



University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Postgraduate Program of Studies
MSc Digital Systems Security

Master's Dissertation Project

Dissertation's Title
Phishing attacks detection and prevention

Supervisor Professor: S. Gritzalis

Name Surname	Email	Student ID
Michael Panorios	michalis.panorios@ssl-unipi.gr	MTE2218

Chapters of Dissertation

Abstract – Περίληψη.....	8
An Introduction to Phishing	9
Phishing Terminology	9
Evolution of Phishing.....	11
Current state & trends of phishing attacks	11
Credential Harvesting Phishing Example	13
Prevention Importance & Consequences	15
Case Study of Phishing	17
Email Components and Communication	18
Email Protocols.....	19
Simple Mail Transfer Protocol - SMTP.....	20
Post Office Protocol - POP3.....	20
Internet Message Access Protocol – IMAP.....	20
Differences Between IMAP & POP3	20
Email Agents.....	21
Mail User Agent – MUA.....	21
Mail Transfer Agent – MTA.....	21
Message Submission Agent – MSA	21
Message Delivery Agent – MDA.....	21
Email Delivery Operation	22
Detailed Email Operation	23
Email Authentication Protocols.....	24
Email Parts and Headers	24
Informational Email Headers	26
Technical Email Headers.....	26
MITRE ATT&CK Framework.....	27
Lab Architecture & Installation	30
Lab Limitations	31
Lab Components	31
Cloudflare Domain	32
Azure Debian 11 Virtual Machine	33
Azure Ubuntu Server 22.04 Virtual Machine	34

Azure Windows 10 Virtual Machine.....	34
Lab Installation	35
Proxmox Mail Gateway Installation.....	35
Private Mail Server Installation	40
Client Thunderbird Installation	50
Elastic Installation	52
Lab Testing.....	67
Phishing Techniques & Detection Methods	71
URL Spoofing.....	72
Spear Phishing.....	73
Whaling	74
Business Email Compromise	75
Vishing.....	75
Clone Phishing.....	76
SMS Phishing.....	76
Pop-up Phishing	77
Social Media Phishing	77
Evil Twin	78
Website Spoofing	78
Elastic Detection	79
Phishing Rules Experiment with Elastic	83
Potential Process Injection from Malicious Document.....	84
Windows Script Executions	85
Windows Script Executing PowerShell.....	86
Suspicious MS Office Child Process.....	86
Suspicious Explorer Child Process.....	87
Execution of File Written or Modified by Microsoft Office.....	88
Suspicious MS Outlook Child Process	89
Suspicious PDF Reader Child Process.....	90
Creation of SettingContent-ms Files	91
O365 Email Reported by User as Malware or Phish	91
Microsoft 365 Exchange Anti-Phish Rule Modification.....	92
Remote XSL Script Execution via COM.....	93

Potential Remote File Execution via MSIEXEC.....	94
Downloaded Shortcut Files	95
File with Suspicious Extension Downloaded.....	95
Microsoft 365 Exchange Safe Link Policy Disabled.....	96
Microsoft 365 Exchange Anti-Phish Policy Deletion	96
Downloaded URL Files	97
Google Workspace Object Copied from External Drive and Access Granted to Custom Application.....	98
Suspicious HTML File Creation	99
Execution of File Written or Modified by PDF Reader	99
Suspicious Execution via Microsoft Office Add-Ins	100
Windows Script Interpreter Executing Process via WMI.....	101
AWS Execution via System Manager	102
Host Isolation with Elastic	102
Proxmox Mail Gateway Controls	104
Mail Gateway Objects	105
ACTION Objects.....	105
WHO Objects.....	106
WHAT & WHEN Objects	107
Phishing and Artificial Intelligence	108
Current practices and future challenges.....	110
OCR Solution for Phishing	111
Conclusion.....	112

Figures of Dissertation

Figure 1 - Phishing attack step-by-step	9
Figure 2 - Percentage of total threat indicators	13
Figure 3 - Credential Harvesting example	14
Figure 4 - Percentages of phishing through 2022	17
Figure 5 - High-risk email threats of 2022.....	18
Figure 6 - Email address structure	19
Figure 7 - Email delivery process between agents.....	22
Figure 8 - Detailed email delivery process	23
Figure 9 - Email headers example on Thunderbird	25
Figure 10 - Email headers sample	26
Figure 11 - MITRE ATTACK framework coverage.....	27
Figure 12 - Phishing for Information tactic	29
Figure 13 - Private mail server architecture.....	31
Figure 14 - Cloudflare DNS records for domain	33
Figure 15 - PMG virtual machine on Azure	33
Figure 16 - Private mail server virtual machine on Azure	34
Figure 17 - Windows client virtual machine on Azure	35
Figure 18 - Mail Server lab details	36
Figure 19 - Proxmox installation through sources	36
Figure 20 - Adding sources to Debian list	37
Figure 21 - Updating Debian to install sources	38
Figure 22 - Port forwarding to access PMG interface	38
Figure 23 - Proxmox Mail Gateway Login interface	39
Figure 24 - Proxmox Mail Gateway graphic user interface	39
Figure 25 - Adding system mail name.....	41
Figure 26 - Accept mail destinations.....	41
Figure 27 - Updates on synchronous queue	42
Figure 28 - Setting up local networks.....	42
Figure 29 - Installing dovecot software.....	43
Figure 30 - Setting protocols on Dovecot configuration file	44
Figure 31 - PMG mail proxy configuration	47
Figure 32 - Relay domains on PMG	47
Figure 33 - Mail Proxy options	48
Figure 34 - Mail transport configuration.....	49
Figure 35 - Email whitelist options.....	50
Figure 36 - POP3 Thunderbird options	51
Figure 37 - Installing Elasticsearch on Ubuntu	53
Figure 38 - Security autoconfiguration information	53
Figure 39 - Elasticsearch system service restart	54
Figure 40 - Response from Elasticsearch	54
Figure 41 - Creating an Elastic enrollment token.....	54
Figure 42 - Enrollment token creation	55
Figure 43 - Kibana installation	55
Figure 44 - Verification of Kibana running on port 5601	55
Figure 45 - Setting up nginx proxy pass	56
Figure 46 - Elasticsearch login page.....	56
Figure 47 - Fleet server installation	57

Figure 48 - Installing Fleet server on the host	58
Figure 49 - Fleet server installation generated command	58
Figure 50 - Adding Windows host on Fleet Server	59
Figure 51 - Fleet Server success installation message	59
Figure 52 - Setting up Elastic Defend integration.....	60
Figure 53 - Folders of Elastic on Windows host	61
Figure 54 - Missing API integration key.....	61
Figure 55 - Generating Kibana encryption keys	61
Figure 56 - Adding encryption keys on yaml file	62
Figure 57 - Predefined Elastic Rules.....	63
Figure 58 - Table of Elastic's default rules.....	63
Figure 59 - Windows sysmon integration module	64
Figure 60 - Installing sysmon executable on Windows	65
Figure 61 - Configuration of Windows integration	65
Figure 62 - Creating a data view	66
Figure 63 - Log collection panel	66
Figure 64 - Elastic detection of calc.exe test.....	67
Figure 65 - Test email for transfer	68
Figure 66 - Proxmox Tracking Center of the above email	68
Figure 67 - Mail managed to reach mail server	69
Figure 68 - Thunderbird sync with mail server	70
Figure 69 - Email reached the destination	70
Figure 70 - URL Spoofing examples.....	72
Figure 71 - URL Spoofing of National Bank of Greece	73
Figure 72 - Spearphishing example.....	74
Figure 73 - Whaling example	74
Figure 74 - SMS Phishing example	76
Figure 75 - Elastic MITRE ATT&CK Coverage of Phishing	82
Figure 76 - Outlook phishing example	83
Figure 77 - Public drive phishing example	83
Figure 78 - Potential Process Injection from Malicious Document query	84
Figure 79 - Windows Script Executions query	85
Figure 80 - Windows Script Executing PowerShell query	86
Figure 81 - Suspicious MS Office Child Process query	86
Figure 82 - Suspicious Explorer Child Process query.....	87
Figure 83 - Execution of File Written or Modified by Microsoft Office query.....	88
Figure 84 - Suspicious MS Outlook Child Process query.....	89
Figure 85 - Suspicious PDF Reader Child Process query	90
Figure 86 - Creation of SettingContent-ms Files query	91
Figure 87 - O365 Email Reported by User as Malware or Phishing query	91
Figure 88 - Microsoft 365 Exchange Anti-Phish Rule Modification query	92
Figure 89 - Remote XSL Script Execution via COM query.....	93
Figure 90 - Potential Remote File Execution via MSIEXEC query	94
Figure 91 - Downloaded Shortcut Files query.....	95
Figure 92 - File with Suspicious Extension Downloaded query	95
Figure 93 - Microsoft 365 Exchange Safe Link Policy Disabled query	96
Figure 94 - Microsoft 365 Exchange Anti-Phish Policy Deletion query	96
Figure 95 - Downloaded URL Files query	97

