Global Information Assurance Certification Paper

ComBAT Phishing with Email Automation

GIAC (GCCC) Gold Certification

Author: Seth Polley, readingroom@nightvisionsecurity.org
Advisor: Sally Vandeven
Accepted: 8/29/2017

Abstract

An analysis of organizations' email reporting processes reveals two challenges facing cyber security departments: successful administration of the managed mailbox provided for user's suspicious email reporting (automation) and effective security awareness training tailored to the business groups based on the type of email received. An effective defense requires an organization to be informed by actual attacks (knowing the enemy) and awareness of internal shortcomings (knowing yourself) so that implemented protections and training are applicable to the threats faced (strategy and tactics).

1. Introduction

Email has become the cornerstone for communication in many organizations and, as such, inbound email has become a business requirement. There is no 'silver bullet' solution to prevent all unwanted email. As users have proven themselves to be the weakest link in cyber security, phishing emails will only continue to become more common, growing increasingly sophisticated as new tools and tactics for creating authentic-looking emails become freely available, there needs to be a means for educating the users based on the type of email they are reporting along with a process for evaluating and responding to malicious email that is allowed into an organization. An approach to automating the email triage process, derived from the shortcomings identified by regional Information Technology (IT) and Information Security (IS) representatives, will be discussed in this paper, programmatically delivering timely classification verdicts to the end users, while providing a means to collect statistics which can then in turn be used to proactively educate targeted user groups against emerging or rising threats. The event-driven automation delivered by StackStorm provides a better approach to managing the designated cyber security mailbox, which users report emails to, and affords a sustainable solution for conveying the findings to the reporting users (StackStorm, 2015). The author's original paper "Dissect the Phish to Hunt Infections" [https://www.sans.org/reading-room/whitepapers/awareness/dissect-phish-hunt-infections-37587] addresses the latter points of evaluating and mitigating the email threats that make it through to the end users; it was written to provide maturing organizations with a process that enables them to move from a passive stance (static tools) to that of an active defense (hunting threats) by gathering information on actual threats they are facing.

To effectively defend an organization, one must be informed by actual attacks, so that the protections put into place are those applicable to the threats. While knowledge of attacks being seen in "the wild" and general threat intelligence has its value, it is not feasible or prudent to incorporate an organization's defenses solely based on these reports. The threats one organization may face or the threat vectors that may be pertinent to them may not be relevant to another organization. One common attack vector today, however, is social engineering in the form of email phishing campaigns. Phishing is a technique that involves tricking one or more users into divulging sensitive information (such as usernames and passwords), clicking a link, or executing malware. These attempts are generally performed by masquerading as confidential, legitimate, or trustworthy sources.

Organizations have migrated to email as the cornerstone of communication with external entities. These phishing techniques have become highly successful for credential harvesting, fraud, and the introduction of malware into a target's environment. Attackers generally follow the low-resistance paths that sidestep breaking stronger technical controls and email has proven itself to be just that threat vector. As such,

> 91% of targeted attacks commence with using email as a point of entry. Further, … 78% of targeted email attacks utilize malware that has been embedded within an attachment. Given these points, clearly attackers perceive email to be a path of least resistance to evade existing security defences and to breach your network. (Corson, 2014)

Malicious or criminal attacks account for 47% of data breach incidents and the average total cost of a successful phishing attack that leads to a data breach is $3.62 million. The average organizational cost of a data breach varies by country, but the US sample comes in the highest at $7.35 million (Ponemon Institute, 2017). A single click by one person, which opens a malicious link contained within a phishing email, can put an entire company at risk.

As email has become a 'fact of life', steps to prevent these attacks must be taken. An organization cannot simply block all inbound email, as this would disrupt the core business processes contingent on external communication. Tools can be implemented to filter out a significant volume of the phishing and spam messages at the external border, but prevention efforts will eventually fail. Configuration errors are made, some tools rely on previously seen 'known bad' attacks, and attackers are becoming more sophisticated too. There is no 'magic solution' or 'silver bullet' to block all unwanted email from entering an organization. The stricter the preventative controls become, the greater the risk that legitimate email will be falsely blocked as unwanted. The stance taken by many business groups is to err on the side of caution, allowing a relaxed filtering of email messages to prevent a negative impact on any business function. Alternative steps should then be taken to reduce this threat.

2. Prevention

Prevention can be established by taking the approach of Defense in Depth (DiD). The external defenses, such as the firewall and secure email gateways (solutions that monitor inbound and outbound enterprise email for undesirable content), can provide the first line of defense. Network-based security

controls, such as Intrusion Prevention Systems (IPS), antivirus, and email security appliances, can be incorporated as the next line of defense. However, no matter the level of safeguards implemented, malicious email can always arrive to the end user's mailbox. Whether the message originates from a legitimate domain that is misconfigured and allows email relays or the sender is a reputable organization that has had accounts compromised, blanket 'blocks' cannot be put into place for many domains. The burden of detection then quickly shifts to the end user receiving the message, but "Unfortunately, many breaches result from a lack of employee awareness of the security risks inherent in their actions." (Symantec Corporation, 2017). A framework must be in place to successfully allow the recipients to detect and report these suspicious messages. The framework begins with applicable user training for the phishing threats and encompasses the processes for reporting these to the SOC – whether by forwarding the messages as an attachment to the designated SOC mailbox(es) or more simply through a pre-configured Outlook plugin (such as the PhishMe Reporter). The users must be provided with security awareness training tailored to the threats they are encountering, which "will raise employee awareness of the reality of threats, vulnerabilities and consequences, and help them take active roles in securing your enterprise" (Symantec Corporation, 2017).

