused by all the various alerting and reporting vectors, and the lack of integration among these messages, there are rarely enough incident responders available to analyze all the data that is collected.[9]

Lack of context: Currently, the most common way of viewing alerts is manually through an Outlook mailbox. In addition to guaranteeing that at least some important alerts will be overlooked, incident responders lack the context to determine the breadth or severity of the problem, and, therefore, how to prioritize it.

In other words, if incident responders lack an easy way to cluster like email messages together, they lack the visibility to determine how potentially widespread an attack could be. In lacking that ability to analyze and prioritize these alerts, incident responders have to rely on a gut feel—and if they have been otherwise occupied, they often fail to check that mailbox for something that gives them that gut feeling.[10]

Inability to identify root cause of attacks: Much of the difficulty in identifying phishing attacks lies in their continually changing attack methods. Many attacks rely on new, unknown types of malware—or, in the case of business email compromise, which manipulates users via targeted social engineering—no malware at all.

Arguably, the greatest challenge for incident responders is trying to keep up with advanced adversaries who seek out all avenues to exploit an organization's system. In addition to social engineering strategies, attackers continue to vary their attacks in an attempt to sneak past corporate policies and exploit weaknesses. If they can stay within the guidelines of what is allowed by those policies, they stand a better chance of infiltrating the system.

All of the aforementioned challenges illustrate the difficulties incident responders face when trying to stop phishing attacks. Incident responders have to navigate through too many alerts from too many sources without a reliable way to filter out duplicates or false positives, let alone organize them into something to be acted on. This bleak scenario leads to alert fatigue and decreased effectiveness against threat actors.[11]

Without the proper support, is it any surprise that the average detection rate of most attacks averages 146 days?[12]

The Solution: Implementing Technologies That Drive Internal Attack Intelligence

To respond to threats based on the deluge of data they receive at any given moment, incident responders need technologies in place that transform data into actionable threat intelligence.

[8] Kovacs, Eduard. "Suffocating Volume of Security Alerts Challenge Incident Response." (Security Week, March 15, 2016)

[9] Dave McKinnon of PhishMe, recalling his time as an incident responder, said that people prioritize the highest risk that they can identify, but "Unfortunately, you cannot do rapid identification when you're looking at an Outlook screen."

[10] MacKinnon, Dave. "ISMG Interview with Dave MacKinnon, Director of Research at PhishMe." (Phone Interview, June 2016)

[11] MacKinnon explains that attackers try multiple attack vectors to establish that needed foothold to embark on mayhem. "It's a difficult position for incident responders—whose goal is to stop everything that's thrown at them—to be in because there's no end in sight," he said in his interview with ISMG.

[12] Mandiant Consulting. M-Trends 2016. (FireEye, February 2016)

Such technologies must be able to:

- Filter the barrage of alerts and reports coming from multiple systems and from human reporting;
- Cluster those alerts so that they may be seen as part of specific incidents;
- Prioritize those incidents so that incident responders may determine the order in which they are addressed;
- Find the root cause of a given incident to mitigate the problem and prevent it from reoccurring in the future;
- Automate mitigation workflows so that organizations can respond to similar threats in real time.

In addition, these technologies should be able to operationally integrate into a solution that shows everything users are reporting, supplies an interface that allows for rapid identification and prioritization, and makes use of intelligence feeds that can augment the overall threat intelligence level and lead to fast, effective response.[13]

Automation: The Incident Responder's Secret Weapon

Most of the aforementioned actions require the ability to crunch large amounts of data and create workflows that find the root cause of attacks, mitigate those attacks and later prevent subsequent attacks from the same or similar source. Therefore, automation is key to making sure incoming data is taken and analyzed in an efficient manner.

Automation aids incident responders throughout the phishing incident life cycle and works best when it is used in conjunction with a dedicated phishing incident response platform in the following ways:

Arguably automation's greatest benefit is its ability to filter out noise and false positives before they reach incident responders.

Filtering
Arguably automation's greatest benefit is its ability to filter out noise and false positives before they reach incident responders. To give one of many examples, if employees are forwarding bundles of legitimate (albeit annoying) LinkedIn messages, incident responders may deploy a script that automatically removes them before they become part of the phishing incident workflow. Similarly, incident responders may implement an automated response that informs these employees to avoid reporting such types of emails going forward.

Information Clustering
Once phishing-related data is gathered from its manifold sources, automation can analyze and then cluster information by incident. This integration allows for additional analysis on a cluster of information, including the state of the email or emails; what, if any, attachments have been included; and URLs and other elements that designate it as a potential phishing email, before the incident responder begins to address the issue.