Figure 96 - Google Workspace Object Copied from External Drive and Access Granted to Custom Application query	98
Figure 97 - Suspicious HTML File Creation query.....	99
Figure 98 - Execution of File Written or Modified by PDF Reader query	99
Figure 99 - Suspicious Execution via Microsoft Office Add-Ins query.....	100
Figure 100 - Windows Script Interpreter Executing Process via WMI query	101
Figure 101 - AWS Execution via System Manager query	102
Figure 102 - Elastic host isolation on Elastic Defender panel	103
Figure 103 - Releasing isolated hosts.....	104
Figure 104 - Default rules of Proxmox	105
Figure 105 - Action objects of rules	106
Figure 106 - Who objects of rules.....	106
Figure 107 - What objects of rules.....	107

Abstract – Περίληψη

The following thesis constitutes the final segment of postgraduate studies within the framework of the "Digital Systems Security" program of the Department of Digital Systems at the University of Piraeus. The chosen topic for this thesis involves the study of phishing attacks, their structural elements, as well as their recognition within the context of networked environments using contemporary methods and techniques employing enterprise digital security solutions. From the early years of internet usage, attackers attempted to exploit humans to achieve their goals. For this purpose, they employed methods of digital phishing. Through this means, malicious actors effectively deceived internet users. Over the years, the technology and methods of such attacks have evolved. Today, it constitutes the primary cause of cyber intrusions. Organizations and individuals use tools and appropriate measures to recognize phishing attacks, thereby avoiding unwanted accesses and deceptions by attackers. The objective of this thesis is to analyze phishing methods as well as detection techniques. Within this scope, the results and impact of countermeasures were evaluated within a virtual laboratory created for this purpose. Finally, particularly crucial is the education of internet users in addressing phishing attacks.

Η ακόλουθη διπλωματική εργασία αποτελεί το τελευταίο σκέλος των μεταπτυχιακών σπουδών στα πλαίσια του προγράμματος «Ασφάλεια Ψηφιακών Συστημάτων» του τμήματος «Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς. Το θέμα που επιλέχθηκε για την εκπόνηση της διπλωματικής εργασίας αφορά την μελέτη των επιθέσεων phishing, των δομικών τους στοιχείων καθώς και την αναγνώριση τους σε δικτυακά περιβάλλοντα με σύγχρονες μεθόδους και τεχνικές χρησιμοποιώντας λύσεις ασφάλειας ψηφιακών συστημάτων. Από τα πρώτα χρόνια της χρήσης του διαδικτύου οι επιτιθέμενοι προσπαθούσαν να εκμεταλλευτούν την ανθρώπινη ψυχολογία προκειμένου να επιτύχουν τον σκοπό τους. Για τον λόγο αυτό, εξελίχθηκαν πολλοί μέθοδοι ψηφιακού ψαρέματος. Με αυτόν τον τρόπο, οι επιτιθέμενοι κατάφεραν αποτελεσματικά να εξαπατούν του χρήστες του διαδικτύου. Με την πάροδο των ετών η τεχνογνωσία και οι μέθοδοι τέτοιων επιθέσεων εξελίχθηκαν. Σήμερα, αποτελεί την κυριότερη αιτία επιθέσεων στον κυβερνοχώρο. Οργανισμοί, εταιρείες, αλλά και άνθρωποι ως απλοί χρήστες χρησιμοποιούν εργαλεία και κατάλληλα αντίμετρα προκειμένου να αναγνωρίζουν phishing επιθέσεις έτσι ώστε να αποφεύγονται οι ανεπιθύμητες προσβάσεις και εξαπατήσεις από τους επιτιθέμενους. Στόχος της διπλωματικής εργασίας είναι να αναλυθούν οι μέθοδοι ηλεκτρονικού ψαρέματος καθώς και μέθοδοι εντοπισμού τους. Στα πλαίσια αυτής, τα αποτελέσματα και η επίδραση των αντιμετρώων ελέγχθηκαν μέσα σε ένα εικονικό εργαστήριο το οποίο δημιουργήθηκε για τον έλεγχο των δυνατοτήτων τους. Τέλος, ιδιαίτερη σημασία πρέπει να δοθεί στην επιμόρφωση των χρηστών του διαδικτύου ως προς την αντιμετώπιση των επιθέσεων ψαρέματος.

An Introduction to Phishing

Phishing is an unauthorized cyber-attack strategy that manipulates individuals into disclosing sensitive information or engaging in destructive actions and has become an ever-present threat in modern digital ecosystem. The following dissertation presents an overview of the current state of phishing assaults, the growth in response to technical advancements and the countermeasures used to limit their impact. Phishing attacks have evolved from simple, text-based email frauds to sophisticated, multi-vector campaigns utilizing social engineering, malware, and AI-driven methods for cybercriminals to achieve their goals. To trick victims into providing personal and financial information, hackers may exploit psychological vulnerabilities, target groups of people, and utilize convincing clones of legitimate websites and services.

Phishing Terminology

Phishing is a form of cybercrime in which victims get contacted by an individual or group of people posing as a reputable institution by email, phone, or messaging. The objective of this scheme is to trick victims into disclosing sensitive information like as personal, bank account, credit card information, and passwords. The data is then utilized to identify and fraud their targets. Phishing employs manipulation as its primary tactic. Messages delivered by text, email, or social media are frequently crafted with the purpose of instilling anxiety and a sense of urgency. Public sources of information, such as social media, are used to identify targets. After identifying the target names, work titles, personal information, and email addresses, believable messages are created and sent. These communications frequently contain a malicious link, attachment, or a request for sensitive information.