There are five critical tenets of an effective cyber defense system (described in Section 2.1) that rely on the pairing of strategy and tactics. Sun Tzu, a renowned military strategist and tactician, once said, "Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." (Tzu & Giles, 1910). Strategy (or the "what") provides the plan of action that is designed to achieve the organization's overall long-term goals, where as tactics (or the "how" and "who") are carefully planned actions intended to achieve a specific end – a concrete goal. Strategy and tactics are not mutually exclusive and should be paired as the means to an end. Similarly, the Center for Internet Security's (CIS) Critical Security Controls is a recommended series of actions for effectual cyber defense through the incorporation of specific AND actionable controls tailored to the most prevalent and threatening attacks leveraged against both public and private sectors worldwide. As a hurricane is unlikely to directly impact a data center in Kansas and it is improbable that a nation-state cyber warfare program would target a local vehicle dealership, it would be unwise for these organizations to channel a significant amount of available cyber security funding into defenses for these threats. The founding principle of the Critical Security Controls is the prioritization of smaller, focused changes that will provide increased dividends when it comes to the defense of an organization. Before discussing any

specific controls or mitigation strategies however, it is important to understand the critical tenets of an effective cyber defense system.

2.1 Critical Security Controls and Mitigation Strategies

The CIS Critical Security Controls (CSC) were designed with five critical tenets that should be reflected in an effective cyber defense system (Center for Internet Security, 2016):

- Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
- Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.
- Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.
- Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

The top four strategies to mitigate cyber security risks will vary by governing body, but a common overlap can be seen within those most predominant. The top four controls recommended by the Critical Security Controls are noted below, with the fifth included for later comparison (Center for Internet Security, 2016):

- CSC 1: Inventory of Authorized and Unauthorized Devices – "Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access."

- CSC 2: Inventory of Authorized and Unauthorized Software – "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers – "Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings."
- CSC 4: Continuous Vulnerability Assessment and Remediation – "Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers."
- CSC 5: Controlled Use of Administrative Privileges – "The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications."

Another well-known entity, the Australian Signals Directorate (ASD) (an intelligence agency in the Australian Government's Department of Defence), assesses that implementing the following top four strategies will "mitigate at least 85% of the intrusion techniques that the Australian Cyber Security Centre responds to" (Australian Signals Directorate, 2013):

- Mitigation 1: application whitelisting
- Mitigation 2: patch applications
- Mitigation 3: patch the operating system
- Mitigation 4: minimize administrative privileges

These Critical Security Controls and Mitigation strategies map closely to each other and it should be noted that the ASD is involved with the process of creating and maintaining the Critical Security Controls. The difference to note is that the Critical Security Controls are intended to be more general, whereas the ASD's recommendations are based directly on their experience responding to and preventing attacks directly leveraged against their government agencies. Comparison of the top five Critical Security Controls and the top four Australian Signals Directorate

strategies shows the common ground – maintaining device, application, and versioning awareness, in addition to controlling and minimizing the usage of administrative privileges that could be used to undermine the former strategies.

Implementation of the top Critical Security Controls or the Mitigation Strategies are not always immediately feasible, can be implemented in a timely manner, or are generally not driven or implemented by the cyber security department. To address the rise in phishing and user reporting of suspicious emails, while adhering to the spirit of the Critical Security Controls, an organization's cyber security department may choose to implement event-driven email automation to assist with the triage and ticketing, education of the end users, and the gathering of metrics to proactively educate or inform users and/or business groups on current threats.

3. Automation

An effective cyber security system will seek to combat phishing through several layers or levels of email automation and will aim to deliver Just-in-Time (JIT) training to the end users. The activities within the workflow process will be reviewed in order – starting with the user reporting of the suspicious message, continuing through email triage utilizing event-driven automation, and concluding with the automated template response providing the initial user education.

3.1 Methods for Reporting Suspicious Emails

The first step in addressing phishing attempts is providing the end users with a means to report suspicious emails. These suspicious emails may originate from unknown external senders (attackers, spammers, marketers, etc.), known external senders (compromised accounts, misuse, etc.), or internal senders (compromised accounts, misuse, uncharacteristic behavior, etc.). Wherever the origin,

> Cyber security teams should have a monitored mailbox where users can report questionable emails. Some teams designate the primary SOC mailbox for all the cyber-related security concerns that arise, while others may create a secondary mailbox specifically for fraud, phishing, and spam messages. Common designations for these mailboxes are user-friendly names like "malicious", "phishing", "spam", and/or "suspicious". Users should be trained

and encouraged to report the emails in question to the SOC by forwarding the messages as attachments, to make full header details available for scrutiny. (Polley, 2017)