In addition, automation can further enrich the intelligence going to incident responders by harnessing an organization's internal attack intelligence, including records of past successful phishing attacks, along with the IP addresses and names used in previous attacks.

Root Cause Analysis
Once relevant data is clustered in this fashion, incident responders gain context into the type of threat or attack they are facing—and ultimately, identify the root cause. Organizations then can see that an attack uses a weaponized Office document, an invoice or whatever type of ingress the attackers are using.

Once able to identify the root cause, incident responders have the freedom to move through the normal incident response process because they now have the bandwidth

[13] MacKinnon, Dave. "ISMG Interview with Dave MacKinnon, Director of Research at PhishMe." (Phone Interview, June 2016)

to conduct in-depth analysis. Among other things, incident responders can determine:

- The number of phishing emails that are in the system;
- The people who received these emails;
- The percentage of people who opened these emails, as well as the percentage who clicked on a link, opened a file or ran a macro;
- Whether or not the organization's anti-virus solution worked and what additional protections must be put in place;
- The number of infected machines.[14]

Prioritization of Threats

Once incident responders understand the cause, level of severity and level of urgency of a phishing attack, they may then prioritize the order in which to mitigate them. For example, incidents may be prioritized by number of clusters, the tripping of a YARA rule, the level of importance of the person sending a report, and so forth. Meanwhile, senior incident responders might handle a bona fide campaign, while a junior analyst might handle clearing out the noise of, say, a bunch of LinkedIn invites that were mistakenly reported by employees. This enables the IR team to pivot based on the criticality of the many threats they face.[15]

Dissemination and Incident Response

As a result of having all this information in hand, incident responders may then mitigate attacks by pushing out the gathered intelligence to the appropriate channels. For example, incident responders can share results with SIEMs (Security Incident and Event Management Systems) and investigation teams so that security controls at endpoints, email gateways and other systems can be updated to stop the latest threat, as well as alert upstream teams to block a malicious attachment or suspicious IP address.[16]

Create New Workflows to Stop Similar Attacks

Finally, automation enables incident responders to create automated scripts that match suspicious emails against certain commonalities and indicators of phishing and then take self-activating measures to stop them.

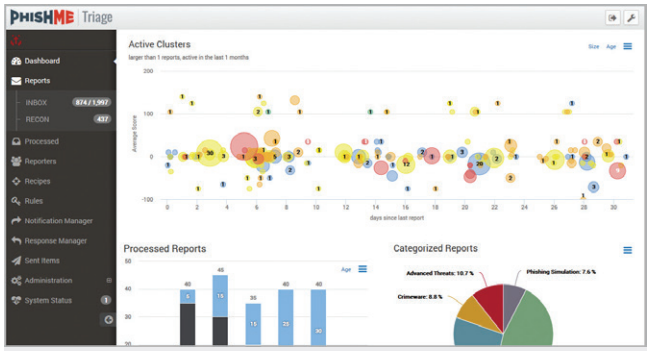
Ideally, a security analyst would review a suspected phishing campaign and approve an automated workflow to protect the organization from damage. These automated workflows could blacklist the senders in your email security products, and block any malicious links via your firewall, proxy or secure web gateway.[17]

In addition, automation may be used in other ways, such as creating workflows that reward employees for reporting suspicious activity. More than anything, however, automation takes care of the heavy lifting so that incident responders can leverage their most effective defense against phishing attacks—their expertise.

Conclusion: Orchestrating Your Phishing Incident Response Program

A successful phishing incident response program requires the ability to collect relevant data, organizing that data into actionable threat intelligence, and getting that optimized threat intelligence into the hands of incident responders who can then make good decisions that reduces an organization's risk. This type of orchestration is critical in protecting organizations from the damage a successful phishing exploit can wreak.

PhishMe Triage was developed precisely on that need for orchestration, which makes sure that information gleaned from multiple systems and users works in concert with incident responders and other security experts to detect and remediate phishing incident. PhishMe's human phishing defense solution drives recognition (PhishMe Simulator), reporting (PhishMe Reporter) and response (Phishme Triage) in a platform designed to automate and optimize the threat intelligence organizations of all sizes needed for an effective phishing incident response program.



PhishMe Triage

PhishMe Triage provides insight into phishing attacks by automating the analysis of disparate sources of information and then orchestrating the workflows incident responders use to mitigate attacks and prevent future ones. It prioritizes reporting analysis based on reporting volume and severity, as well as user reputation to provide actionable intelligence for SOC and IR teams, and leverages anti-malware and sandbox technologies to provide additional analysis that other security technologies can use to increase detection rates.