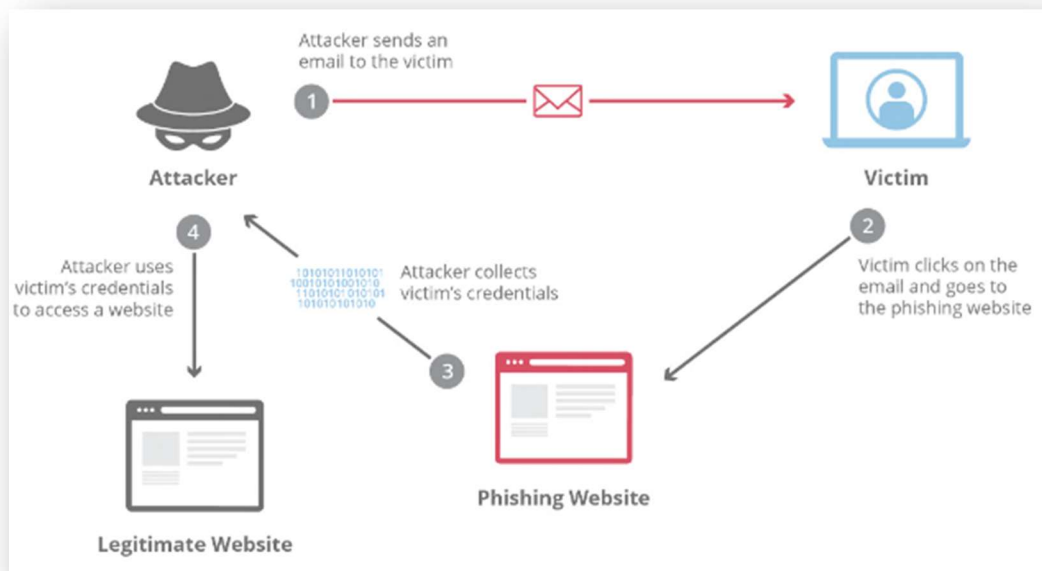


Figure 1 - Phishing attack step-by-step

There are different types of phishing¹. A list of the most common types of phishing frauds and how they occur will be described. The types of phishing are:

- **Email phishing** is the most common type of phishing in which the victims receive emails informing them that their personal accounts have been compromised and immediate response is required. Email phishing aims to create a sense of urgency and make the victim click on a malicious link that leads to a fake login page. Sensitive personal information is delivered straight to the scammers.
- **Spear phishing / Whaling** is used in targeting specific individuals, groups, and organizations. Spear phishing often involves research on the target and publicly available sources of information. The goal of spear phishing is to gain access to an individual account or impersonate high-ranking staff as well as staff in possession of confidential information. An email including the target's name, rank, and an attachment is usually sent to carry out spear phishing. Whaling is a type of spear phishing that is usually directed at top-level executives. The scammers pretend to be legitimate sources, and they encourage victims to share sensitive information or wire large amounts of money.
- **Business Email Compromise (BEC)** is a form of spear phishing attack aimed at extracting substantial amounts of money or highly valuable data, such as trade secrets, customer information, or financial data, from corporations or institutions. BEC compromise can occur with variety of social engineering methods such as CEO fraud where the scammer impersonates a C-level executive's email account, or hacks into it directly, and sends a message to a lower-level employee instructing them to transfer funds to a fraudulent account, make a purchase from a fraudulent vendor, or send files to an unauthorized party.
- **Smishing**, otherwise known as SMS phishing, is a form of phishing in which victims are deceived to click a link or provide private information through text messaging. Smishing is done with the use of basic target information such as name, age, and location. If a link is included in the text message, it may lead to a fake website or malware designed to compromise the phone. The malware may be used to snoop on the users' phone data or send sensitive data to an attacker-controlled server. Smishing comes in different forms: from messages stating that you are in trouble, to messages showing you have won a parcel.
- **Vishing or voice phishing**² is a form of phishing in which the victims are manipulated into revealing personal information like bank details and credit card numbers through phone calls and voice messages. In most cases, the scammers pretend to be from reputable organizations like banks, tax departments, police, or the government. Vishing is done by using threats and convincing language to make the victims believe that they must call back immediately or face the risks of being arrested and losing bank accounts.
- **Evil twin phishing** Evil twin phishing involves the setup of a Wi-Fi access point that disguises as a legitimate one to gain access to sensitive information without the victim's knowledge. Scammers observe the details of a legitimate Wi-Fi access point and create an identical access point with

¹ Hadnagy, C., & Schulman, S. (2021). *Human hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You*. Harper Business.

² Park, H., Kim, J. B., & Bae, M. (2018). Prevention of Voice Phishing through Analysis of Telephone Call Voice Characteristic. *International Journal of Engineering & Technology*, 7(3.33), 62.
<https://doi.org/10.14419/ijet.v7i3.33.18525>

the same name. Victims connect to the Wi-Fi access point and the evil twin Wi-Fi becomes their wireless AP. Hackers can then intercept sensitive data such as login information, bank details, or credit card information.

- **Social media phishing** is a form of phishing that employs the use of social media platforms such as Facebook, LinkedIn, Twitter, Instagram, etc., to deceive victims into revealing sensitive data. On some occasions, these phishing frauds occur when victims receive messages asking them to pay for followers. On other occasions, the messages could include malicious links to a fake social media login page. On login, the victim's credentials are saved for impersonation and access to financial and personal information.

Evolution of Phishing

Phishing techniques date back to the 1990s, when black hat hackers and members of the known Warez community exploited AOL to steal credit card information and perform other online crimes. The term "phishing" is reported to have been coined by Khan C. Smith, a well-known hacker, and its first recorded use was in the 1995 hacking program named AOHell which enabled hackers to imitate AOL employees and send instant messages to victims requesting credentials. As a result, AOL instituted anti-phishing measures and eventually shut down the Warez on their platform. Phishing assaults become increasingly coordinated and specialized in the 2000s. The first documented direct effort against a payment system, E-gold, happened in June 2001, and a "post-9/11 id check" phishing attack followed shortly after the September 11 attacks. In September 2003, the first recorded phishing attempt against a retail bank was reported. Between May 2004 and May 2005, roughly 1.2 million computer users in the United States experienced damages of around 929 million US dollars because of phishing. Phishing was identified as a fully organized part of the illegal market, and specializations built on a global scale that provided phishing software for money, which organized gangs gathered and deployed into phishing campaigns. The number of phishing attacks increased significantly in the 2010s. A phishing assault in 2011 stole the master keys for RSA SecurID security tokens. Chinese phishing attacks also targeted high-ranking officials in the governments and militaries of the United States and South Korea, as well as Chinese political activists. These ongoing drastically phishing events have made clear that this threat will be major in the upcoming years. As demonstrated on July 15, 2020, Twitter breach, phishing attempts have broadened to include elements of social engineering. A 17-year-old hacker and his collaborators created a fake website that replicated Twitter's internal VPN service, which was utilized by remote working workers. Posing as helpdesk representatives, they called several Twitter employees and directed them to the bogus VPN website. They were able to take control of many high-profile user accounts, including those of Barack Obama, Elon Musk, Joe Biden, and Apple Inc.'s company account, using the information provided by the unknowing employees³.

Current state & trends of phishing attacks

Considering the continuously advancing nature of technology and the expanding digital landscape, the current state of phishing attacks is becoming even more sophisticated and prevalent. Social engineering strategies and spoofing techniques are increasingly being used by cybercriminals to

³ Gupta, B.B., Tewari, A., Jain, A.K. et al. Fighting against phishing attacks: state of the art and future challenges. *Neural Comput & Applic* 28, 3629–3654 (2017).

deceive unsuspecting users into disclosing sensitive information such as personal credentials, financial data, or confidential company's information. Furthermore, with the advent of remote work and a greater reliance on digital communication and transactions, the potential for phishing assaults has been increased, posing a substantial threat to both individual users and organizations.

Nowadays, it is claimed that 90% of successful cyber-attacks begin with email phishing, which is still profitable for attackers. Today, there is not much that can be done to prevent phishing attempts besides email analysis robust user education programs that raise awareness about common phishing tactics. However, to prevent successful attacks, it is critical to recognize (and solve) growing phishing trends, such as how attackers exploit intended victims' faith in "known" email senders. Attackers typically use a combination of social engineering and technical obfuscation techniques to make their messages seem legitimate⁴. For that reason, to identify phishing emails, there are methods which a user and large organizations can implement such as:

- Employing heuristics and machine learning models tailored for phishing cues to conduct structural scrutiny of headers, body content, images, links, attachments, payloads, and other elements.
- Utilizing sentiment analysis to identify alterations in patterns and behaviors, such as changes in writing styles and expressions.
- Assessing trust graphs to analyze partner social connections, email transmission records, and the likelihood of partner impersonation.