To simplify these reporting actions (and continuing the spirit of automating defenses), organizations may choose to implement Outlook plugins that allow the user to simply click once or twice to properly report the email as an attachment to a pre-configured mailbox. Some tools that provide this functionality, often in conjunction with the capability of managed phishing drills, are PhishAlarm, PhishMe, PhishReporter, ThreatSim, Microsoft Junk E-mail Reporting Tool, etc. These plugins will not always be available to an end user though, such as in the case of Outlook launching in Safe Mode, corporately issued mobile phones, or BYOD (Bring Your Own Device). To address this and continue to encourage the reporting of suspicious emails, the users should be instructed to manually forward the email as an attachment (when possible) or, as a final resort, simply forward the email to the managed mailbox. To manually forward an email as an attachment in Outlook, the user can right-click one or more messages, selecting "Actions" or "More Actions", and then "Forward as Attachment" from the menu. Alternatively, the keyboard shortcut "Ctrl + Alt + F" can be used. Valuable response and threat intelligence information can be gathered from the email header fields, such as the "Return-Path", "client-ip", and "X-Mailer", where some fields can only be analyzed (third party) by reviewing the original email as an attachment. No matter the method, it is more important to encourage the users to report suspicious emails than it is to chide them for not using an automated means or forwarding the email as an attachment.

3.2 Event-Driven Automation

Once users are reporting suspicious emails to a central, managed mailbox, the next step is providing them with an assessment of the reported message. An unsustainable and inconsistent method is to manually respond to each individual message. Whether through handcrafted response or by utilizing a base email template, these actions are not only time consuming, but are also humanly repeated and prone to error or failure. Automation should be considered to provide a standard response; one that is reliable, scalable, and lends to continuous measurement (metrics) in keeping with the Critical Security Controls.

By incorporating automation, organizations can replace manual response, removing operational bottlenecks and improving the security stance. Verizon's 2016 Data Breach Investigations Report (DBIR) found that manual attempts to block security breaches were not preventing attacks (Verizon Enterprise, 2016). Managing these known operational security chokepoints through email automation, an organization can effectively overcome unpunctual responses, improve user awareness, and can also collect metrics that allows for tailored education by business groups. Analyzing the data being produced by the reporting of suspicious emails, an organization can then make the necessary changes to improve performance and security by tailoring automated responses and custom training to efficiently and responsively address the underlying needs of the end users.

However, such automation should only be considered where feasible and prudent. For example, the investment in automation for an organization of five to twenty employees may be unwise when resources could better be applied in another capacity. Conversely, when email automation is implemented by an organization of 55,000+ employees, it allows a single security analyst to successfully sustain hundreds to thousands of emails reported over the duration of his or her shift. Without email automation, the 'managed' mailbox of even small to medium organizations can quickly become out of control and therefore unmanaged, posing unknown risks to the organization when reported malicious emails go unaddressed or the review turnaround is delayed. The malicious phishing emails can quickly become obscured by the volume of legitimate or spam messages reported, potentially leaving an active threat or compromise unaddressed within the organization's environment for days or an indefinite period of time.

There are better approaches and solutions to managing the mailboxes that users report suspicious emails to than the unsuccessful or unsustainable solutions adopted by many organizations today. Through interviews with members of regional organizations responsible for managing these efforts, there are no existing or sustainable processes that have been implemented to address these frustrations and shortcomings. The research drew from a regional base of organizations in a representative, non-statistical sampling. The cyber security professionals were employed within varied industry classifications (Education, Financial, Industrial, Public Sector, etc.). The demographics by total headcount were most evenly split between organizations of 5,001 to 10,000

employees and 10,001 to 25,000 employees, though did encompass outliers of 1,001 to 5,000 employees and 25,001 to 50,000 employees. For purposes of confidentiality, no company-specific information was captured that could link responses to participating companies. The following examples highlight some of the existing approaches to mailbox management adopted by organizations today. A representative from Organization A stated that the mailbox management was strictly a manual process where an analyst would respond to each individual by drafting a custom message. The representative from Organization B noted a similar manual response process where an analyst would generate individual responses from a base Outlook template (see "Send an email message based on a template" in the References for more information). Organization C handled the response process by creating unique Outlook signatures with each template, injecting these into the email response, modifying select portions of the response to present a 'unique' and 'individual' feel with each message. These manual processes are time-consuming and error-prone, relying on the analyst to customize and proofread each response, often times resulting in templates being sent with unmodified prompts such as "Hi <user>," or "The reported email <subject line>". A common theme brought to light through the interviews was unsustainable processes – processes where legitimate and spam messages that were reported would accumulate in the Inbox and go unresponded to when the analysts only had time to address the phishing threats that stood out from the onslaught of reported messages. What solutions are available then, to automate email response and address these concerns? Analysis of the mailbox handling processes implemented by a world-class SOC, one equipped to handle Advanced Persistent Threats (APTs) – nation-state actors and state-sponsored cyber attacks, show there are powerful approaches that provide event-driven automation through workflows. The most basic example of this is the "if-then" conditional flow statement in programming – if this condition exists, then perform that action (known as "If This, Then That" rules or simply IFTTT). By chaining together simple conditional statements, an extendable and flexible workflow can be established. One example of conditional chaining is to combine Outlook templates with macros to eliminate these repetitive triage and response tasks, establishing an event watcher for new items added to one or more folders, which then generates an email containing the response template to the reporting user. An open-source automation platform providing these capabilities with greater extensibility is StackStorm (StackStorm, 2015). StackStorm not only provides basic email integration (StackStorm, 2017), but it can provide auto-remediation in response to security events or other use cases including external operational events associated with major platforms like:

- ChatOps – HipChat, IRC, Slack, and other chat services via Hubot
- Cloud Computing – Amazon Web Services (AWS) and Microsoft Azure
- Email – Microsoft Exchange or other SMTP and IMAP services; Mailgun
- Open Source Monitoring – Icinga and Nagios
- Relational Database Management Systems (RDBMS) – Microsoft SQL Server (MSSQL) and Oracle MySQL
- Searching and Monitoring – Elasticsearch and Splunk
- Security Services / Solutions – Alert Logic, FireEye, Lastline, and Qualys
- Ticketing / Tracking – Jira and ServiceNow (StackStorm, 2017)

Given the powerful automation platform that StackStorm provides and the broad variety of use cases that it can be applied towards, the usage of StackStorm over Outlook macros, as it applies to email automation, will solely be discussed moving forward.