[14] Ibid.

[15] Galway, Will. "ISMG Interview with Will Galway, Director of Product Management, Triage, at PhishMe." (Phone Interview, June 2016)

[16] Ibid.

[17] Sanabria, Adrian. "ISMG Interview with Adrian Sanabria, senior security analyst at the 451 Group." (Phone Interview, June 2016)

Employee Phishing Boot Camp: 3 Key Process Elements

Given the continued increase in the number of phishing attacks—and the potential havoc they wreak on organizations[18]—enlisting users in the fight against phishing-related risks should be a key part of your overall layered security strategy. The good news is that your users don't have to be perfect to be effective. You only need enough of them to detect and report a campaign to be able to stop it before any damage is caused.[19]

At the same time, you don't want the sort of scenario described in the introduction, where people are reporting dubious emails in a haphazard fashion. You need the right combination of education, technology and processes to protect your organization from phishing attacks in an efficient and cost-effective manner. This involves a consistent, strategic campaign of employee conditioning, the ability to measure results of this conditioning, and the capacity to refine these steps as needed. And it also requires technology that will facilitate both the training and actual reporting of suspicious activity that will empower your IT security to take the appropriate action against such attacks.

1 Condition

The first step is a consistent conditioning campaign to better educate users about what constitutes phishing, how to detect it, and what to do about it.

Hackers use emotional triggers such as fear, curiosity, reward, urgency and excitement to lure users into opening their emails or clicking on an attachment. An email describing a package to be delivered may trigger a recipient's curiosity. Another email from the boss demanding the review of an attached file may trigger an employee's anxiety. Both scenarios could result in a successful attack if the users aren't versed in the social engineering cues being used to precipitate the desired response.

However, commonly used methods of conditioning, such as computer-based training (CBT), tend not to be effective. Putting employees through a 20-30 minute CBT is in most cases a punitive measure because most employees lack the time to sit through 30 minutes of training on a topic that they, essentially, don't care about. Worse, this type of generalized training rarely sticks, particularly when attackers leverage social engineering tactics that trigger employees into reacting without first considering the situation.[20]

One way you can condition your users is to simulate actual attacks. Depending on the end user's response to the simulation, you would then quickly send a "thank you" email to those who accurately identified and reported threats or on-the-spot training that lasts for 60 to 90 seconds in an engaging format for those who mistook a phishing email for a legitimate one. This emphasis on gentle retraining is critical to helping them absorb these teachings.

2 Track

To capitalize on employee conditioning, effective tracking of employee progress must accompany the training component of your strategy. Before sending out a simulated attack, coordinate with departments that are most affected by phishing attempts, such as security, IT, legal and HR, so that they are aware of your training efforts and have taken the proper steps to minimize any potential complications.

In addition, set specific trackable goals, such as percentage reductions in the number of users who click on links or open attachments in suspicious emails. Not only will these metrics help you refine your training and response program, you may also use this information to communicate the value of this training to senior management.

Make sure to focus special attention on tracking "repeat offenders" who consistently open phishing emails or click on attachments, despite

[18] Korolov, Maria. "Phishing is a $3.7-million annual cost for average large company." (CSO Magazine, August 26, 2015)

[19] Sanabria, Adrian. "ISMG Interview with Adrian Sanabria, senior security analyst at the 451 Group." (Phone Interview, June 2016)

[20] Belani, Rohyt & Field, Tom. "Ransomware: Healthcare Fights Back." (ISMG, April 1, 2016)

To capitalize on employee conditioning, effective tracking of employee progress must accompany the training component of your strategy.

your training efforts. For example, you might customize your follow-up messages and training to change the behavior of the users who fall for attacks most often and reflect the types of phishing emails to which they fell victim. Simulated phishing attacks can be useful, but reusing actual successful phishing emails is the most effective way to determine which attacks have been successful and how to educate users to report them in the future.

3 Reward

Finally, organizations should consider implementing a rewards plan that will encourage users to report on potential phishing attacks. Such a plan should aim to encourage behavioral changes that would motivate employees to identify and report suspected phishing schemes.

The type of reward that works best depends on the size and culture of your organization. The best rewards do not have to be financial or (if they involve cash) do not need to be expensive. Often, the best reward is acknowledging your employees' innate desire to do the right thing, to contribute to the organization, and to be recognized by their peers for doing so.

At the same time, continually reassure employees that they will not be punished if their actions—such as clicking on a questionable file—may have led to an attack. A punitive approach will only lead to employees hiding their actions, which will be far more damaging to your organization in your quest to thwart phishing attacks.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification.

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com