Advanced threat detection systems, including email filters, anti-phishing software, and AI-driven anomaly detection, play a crucial role in identifying suspicious emails, links, and websites commonly associated with phishing attempts. These systems often analyze various attributes of incoming messages, such as sender reputation, message content, and embedded URLs, to assess their legitimacy and potential threat level. Below snapshot is an example of threat detection categories because of Cloudflare's research which took place from May 2022 to May 2023.

⁴ Dzuba, E. (2023, October 26). Introducing Cloudflare's 2023 phishing threats report. Retrieved from <https://blog.cloudflare.com/2023-phishing-report/>

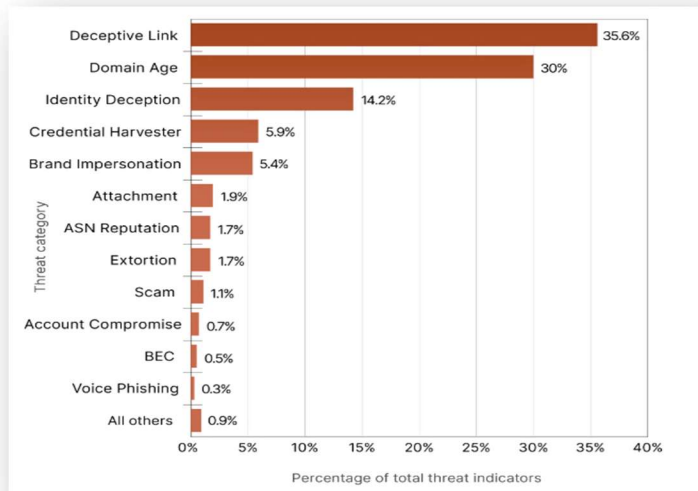


Figure 2 - Percentage of total threat indicators

When a victim clicks on a link in a phishing email, it can lead to the opening of a deceptive webpage in the user's default web browser, displaying data referenced in the link, or directly launching an application, such as a PDF viewer. Attackers can manipulate the display text of a hyperlink in HTML to make a URL appear innocuous, even when it leads to a malicious site. The age of a domain is linked to its reputation score, which reflects its overall trustworthiness. For instance, domains that rapidly send out numerous emails soon after registration typically have a lower reputation score due to suspicious activity. Identity deception involves an attacker or malicious actor sending an email under false pretenses, claiming to be someone else. The techniques and strategies employed in such deception can vary widely. Some tactics include registering domains that look similar (aka domain impersonation), are spoofed, or use display name tricks to appear to be sourced from a trusted domain. An attacker sets up credential harvesters to trick users into surrendering their login credentials. **Brand impersonation** is a type of identity theft in which an attacker sends a phishing message impersonating a well-known firm or brand. A variety of tactics are used in brand impersonation. An **email attachment** that, when viewed or run in the context of an attack, contains a call-to-action (e.g., entices the target to click a link) or conducts a series of actions determined by the attacker.

To combat the growing threat of phishing attacks in the modern digital era, individuals and organizations must remain vigilant and proactive in implementing robust cybersecurity measures such as regular security awareness training, advanced email filtering systems, and multifactor authentication.

Credential Harvesting Phishing Example

Cloudflare detected and banned a phishing campaign exploiting the Microsoft brand to harvest credentials via a legitimate - but compromised - site in early 2023.

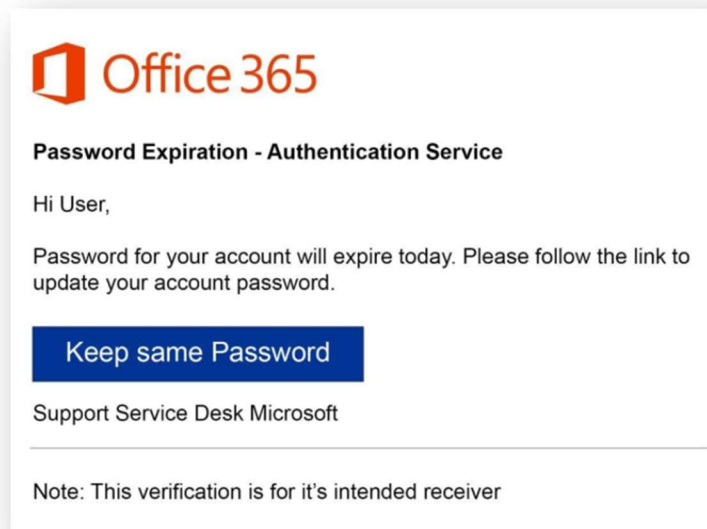


Figure 3 - Credential Harvesting example

Despite its appearance, there is no text in the body of the email in the sample below. The entire body is a JPEG image that is hyperlinked. Thus, even if the recipient does not intend to click the link, they are functionally clicking it if they click anywhere in the body.

The image's linked looks to be an unimportant Baidu URL:

[http://www.baidu\[.\]com/link?url=-yee3T9X9U41UHUa3VV6lx1j5eX2Eol6XpZqfDgDcf2NYQ8RVpOn5OYkDTuk8Wg#<recipient's email address base64 encoded>](http://www.baidu[.]com/link?url=-yee3T9X9U41UHUa3VV6lx1j5eX2Eol6XpZqfDgDcf2NYQ8RVpOn5OYkDTuk8Wg#<recipient's email address base64 encoded>)

If the target clicks on this link, the browser is forwarded to a compromised site that is hosting a credential harvester. The attacker employed Microsoft Office 365 branding but tried to avoid detection by embedding the brand information within the image (i.e., there was no plaintext or HTML content that could be analyzed to identify the brand). Nevertheless, through the application of optical character recognition (OCR), Cloudflare effectively detected instances of "Office 365" and "Microsoft" within the image. This OCR technology enabled the identification of suspicious account enticements associated with passwords. In this scenario, the attackers employed the following techniques: **Inclusion of only a JPEG image** (impossible to detect words without OCR)

- Embedding a hyperlink within the image, where clicking anywhere in the image body would activate the link.
- Hyperlinking to a Baidu URL, a tactic utilized to evade reputation-based URL detection methods.
- Directing the recipient's browser to a credential harvesting site through the Baidu URL redirection, effectively bypassing email security measures that lack deep link inspection capabilities. Hosting the credential harvester on a legitimate site that had been compromised by the attacker (even with deep link inspection, will again attempt to bypass URL detection techniques based on reputation)

This attack vector exploits the strong reputation and authenticity of Baidu to circumvent the reputation checks of the genuine host/IP where the credential harvester is located. While this attempt focused on stealing Microsoft credentials, attackers use similar approaches to circumvent brand identification and deceive victims into downloading malware and other harmful payloads. URL redirection tactics are frequently used in phishing campaigns, but threat actors are refining their approach by abusing increasingly valid domains such as baidu.com, bing.com, goo.gl, and so on. Extensive detection skills enable cyber security analysts to do deep link examination of URLs utilizing various redirection strategies, including those that exploit genuine domains.

Prevention Importance & Consequences

Phishing attacks, a form of cybercrime that involves the fraudulent acquisition of sensitive information through deceptive electronic communications, have increasingly significant consequences in the digital era. These malicious attempts to deceive individuals into disclosing personal information or executing harmful actions have grave repercussions for both individuals and organizations. From financial losses and identity theft to compromised data security and damaged reputations, the aftermath of successful phishing attacks can lead to profound disruptions in personal and business realms, highlighting the urgent need for robust cybersecurity measures and heightened awareness among internet users⁵. The cost of a phishing attack can be grave depending on the attack scope. More specifically,

1. Loss of Data

Clicking on a malicious link in an email can provide a hacker access to an organization's data and system. They are then free to do anything they want, including stealing for further illegal reasons, data corruption, and data deletion. The most serious consequence of phishing assaults is data loss.