3.2.2 StackStorm Configuration (Pre-Automation Triage)

The installation and configuration of StackStorm (or alternative platforms) will not be covered in this research paper, as extensive documentation exists on these processes, but the concept of the configuration and operation will be discussed to establish a reference point while noting common pitfalls which may not readily be apparent in the planning process. Assuming a clean 64-bit Linux box that fits the system requirements is available, it takes little time to implement the base Proof of Concept (PoC) environment – about 4 minutes to install by utilizing the provided installation script that installs and configures a stable version of StackStorm following the single host "reference deployment" (StackStorm, 2017).

As discussed earlier, users have been instructed to report suspicious messages to a central and managed mailbox, such as "SOC" or "Suspicious". For ease of typing, the "SOC" mailbox will be used for ongoing reference. Within the SOC mailbox, a series of subfolders should be created for "Legitimate", "Phishing (*)", "Spam", "Scam", and "Targeted" automated responses, which can be seen in Figure A below:

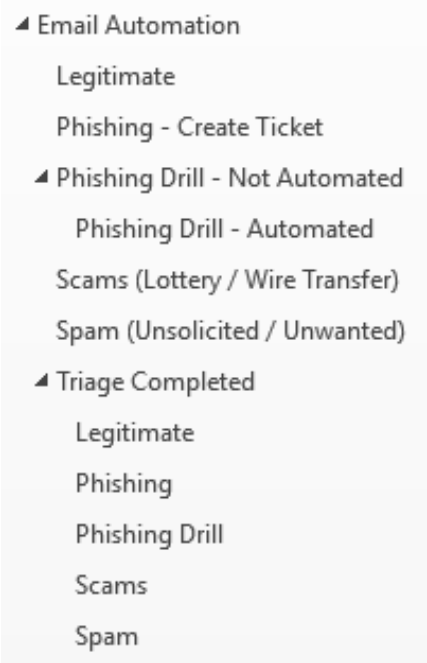


Figure A – Sample Folder Structure for Email Triage

When an analyst triages the incoming email messages, they are making the determination as to what classification should be applied to the reported suspicious messages. After making the determination, the analyst moves the reported email to the appropriate subfolder. When StackStorm processes the message, a predefined template (discussed next in Section 3.2.3) assigned to the specified folder is automatically generated to the reporter of the suspicious email. To contrast, an entirely manual approach would require the analyst to draft a custom response to each and every user or to manually inject a templated response from a local file or a list of signatures. After the template has been sent to the reporter, the original email is moved into a "Triage Completed" folder and placed into the respective subfolder based on triage classification. Triaged emails that warrant further review (as determined by the organization's processes), such as phishing attempts, would then be forwarded or otherwise ingested by the ticketing system (through APIs or other integrations). When successfully implemented, the process would allow for minimal effort required by users reporting suspicious emails (versus contacting the help desk or manual ticket creation for email analysis). By tailoring the processes for the ease of end user reporting, as opposed to the aforementioned manual processes that may take 5-15 minutes and may be seen as negatively impactful to a user's time, the active threats are more likely to be reported to the SOC where they can be handled in a timely manner. Likewise,

after an analyst has made the determination by classifying the reported email, a response to the user will only take the analyst a matter of seconds – the time it takes an analyst to drag or move the reported email into the appropriate automated folder where it is processed by the event-driven automation solution that generates the automated response template to the reporter of the email.

3.2.3 Automated Response Templates

The automated response templates can be used to generate one or more different response types to the reporting user based on the conditions that are evaluated. To continually reinforce the authority and legitimacy of the response, it is recommended to place the cyber security department's logo at the top of the template response – as where one would generally see a header placed. While the company logo can be used alone, these are generally externally facing, allowing a potential Advanced Persistent Threat (APT) actor to easily incorporate the image into any spoofing or targeted phishing attempts. As many cyber security departments have their own internal logo, these can become a more unique identifier for an unsuspecting end user. When used alone or paired with the corporate logo, this imagery continually reinforces a unified cyber security approach – especially when considering organizations of medium or large stature that have multiple teams within the overarching cyber security department.

The automated response template should clearly define the assessed classification of the reported email. The text can be featured in an increased font size, bold typeface, color coded by threat assessment, or even a single, bright text color or highlight to place emphasis on the determination. For example, when color coding by threat assessment, a "Legitimate" assessment may be placed in a darker green font color, whereas a darker yellow font color can be utilized for a "Spam" message, and a greater weight is placed on a "Phishing" message with a darker red font color. Alternatively, all assessment could be defined in a darker red font color and/or a colored highlighting applied. The primary caution when considering colored emphasis is to people with deuteranomaly and protanomaly (collectively known as red-green color blindness), as they generally have greater difficulty distinguishing between green and red colors.

The automated template can lend to even greater unity through the cyber security department's response by transparency in providing resources that an end user can take advantage of to further his or her knowledge and understanding of threats that are commonly leveraged against the organization. Thank the user for taking the time to report the suspicious message and reaffirm their effort is helping protect and secure the organization. Take advantage of the user's attention and provide additional resources that may benefit them. All templates might include a link to the cyber security department's internal website (such as SharePoint team site or a corporate Wiki page) or text-based navigational directions on how to reach the same website from the corporate intranet homepage. Consider exercising caution with the inclusion of unfamiliar links – links that have not been globally promoted within the organization and which may generate concern or suspicion on their own. Otherwise, targeted training could be leveraged on a per-template basis. For example, if the user has reported a "Legitimate" message, the template might include a few indicators the user should have noticed or a link to a website containing similar material. If the user has reported a "Spam" message, the template response may change to inform the user that spam messages frequently contain marketing (new products, services, or training opportunities), pharmaceutical ads (medication, dietary supplements, or sexual enhancement products), or 'personal' ads (dating, sexting, sexual encounters, etc.).

Though the content and intent of an automated response may vary by type of suspicious message reported, the length of the message should be considered. An email template should be clean and concise in terms of the design and layout. According to a study by Microsoft Corporation, "people now generally lose concentration after eight seconds, highlighting the affects of an increasingly digitalized lifestyle on the brain" (McSpadden, 2015). Utilizing whitespace and avoiding a lengthy 'wall of text', an organization can more effectively reach their target audience without unintentionally leading them to lose concentration and focus, which may ultimately nullify the company's efforts to inform and educate them. Likewise, the presence of too many links within a given template may desensitize a user, leading to a lower level of scrutiny taken before clicking one or more links asserting to be from a reputedly trusted source. Examples of concise email templates will be presented in the following sections that could be incorporated into an automated response.

3.2.3.1 Legitimate Emails Template

The Legitimate emails template confirms that the email is legitimate and attachments or links can be safely opened. As some users are unaware of how to retrieve the email after it has been reported via PhishMe, a reminder is given that the message is located in the "Deleted Items" folder, should the user need to access the legitimate email again. A link is provided to the Security Operation's Center website where the user can better educate themselves on their identification of suspicious emails. Figure B provides a sample email template for Legitimate messages:

Figure B – Sample Legitimate Emails Template

3.2.3.2 Spam Emails Template

Spam messages are unwanted and/or unsolicited messages. The Spam messages may include Scams (Lottery / Wire Transfer) or a separate template can be created for these. The users should not be instructed to 'Unsubscribe' from these as a default behavior, as non-reputable sources will simply take this as indication of an active mailbox, then continue the spam and/or sell the active mailing list to the next entity. An example of the Spam emails template can be seen in Figure C below:

Figure C – Sample Spam Emails Template

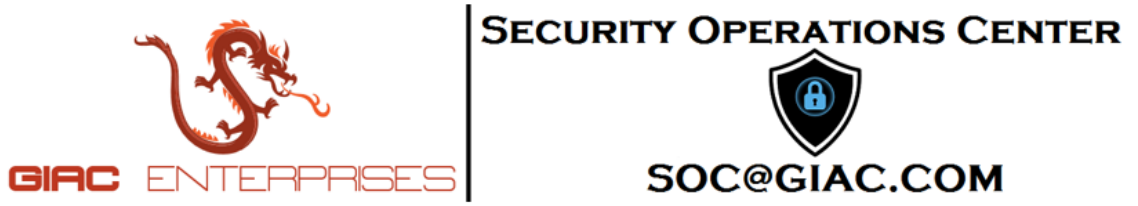
3.2.3.3 Phishing Emails Template

Phishing emails are generally attempts by a malicious actor trying to trick an end user into divulging sensitive information and/or executing malicious content on his or her computer. The preferred way to report these is by attachment, as mentioned earlier, to make specific email header fields available for triage, response, and later attribution. A sample template is provided below in Figure D, but these can be altered based on how the email was reported and/or triaged. If the email was forwarded to the SOC mailbox, an altered template might encourage the user to forward the email as an attachment (if possible) and/or provide steps the user can take to manually install the PhishMe reporter (or like plugin) from Software Center (Windows) or source. Should the phishing target be a C-level executive or other high value target, an organization may choose to generate a different response template based on the reporting user, hold the message so a manual 'handwritten' note can be sent, and/or ingest the reported message into the ticketing system with a higher priority automatically assigned. The event-driven workflows allow for a flexible response to varied phishing attempt scenarios.

Secure email gateways, such as Cisco Email Security (formerly IronPort) and Proofpoint Email Protection, allow configuration for blocking or stripping of attachments by attachment type. An organization may wish to create a specific template for this configuration, instructing the user that the attachment in question has been blocked or removed, explaining what attachment types are prohibited and why, then providing the user with approved methods to bypass this in the event they were expected a legitimate message. For example, the template might contain an explanation like:

> One or more attachments were blocked/removed by the email security solution. The noted file extensions are commonly abused by malicious actors with the intent of introducing malware into the network. If you were expecting an attachment from a legitimate source, instruct them to rename the file extension (<steps provided>) before sending or utilize our authorized/corporate file sharing solution <Box, Dropbox for Business, Google Drive, OneDrive, etc.>.