2. Damaged Reputation

Companies suffer reputational damage because of a data breach caused by phishing attempts. When a breach is announced, the public loses trust in the company. Regardless of an organization's past reputation, data breaches have a significant negative impact on its brand, and it may be perceived as untrustworthy for a long period after a successful hack. It could result in a public backlash against a corporation for failing to do enough to protect users' data. Direct Monetary Loss

3. Direct Monetary Loss

Further costs will be required to manage identity protection and compensation for consumers or workers whose data was taken because of a phishing attempt. Funds could also be transferred out of a company's account using phishing impersonation.

4. Loss of Productivity

Data breaches or system compromise caused by phishing attempts hurt company. Following a successful phishing assault, a significant portion of a company's time will be spent attempting to retrieve

⁵ Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something Smells phishy: Exploring definitions, consequences, and reactions to phishing. *Proceedings of the Human Factors and Ergonomics Society . . . Annual Meeting*, 56(1), 2108–2112. <https://doi.org/10.1177/1071181312561447>

stolen data and investigating the breach, leaving little time for actual business. Employee productivity will suffer when numerous systems are brought down for reconfiguration and cleaning.

5. Loss of Customers

A successful phishing attack drives customers away from a company. According to a UK survey, more than half of consumers stop doing business with a compromised organization for several months after a data breach while 41% of customers no longer shop firms whose data has been compromised. This effect might linger for a long time in an organization.

6. Financial Penalties

When sensitive consumer data becomes public, the impacted company is held accountable. In addition to the immediate monetary loss from failing to fight against phishing, a firm may face substantial regulatory fines for mishandling consumer data.

The fines are aimed at organizations who do not adhere to best practices for securing their customers' personal information. Violations of regulatory regulations like as HIPAA, PCI, and the European GDPR may result in significant fines. The severity of the fines is determined by the industry and the breadth of the breach.

7. Intellectual Property Theft

A business asset is not only about money or equipment, but intellectual property could also even be more important. Intellectual property may be stolen through phishing attacks and could even be the motivation for the attack in the first place.

8. Loss of Company Value

Phishers can also cost a company a significant part of its market value because of the loss of investors' confidence. Some investors would no longer trust the affected organization and may move their funds elsewhere to protect their portfolio. A phishing attack can have multiple negative effects on an organization. This may include data loss, compromised credentials, ransomware, and malware infestation. It is pertinent that you prioritize employee cybersecurity education, install advanced security solutions, and implement policies that will block phishing attempts and protect businesses from the impacts.

Case Study of Phishing

In 2022, the global cybersecurity landscape was fulfilled with threat actors, revealing the daunting extent of digital vulnerabilities. Reports unveiled a disquieting surge in cyber threats, including a disheartening 384,000 instances of Business Email Compromises, 4.2 million malicious emails leading unsuspecting users to the treacherous precipice of malware, and a staggering 35.2 million malicious phishing URLs⁶. Approaching the forthcoming years, it is disquieting to contemplate the potential trajectory of these numbers. With the proliferation of sophisticated cybercrime tactics and the increasingly interconnected nature of our digital infrastructure, experts project a worrisome escalation in these figures, cautioning against a potential exponential rise in Business Email Compromises, a manifold surge in malware-infected emails, and an alarming proliferation of malicious phishing URLs, signaling an urgent need for heightened cybersecurity measures and resilient digital defense mechanisms in the years ahead.

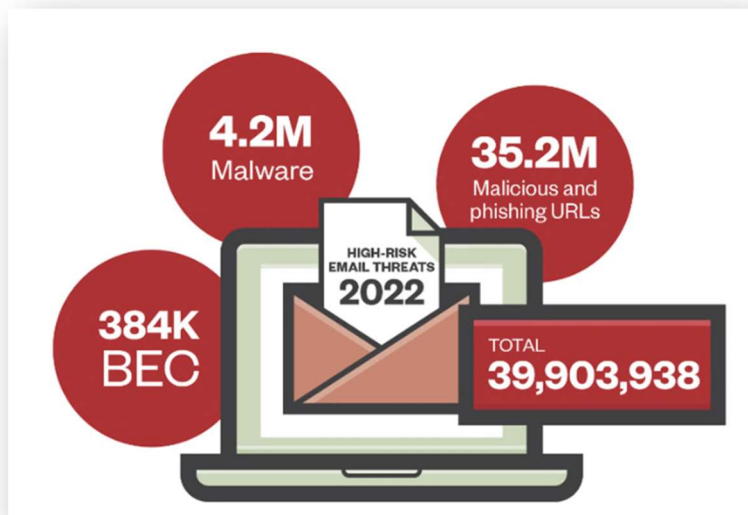


Figure 4 - Percentages of phishing through 2022

The evolving landscape of high-risk email threats is characterized by a complex interplay of known and unknown perils, resulting in a dynamic challenge for cybersecurity professionals. Notably, recent statistics paint a nuanced picture: while there has been a commendable 32% decrease in the detection of known malware, an alarming 46% surge in the detection of unknown malware underscores the growing sophistication of covert phishing attacks. Moreover, the unsettling revelation of a 35% increase in Business Email Compromise (BEC) detections, coupled with a concerning 29% rise in phishing

⁶ Worldwide 2022 Email Phishing Statistics and Examples. (2023, May 31) (https://www.trendmicro.com/en_us/ciso/23/e/worldwide-email-phishing-stats-examples-2023.html)

detections, exemplifies the persistent threat posed by targeted email-based intrusions. As organizations grapple with these escalating risks, a noteworthy 4% uptick in credential phishing detections serves as a stark reminder of the critical importance of robust authentication protocols. Most notably, the staggering 205% surge in credential phishing detections facilitated through AI-based computer vision underscores the change in basic assumptions towards increasingly sophisticated and automated cyber threats, highlighting the urgent need for adaptive and proactive defense strategies in the realm of email security.

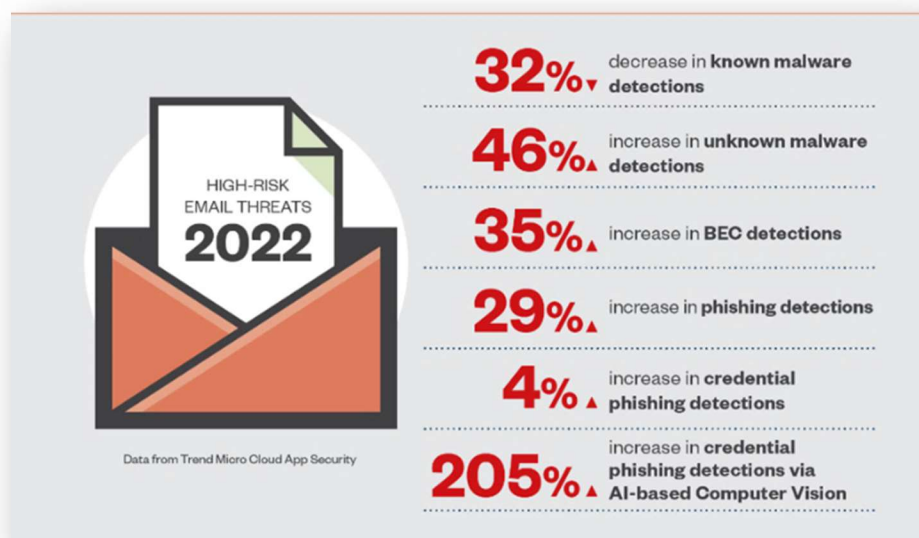


Figure 5 - High-risk email threats of 2022

Predicting the exact trajectory of social engineering, particularly phishing attacks, in the coming years involves considering the existing trends and potential technological advancements. Statistically, the evolution of phishing attacks is likely to follow an upward trajectory, fueled by the integration of advanced technologies and the growing sophistication of cybercriminals. According to industry forecasts, a projected 40% increase in targeted phishing attacks is anticipated over the next three years. Additionally, the proliferation of AI-driven phishing techniques is expected to contribute to a staggering 60% rise in AI-enabled social engineering attacks, leveraging increasingly sophisticated algorithms to deceive unsuspecting users. With the continued integration of deep learning and natural language processing, experts anticipate a 35% surge in personalized phishing attacks, tailored to exploit specific individual vulnerabilities, further amplifying the effectiveness and success rate of these malicious campaigns. As cybercriminals continue to adapt and innovate, the convergence of social engineering with emerging technologies poses an ominous threat to cybersecurity, necessitating an initiative-taking and multifaceted defense approach to mitigate the escalating risks associated with these evolving phishing tactics.