Small efforts like these that are taken to increase user awareness around security tools can significantly improve the user's perception towards security tools and increase acceptance of actions that may otherwise negatively impact an end user's daily tasks.



Thank you for taking the time to report the suspicious email to the GIAC Security Operations Center (SOC).

THE REPORTED EMAIL IS A PHISHING ATTEMPT.

If you've interacted with any content in the email (clicked on any links, submitted credentials, opened attachments, or responded to the sender), please contact the SOC immediately at extension x1337 for further assistance. Otherwise, no further action is required from you at this time.

To learn more about how to identify the difference between Legitimate, Spam, and Phishing emails, please visit the Security Operations Center's website on SharePoint (https://www.cybersecurity.com).

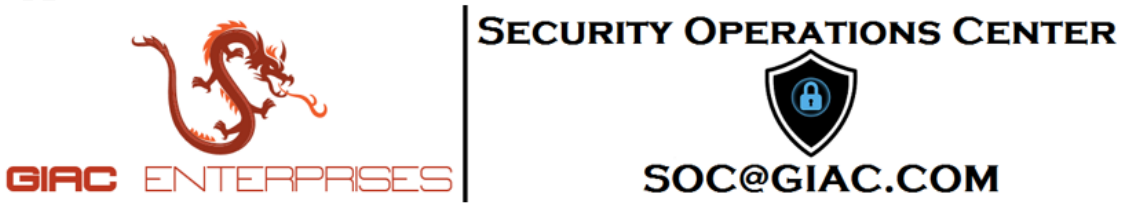
Thank you for helping to keep GIAC Enterprises secure!

Security Operations Center
soc@giac.com
Extension: x1337

Figure D – Sample Phishing Emails Template

3.2.3.4 Phishing Drill Emails Template

Organizations frequently perform authorized phishing drills for assessment and with the intent of increasing user awareness through JIT training. When automated tools (such as PhishMe) are utilized, the plugins can inform users that this was an authorized phishing drill and can congratulate them on detecting the phishing attempt. However, there are times when manual phishing drills are performed or users can/do not utilize the plugins for automated reported. To address these scenarios, an organization might create an automated folder to handle the reported phishing drill emails. Should the cyber security team performing the drills wish for a delayed response to the reporting user, the automated folder can be placed into a non-automated parent folder that collects the emails. At a later time, after the phishing drill has subsided or the desired period of time given to the users for reporting has passed, the messages can then be moved from the non-automated folder into the automated subfolder for processing to send the template response to the reporting users. A sample response template is shown in Figure E for reference:



Thank you for taking the time to report the suspicious email to the GIAC Security Operations Center (SOC).

THE REPORTED EMAIL IS PART OF AN AUTHORIZED PHISHING DRILL.

Thank you for staying vigilant!

To learn more about how to identify the difference between Legitimate, Spam, and Phishing emails, please visit the Security Operations Center's website on SharePoint (https://www.cybersecurity.com).

Thank you for helping to keep GIAC Enterprises secure!

Security Operations Center
soc@giac.com
Extension: x1337

Figure E – Sample Phishing Drill Emails Template

3.2.3.5 Other Email Templates

After creating templates to address the most frequent email reporting scenarios, such as Legitimate, Spam, and Phishing attempts, an organization may consider drafting templates for less common malicious scenarios. Should a user receive a cold call phishing attempt, the organization may direct the individual to take note of all the details he or she can recall (phone number, sex and accent of individual, who they claim to be, etc.), reporting this information to the SOC. A like-phishing template can be utilized to inform the user that an analyst will review the information before contacting them to follow-up and then a ticket can be generated to document the event. Some organizations have seen an increase in job fraud too – whether through social media or social networking sites (like Facebook or LinkedIn), job search websites (like Indeed, Job.com, and Monster), or other spoofed websites. Triage folders could be created for automated ticketing based on these or other compliance and legal concerns (such as cease and desist letters, domain abuse notices, or misuse of published trademarks).

3.2.4 Recommended Process Safeguards

Though specific event-driven automation configurations won't be addressed in this research paper, some recommendations will be provided pertaining to process safeguards.

Organizations should consider delaying the automated processing of triaged emails for 1-5 minutes (in the event of accidental mistriage). Should an analyst accidentally place a phishing email into one of the designated legitimate folders, a configured mandatory delay would allow the analyst to reconcile the mistriage before a response is instantaneously generated to the end user.

To prevent a failure of operational security, only allow automated responses to be sent to internal recipients; do not send the automated templates to external senders (accidentally or intentionally). Consider the following scenario: An attacker sends a phishing email to the SOC mailbox, an analyst fails to observe the sender as external, and triages the email as a phishing attempt. Without a configuration safeguard in place, the event-driven automation would automatically generate a response to the sender, providing the attacker (in this scenario) with the

exact template the security team sends to its end users and, thus, insight into the resources or tools available to them. A malicious actor could then utilize this information to craft a malicious email to the end users, substituting the links or attachments with those of malicious nature from a domain resembling the organization's legitimate one (domain or typo squatting, homograph or Punycode attacks, etc.). A whitelist can be created to allow the templates to be sent only to the organization's domain (and to any other owned or partnered domains for which the cyber security team is responsible).