Email Components and Communication

Email was invented before the internet is nowadays. Email was designed to allow computers to communicate with one another. ARPANET, a computer communications network founded by the United

States Department of Defense, devised a method of email exchanges in the early 1960s that depended on the known "@" sign. Ray Tomlinson, widely credited with inventing email as the world knows it, chose the @ symbol on purpose. That is because the @ sign did not appear in names, there was no confusion about where the distinction between login name and hostname occurred.

The @ symbol allowed messages to be sent to specified users on specific machines rather than to localhost. The email address was now formatted as **username@domain.tld**. This separation of usernames and host names works in the same way that website IP addresses are assigned domain names. Email addresses took the format once the domain name system (DNS) was created.

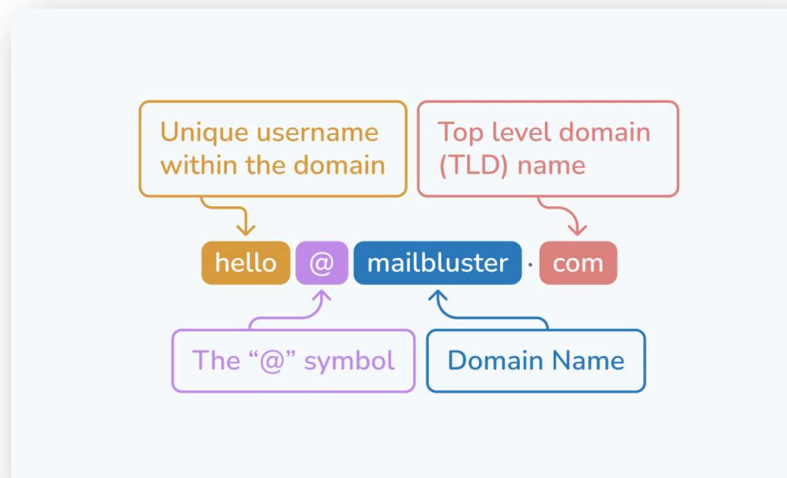


Figure 6 - Email address structure

Emails are routed to user accounts between different computer servers. They transport the messages to their destination and store them so that users can retrieve and send them whenever they connect to the email service. An email can be viewed using an email client or a web interface. When the send button is pressed, the message is sent from a computer to the server connected with the recipient's email address. Before the message reaches its intended recipient's mailbox, it often passes through numerous different servers. Electronic mailboxes are critical to how emails function for end users. When a user receives an email, the mail system immediately forwards it to mailbox. The inbox improves the usability of emails. They can be organized into folders, such as inbox, outbox, and junk, and let users to scan, copy, delete, or forward mail to another user.

Email Protocols

Email protocols are intricate systems that govern the exchange of electronic messages between users, servers, and email clients, enabling the seamless transfer and management of data across the internet. These protocols consist of a series of rules and standards, including SMTP, POP3, and IMAP, which dictate how emails are sent, received, and accessed. Employing sophisticated communication mechanisms, encryption techniques, and authentication procedures, these protocols ensure the secure and reliable transmission of emails, catering to the diverse needs of users and organizations while upholding the integrity and confidentiality of digital communications.

Simple Mail Transfer Protocol - SMTP

Unlike the physical mailboxes, where one service, the post office, manages all the mails, the incoming and outgoing mails are being handled differently with email. There are two types of servers. The Simple Mail Transfer Protocol (SMTP) is indeed an email delivery protocol utilized for sending mail across the internet. SMTP provides informative details regarding the transmission data of an email message and for outgoing mail. It operates on port 25 and on port 587 for encrypted communications as an authenticated relaying.

Post Office Protocol - POP3

POP3⁷ is an old protocol that was originally designed to be used only on a computer. POP3 only supports one-way e-mail synchronization, allowing users to receive e-mail only from one server to one client computer. Because of this feature, POP3 accounts lack most of the basic features found in more modern services, such as:

- The ability to mark a message as read on multiple devices.
- The ability to send data from multiple devices. Sent items cannot be synchronized using POP and can only be stored on the device they came from.
- The ability to forward emails to your device as they arrive. Instead, your device must be set to automatically periodically check your email server to see if new messages have been received.
- The ability to make folders created or settings defined on one device available to all devices using that email account. By using the POP protocol, users must create or configure these parameters individually on all their devices. This means that if users organize their email on one device, they will need to do it again for every other device that uses the POP email account.

Internet Message Access Protocol – IMAP

With IMAP⁸ accounts, messages are stored on a remote server. Users can log in through multiple email clients on computers or mobile devices and read the same messages. All changes made to the mailbox will be synchronized across multiple devices and messages will be removed from the server only if the user deletes the email.

- Connecting to multiple computers and devices at the same time.
- Email files are synchronized and stored on the server so you can access them from all connected devices.
- Both incoming & outgoing emails are stored on the server until the user chooses to delete t.

Differences Between IMAP & POP3

POP3 (Post Office Protocol 3) and IMAP (Internet Message Access Protocol)⁹ both are message accessing agents, both protocols are used to retrieve messages from the mail server to the receiver's system. Both protocols are accounted for spam and virus filters. IMAP is more flexible and complex than POP3.

⁷ Wikipedia (2023, August 18). Post office protocol. Wikipedia. https://en.wikipedia.org/wiki/Post_Office_Protocol

⁸ Wikipedia (2023, October 11). Internet Message Access Protocol. Wikipedia. https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

⁹ Differences between POP3 and IMAP. GeeksforGeeks <https://www.geeksforgeeks.org/differences-between-pop3-and-imap/> (2019, April 26).

Email Agents

Architectural email agents are complex systems composed of multiple interconnected components, including user interfaces, email servers, databases, and network protocols. These components work in together to ensure the efficient management, storage, and retrieval of email messages, to fulfill the needs of users and organizations. The architecture of these agents is designed to oversee a high volume of emails securely, while also providing functionalities such as filtering, categorization, and integration with other applications and services for a comprehensive user experience.

Mail User Agent – MUA

A Mail User Agent (MUA), also referred to as a mailbox, is a computer application that allows users to send and retrieve email¹⁰. A MUA is what a user interacts with, as opposed to an email server, which transports email. MUAs could be software applications, such as Microsoft Outlook, or they can be webmail services such as those provided by Gmail or Yahoo. Mail User Agent are the components where the Simple Mail Transfer Protocol is responsible for creating email messages to be provisioned to a Mail Transfer Agent (MTA).

Mail Transfer Agent – MTA

Also referred to as mail server, mail exchanger, and MX host, MTA is a software that routes a mail message towards its destination by sending the message to another MTA¹¹. The MTAs communicate with each other via SMTP. It is sometimes referred to as SMTP Server. Examples of MTAs used in mail carrier are Postfix and Sendmail.

Message Submission Agent – MSA

A message submission agent (MSA), also known as a mail submission agent, is a software program or agent responsible for receiving electronic mail messages from a mail user agent (MUA) and working together with a mail transfer agent (MTA) to deliver the mail. It utilizes ESMTP, a variation of the Simple Mail Transfer Protocol (SMTP). It is worth noting that while many MTAs also perform MSA functions, there are programs specifically designed as MSAs without full MTA capabilities. Traditionally, both MTA and MSA functions operate on port number 25 in Internet mail, but the designated port for MSAs is 587. The MTA handles incoming mail from users, whereas the MSA manages outgoing mail from users.

Message Delivery Agent – MDA

A message delivery agent (MDA)¹², or mail delivery agent, is a computer software component that is responsible for the delivery of e-mail messages to a local recipient's mailbox. Also, it is called a local delivery agent (LDA). In the architecture of Internet mail, local message delivery occurs through a process that involves handling messages from the message transfer agent (MTA) and storing mail into the recipient's environment.

¹⁰ Mail User Agent (MUA) – LibraEsva Docs. (n.d.). <https://docs.libraesva.com/glossary/mail-user-agent-mua/>

¹¹ Wikipedia (2024, January 22). Message transfer agent. Wikipedia.
https://en.wikipedia.org/wiki/Message_transfer_agent

¹² Wikipedia contributors. (2023c, September 25). Message delivery agent. Wikipedia.
https://en.wikipedia.org/wiki/Message_delivery_agent



Figure 7 - Email delivery process between agents

Email Delivery Operation

Email messages are sent from a mail client (mail user agent, MUA) to a mail server (mail submission agent, MSA) via SMTP over TCP port 587, although many mailbox providers still permit submission on the conventional port 25. The MSA then transfers the email to its mail transfer agent (MTA), often employing the same software as the MSA, with different configurations on the same device. Local processing can occur on a single machine or be distributed across multiple machines, allowing mail agent processes on one device to share files, while those on different devices transfer messages using SMTP, configured to use the subsequent device as a smart host. Each process operates as an MTA (an SMTP server) independently.

The boundary MTA relies on DNS to search for the MX (mail exchanger) record corresponding to the recipient's domain (the part after the @ symbol in the email address). This record includes the target MTA's name. Considering the target host and other criteria, the sending MTA selects a recipient server and establishes a connection to complete the email exchange.

Message transfer¹³ occur in a direct connection between two MTAs or through a series of hops via intermediary systems. The receiving SMTP server can serve as the destination, an intermediate "relay" that stores and forwards the message, or a "gateway" that forwards the message using a protocol other than SMTP.

Upon acceptance by the final hop, the incoming message is handed over to a mail delivery agent (MDA) for local delivery. An MDA stores messages in the relevant mailbox format. Like the sending process, this reception can be managed by one or multiple computers, as depicted in the diagram, where the MDA is illustrated as a single box near the mail exchanger. An MDA might deliver messages directly to storage or transmit them over a network using SMTP or another protocol like the Local Mail Transfer Protocol (LMTP), a variation of SMTP designed for this purpose.

Once stored on the local mail server, the mail is retained for batch retrieval by authenticated mail clients (MUAs). End-user applications, known as email clients, use either the Internet Message Access Protocol (IMAP) for accessing and managing stored mail or the Post Office Protocol (POP), which typically operates using the traditional mail file format or proprietary systems like Microsoft Exchange/Outlook. SMTP's role is to define message transport, excluding the message content itself. It outlines the mail envelope and its parameters, including the envelope sender, but does not dictate the message header (apart from trace information) or the message body.

¹³ How email works - An overview of what happens behind the email. (n.d.). Zoho. <https://www.zoho.com/mail/help/how-email-works.html>

Detailed Email Operation¹⁴

The sequence of events that unfold when sender Alice sends a message using a mail user agent (MUA) addressed to Bob's recipient email address typically proceeds as follows:

1. The **MUA** formats the message into an email format and employs the submission protocol, a variation of the Simple Mail Transfer Protocol (SMTP), to transmit the message content to the local mail submission agent (MSA), such as smtp.a.org.
2. The **MSA** ascertains the destination address provided in the **SMTP** protocol, the fully qualified domain address (FQDA) bob@b.org, by resolving the domain name to identify the fully qualified domain name of the mail server in the Domain Name System (**DNS**).
3. The **DNS** server for the domain b.org (ns.b.org) provides MX records listing the mail exchange servers for that domain, such as mx.b.org, an intermediary message transfer agent (MTA) operated by the recipient's Internet service provider (ISP).
4. smtp.a.org dispatches the message to mx.b.org through **SMTP**, requiring the relay of the message to other **MTAs** before it ultimately reaches the final message delivery agent (**MDA**).
5. The **MDA** delivers the message to the mailbox of the recipient, Bob.
6. Bob's **MUA** retrieves the message either through the Post Office Protocol (**POP3**) or the Internet Message Access Protocol (**IMAP**).

This sequence can be affected by various factors and alternative setups, such as corporate email systems with their proprietary protocols, the use of webmail services, the presence of individual MTAs on sender computers, and the use of multiple mail exchange servers for enhanced reliability. Additionally, the decline of open mail relays, once commonly used for email delivery, has resulted from their vulnerability to abuse by senders of unsolicited bulk emails.

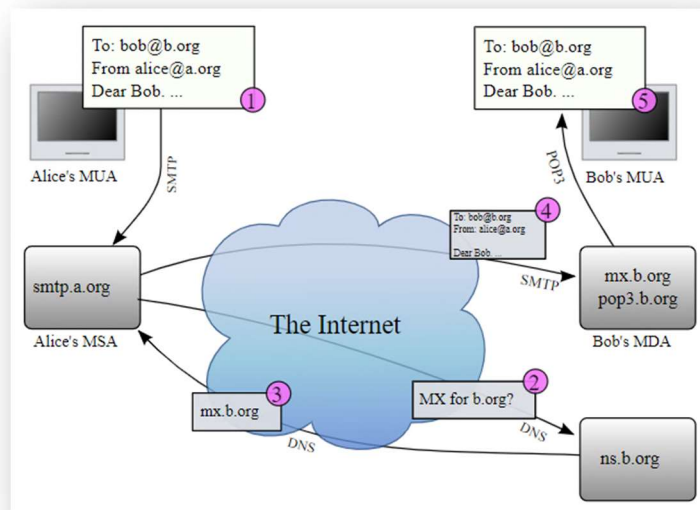


Figure 8 - Detailed email delivery process

¹⁴ How does email work? - Email service - Namecheap.com. (2023, April 4).
<https://www.namecheap.com/support/knowledgebase/article.aspx/10589/2179/how-does-email-work/>

Email Authentication Protocols

Email authentication protocols¹⁵ are defensive mechanisms used by the recipient's servers. They ensure that the message was not hijacked, altered, or forged before getting delivered to validate the authenticity and accuracy. Most modern servers use the following protocols:

SPF is a fundamental protocol employed for verifying the legitimacy of the sender's IP. It is stored in DNS records in a TXT format, and the recipient's server checks the DNS to confirm if the IP is authorized. If the IP is on the list of authorized IPs, the email is delivered; otherwise, the message is flagged or rejected.

DKIM, on the other hand, is a form of digital signature embedded in the email's source code to authenticate the sender's domain and ensure that the email content remains unaltered. DKIM generates a hashed private key using various tags and characters. Upon reaching the receiving server, it looks for the corresponding public key, and successful authentication occurs when the public and private keys match.

DMARC, a more sophisticated authentication approach, can utilize SPF, DKIM, or both. When configuring DMARC, domain owners can specify the chosen authentication protocols and the strictness of the validation process, such as whether to allow subdomains or exact domain matches. This protocol enables domain owners to enhance their sender reputation gradually by instructing the receiving server on actions to take upon authentication failure (e.g., quarantine, rejection, or no action). It also facilitates the sending of reports for each failed authentication, allowing for swift responses in case of domain spoofing.

BIMI, the latest addition to authentication protocols, builds upon DMARC by introducing an extra layer of security to validate brand logos. When BIMI is implemented, the DNS includes a TXT record containing information about the brand's logo. Recipients can then view the logo when they receive emails from the corresponding brand. Despite its ongoing testing phase by email providers, BIMI's adoption remains limited.