When an email is mistriaged, as in the above case of an external sender, a report of the potential mistriage should be generated to the SOC mailbox, the lead or manager, and the tool administrator (if necessary). A report generated to the SOC mailbox would give the triaging analyst visibility into a potential mistake he or she made, while the lead or manager should have awareness in the event corrective action (educational or disciplinary) is needed in the event of repeat failure. When there are cases of a false positive, as in the event of a legitimate partnered domain that has not yet been whitelisted or network interruptions, the tool administrator would then have visibility into any technical corrective action needed.

4. Metrics and Security Awareness Training

The final tenants of the CIS Critical Security Controls are "Metrics" and "Continuous diagnostics and mitigation". The knowledge of actual [email] attacks provides the foundation to inform defense and allow for the incorporation of practical defenses to stop known attacks ("Offense informs defense"). "Prioritization" invests in Controls that will provide the greatest risk reduction by implementing feasible measures of defense and "Automation" has been the overarching theme of the event-driven email automation. "Metrics" will provide a shared corporate language to measure the effectiveness of security measures and the "Continuous diagnostics and mitigation" can help test and validate the effectiveness plus drive the priority of next steps in the organization's security awareness training.

4.1 Detection and Response

How would an organization measure the success of event-driven email automation efforts and the correlating security awareness training? Organizations like PhishMe can help identify trends

in phishing risks, including the susceptibility of users to clicking links and/or opening attachments, and the mean time to report a suspected threat once it has been viewed and/or executed by the user. When the user fails the authorized phishing drills, JIT training is presented to him or her, but many exit this quickly or view the materials while continuing to struggle to identify the difference between Legitimate, Spam, and Phishing attempts. Event-driven automation, such as that provided through StackStorm, can help generate a more holistic view as to the successes of cyber security department's efforts.

Statistics can be gathered on multiple facets to measure success. An organization might consider the number of Legitimate vs. Phishing or Spam vs. Phishing emails reported, for example. If a particular business group or the organization as a whole is struggling to identify the difference between Legitimate, Spam, and Phishing emails, this will become evident when the number of triaged emails is assessed. Though it may be difficult to quantify the number of total phishing emails an organization receives by the triaged numbers alone, these numbers can help highlight deficiencies in user education if thousands of Legitimate and Spam messages are reported when only ten phishing emails have been (as an extreme for illustration purposes).

Statistics can be analyzed to ascertain the greatest phishing threats to an organization. An analyst should determine how many phishing emails contain links versus those with attachments (or stripped attachments). An increase of emails containing links may indicate an increase in credential harvesting attempts, potentially leading to security awareness notifications being sent to the organization or efforts being geared towards user education around using unique passwords for every account, incorporating password managers, and enabling Multi-Factor Authentication (MFA) when possible for a two-step verification. An influx of phishing emails containing abnormal (ACE, ALZ, LZH, etc.) or risky (BAT, JS, VBS, etc.) attachment types may warrant a re-evaluation of the file type blocks that are implemented at the edge email appliances. Information gleaned from the most common email threats should be incorporated into upcoming phishing drills too – using like content (attachment names, file types, and/or links) in order to proactively strengthen the defensive stance of an organization's user base.

Mean time can give visibility into an organization's response time to address phishing threats. What is the mean time from detection to response, response to remediation, or remediation to reporting? As Wired author Kim Zetter states, "you've got one minute and 20 seconds to save your company from being hacked. … It's the median time it takes for an employee to open a phishing email … setting in motion a race to prevent data from leaking." (Zetter, 2017). When an end user reports the suspicious message and the analyst triages it as phishing generating a ticket for review and/or remediation, how long does it take for the ticket to be addressed? Verizon evaluated how long it takes an attacker to establish a foothold – "The data showed that nearly 50% of users open e-mails and click on phishing links within the first hour." (Verizon Enterprise, 2015). Messages in phishing campaigns are infrequently sent in an isolated manner – many phishing attempts arriving in waves whereas others may trickle in every few minutes over an hour or two timespan. A timely response process may allow an analyst to create a block for the malicious domain or IP being utilized in the phishing campaign, protecting an organization by preventing any future clicks by unwary users from successfully compromising credentials or a device. The statistics on an organization's mean time to response and remediation may highlight deficiencies in processes or even simply resource allocation concerns.

4.2 Awareness and Protection

Through the collection and evaluation of metrics on the user reporting of suspicious emails, an organization can implement Business Awareness Training to combat the threat of phishing. Continuous diagnostics and mitigation provides an organization with capabilities and tools that identify cyber security risks on an ongoing basis, the ability to prioritize these risks based upon potential impacts, and enables cyber security personnel to mitigate the most significant problems first (U.S. Department of Homeland Security, 2017). The key to success is to know not only the enemy, but to know the organization and its users too:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Tzu & Giles, 1910)

The information gleaned from an event-driven automation solution would allow an organization to move from a reactive or JIT training approach to that of a proactive and targeted approach. Organizations commonly deliver only generic phishing awareness training (addressing the underlying motivators of urgency, emotional response, and the nature of sensitivity). Incorporating statistics from the triaged phishing emails, an organization can not only determine the common threat vectors (email links, attachments, etc.) but also can develop training based on the type of phishing ruses used. Should there be an influx of banking or file sharing credential harvesting attempts seen, examples can be extracted to deliver proactive training. Similarly, if there is an influx of malicious attachments claiming to be Request For Quotes (RFQs) or invoices, an organization could proactively train the affected business groups to be aware of common indicators of malicious intent. Establish a Business Awareness Team (BAT) to manage the event-driven automation platform, creating and updating the templated responses as needed, collecting and evaluating the metrics, then providing dynamic training to the organization. The email triage metrics can help test and validate the effectiveness of an organization's identification, response, and remediation processes plus drive the next steps of the security awareness training.

5. Conclusion

Start preparing the organization to effectively defend against phishing attacks by developing a framework of automation through which users can report suspicious emails with minimal effort, analysts can triage the messages with similar ease, and user education can proactively be delivered. An effective defense requires an organization to be informed by actual attacks (knowing the enemy) and awareness of internal shortcomings (knowing yourself) so that implemented protections and training are applicable to the threats faced (strategy and tactics).

Humans, the weakest link in the security chain, are susceptible to phishing attempts today. The capabilities and sophistication demonstrated by attackers are steadily rising, to the degree that the recent Mandiant's M-Trends 2017 report states "Today, the line between the level of sophistication of certain financial attackers and advanced state-sponsored attackers is not just blurred – it no longer exists." (Mandiant Consulting, 2017). Organizations have seen that, time and time again, users are vulnerable to modern social engineering efforts. Attackers are flourishing through present-day techniques and many organizations are not effectively preparing their users to handle those threats, let alone even considering

preparing them for anything worse. Develop a framework of automation that helps educate the end users and allows for the collect of metrics which can in turn drive tailored training that can help users understand and identify current threats.

The threat landscapes will vary by industry and each approach should be tailored to the specific attacks being leveraged against your organization. In the author's opinion, the benefit of combining automation and training will not only be seen in monetary and time savings to the Information Technology (IT) departments and the organization as a whole, but in the mentality of the end users who are now able to assist in the fight against the cyber-attacks being leveraged against the organization.

References

Anti-Phishing Working Group (APWG). (2016, May 23). Phishing Activity Trends Report. Retrieved April 15, 2017, from [http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf]

Australian Signals Directorate. (2013, July). 'Top 4' Strategies to Mitigate Targeted Cyber Intrusions. Retrieved April 15, 2017, from [https://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf]

Center for Internet Security. (2016, August 31). The CIS Critical Security Controls for Effective Cyber Defense. Retrieved April 15, 2017, from [https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf]

Corson, B. (2014, June 23). Stop Targeted Email Attacks: Removing the Path of Least Resistance for Attackers. Retrieved April 15, 2017, from [http://blog.trendmicro.com/stop-targeted-email-attacks-removing-path-least-resistance-attackers/]

Mandiant Consulting. (2017, March). M-TRENDS 2017. Retrieved May 24, 2017, from [https://www2.fireeye.com/rs/848-DID-242/images/RPT-M-Trends-2017.pdf]

Microsoft. (2017). Send an email message based on a template. Retrieved August 19, 2017, from [https://support.office.com/en-us/article/Send-an-email-message-based-on-a-template-56c645fc-1b25-4059-808b-55ee72b6bc2d]

McSpadden, K. (2015, May 13). You Now Have a Shorter Attention Span Than a Goldfish. Retrieved April 15, 2017, from [http://time.com/3858309/attention-spans-goldfish/]

Polley, S. (2017, February 2). Dissect the Phish to Hunt Infections. Retrieved April 15, 2017, from [https://www.sans.org/reading-room/whitepapers/awareness/dissect-phish-hunt-infections-37587]

Ponemon Institute. (2017, June). 2017 Cost of Data Breach Study: Global Analysis. Retrieved August

27, 2017, from [https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN]

StackStorm. (2017). Event-driven automation. Retrieved April 15, 2017, from [https://stackstorm.com/]

StackStorm. (2017). Installation. Retrieved April 15, 2017, from [https://docs.stackstorm.com/install/]

StackStorm. (2015, September 24). StackStorm 101 - Event-Driven Automation. Retrieved April 15, 2017, from [https://www.youtube.com/watch?v=pzZws3ftDtA]

StackStorm. (2017). StackStorm Exchange. Retrieved April 15, 2017, from [https://exchange.stackstorm.org/]

Symantec Corporation. (2017). Security Awareness Program. Retrieved April 15, 2017, from [https://www.symantec.com/services/education-services/campaigns/security-awareness]

Tzu, S., & Giles, L. (1910). *The Art of War*. Oxford: Clarendon Press.

U.S. Department of Homeland Security. (2017, February 17). Continuous Diagnostics and Mitigation (CDM). Retrieved April 15, 2017, from [https://www.dhs.gov/cdm]

Verizon Enterprise. (2015). 2015 Data Breach Investigations Report. Retrieved April 15, 2017, from [http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf]

Verizon Enterprise. (2016). 2016 Data Breach Investigations Report. Retrieved April 15, 2017, from [http://www.verizonenterprise.com/verizon-insights-lab/dbir/]

Zetter, K. (2016, April 14). Email Phishing Attacks Take Just Minutes to Hook Recipients. Retrieved

April 15, 2017, from [https://www.wired.com/2015/04/email-phishing-attacks-take-just-minutes-hook-recipients/]