Email Parts and Headers

Email headers are indeed metadata that accompany every email and provide detailed information such as the sender's and receiver's addresses, the email's route through various servers, timestamps indicating when the message was sent and received, as well as other relevant details. Email headers are used by mailboxes and email service providers to authenticate email senders and properly distribute emails to inboxes. The information in the email header is created automatically. Even though there is a standard for what email metadata should contain, a mail server can add whatever it wants to it. Most of the software and web-based mailboxes have their own shortcut to view each mail metadata. For example, in Thunderbird to watch metadata it is needed to Open email, click View Select Headers and mark All or Select Message Source as the image below:

¹⁵ Bandy, M. T. (2011). Effectiveness and limitations of E-Mail security protocols. *International Journal of Distributed and Parallel Systems*, 2(3), 38–49. <https://doi.org/10.5121/ijdps.2011.2304>

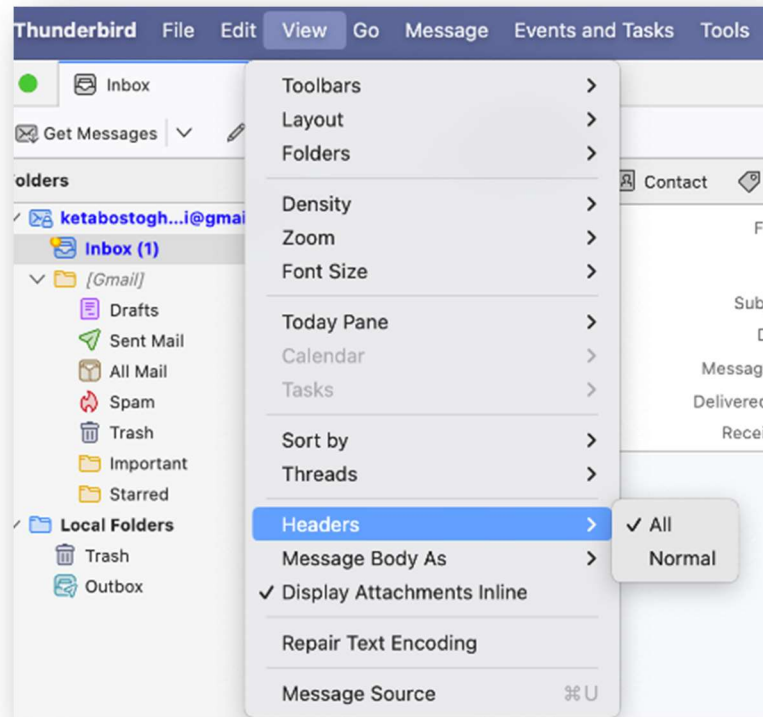


Figure 9 - Email headers example on Thunderbird

The format of email headers is structured into fields, with each field comprising a name, a separator character, and a corresponding value identifier. Key fields found in the email message header include "From," "To," "Subject," and "Date." Additionally, the header may encompass various technical details like "Return-Path," "Reply-To," "Message-ID," and others, although only "Date" and "From" are mandatory. Each email header is unique and may include additional specific information.

- **Message-ID** is a unique identifier, generated automatically to prevent multiple deliveries. It includes various (around 50) letters and numbers.
- **Multipurpose Internet Mail Extensions or MIME** is an internet standard regarding media attachments to an email. In MIME header, a user may be able to discover the type of origin of the attachment found on the sent or received email. It is recommended to use MIME-Version: 1.0 when sending out an email containing one of the following:
 - Non-text attachments
 - Message bodies with multiple parts.
 - Text in character sets other than ASCII
 - Header information in non-ASCII character sets

MITRE ATT&CK Framework

The MITRE ATT&CK® framework serves as a comprehensive repository of adversary tactics and techniques, drawing from real-world observations. It functions as a cornerstone for developing tailored threat models and methodologies across various sectors, including the private industry, government, and the cybersecurity product and service community. By creating ATT&CK, MITRE is advancing its mission to address challenges and promote a safer world, fostering collaboration among diverse stakeholders to enhance cybersecurity effectiveness.

ATT&CK's accessibility extends globally, providing individuals and organizations with an invaluable resource at no cost. Through correlating adversary groups with specific techniques, the framework enables security teams to gain deeper insights into the adversaries they confront. This understanding allows teams to assess their defenses more effectively, identifying areas for improvement and reinforcing security measures where they are most needed.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Exfiltration	Impact
Active Scanning (T1)	Aspen Access (T1)	Content Injection (T1)	Cloud Administration Command (T1)	Account Manipulation (T1)	Abuse of Elevation Control Mechanism (T1)	Account Discovery (T1)	Internal Discovery (T1)	Discovery of Remote Services (T1)	Application Layer Malware (T1)	Account Access Removal (T1)
Daphne Victim Host Information (T1)	Compromise (T1)	Directly Compromise (T1)	Command and Scripting Interactions (T1)	BITS Jobs (T1)	Access Taken Manipulation (T1)	Block Filter (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Daphne Victim Identity Information (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Daphne Victim Network Information (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Daphne Victim Org Information (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Feigning for Information (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Search Closed Sources (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Search Open Technical Channels (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Search Open Webpages (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)
Search Victim-Owned Websites (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Consumer Administration Command (T1)	Boot or Login Assistant Installation (T1)	Access Taken Manipulation (T1)	Browser Information Discovery (T1)	Browser Information Discovery (T1)	Internal Spearphishing (T1)	Automated Malware (T1)	Account Access Removal (T1)

Figure 11 - MITRE ATTACK framework coverage

These tactics represent specific technical goals that an adversary aims to accomplish. They are categorized based on the objectives they seek to achieve. For instance, there are currently 14 tactics cataloged in the enterprise matrix:

- **Reconnaissance:** Techniques that actively or passively gather information to plan future targeted attacks.
- **Resource development** involves attackers acquiring resources, either by purchasing or stealing them, to utilize in future attacks.
- **Initial access:** Techniques where adversaries try to gain a foothold in your network through different attack vectors.
- **Execution:** Adversary techniques that try to run malicious code on a local or remote system.
- **Persistence** tactics are employed by adversaries to uphold their presence within a local or remote network, ensuring continued access and control.
- **Privilege escalation:** When an adversary tries to gain higher-level permission into your organization's network.
- **Defense evasion:** Adversary techniques to avoid detection when they move through your network.
- **Credential access:** Tactics focused on retrieving sensitive credentials such as passwords.
- **Discovery:** attackers try to gain an understanding of how your systems work.
- **Lateral movement:** Involves adversaries that enter and control systems, moving through your network.
- **Collection:** Techniques that gather information from relevant sources within your organization.
- **Command and Control (C2 or C&C):** When adversaries communicate with compromised systems to gain control.
- **Exfiltration:** Consists of techniques that straight up steal data from your network.
- **Impact:** When adversaries focus on disrupting data availability or integrity and interrupting business operations.

Each tactic includes a few sub-techniques.

Each technique within the MITRE ATT&CK framework delineates a singular approach that adversaries may employ to achieve their objectives. Numerous techniques are cataloged under each "tactics" category because adversaries may opt for different methodologies based on various factors such as their skillsets, the configuration of their targets' systems, and the availability of suitable tools. Each technique entry includes a comprehensive description of the method, specifying the systems and platforms to which it applies. Additionally, if known, the entry identifies adversary groups that have utilized the technique. Mitigation strategies to counteract the activity are also provided, along with references to real-world instances where the technique has been observed. This multifaceted approach enables security practitioners to better understand, anticipate, and defend against potential threats.

In MITRE ATT&CK framework there are two techniques which are relevant to phishing attacks that are being used from many threat groups around the world. These techniques are being used on Reconnaissance and Initial Access tactics.

In **Reconnaissance** (with ID TA0043)¹⁷ the adversary is trying to gather information they can use to plan future operations. Reconnaissance encompasses techniques utilized by attackers to gather information crucial actively or passively for targeting. This information may comprise details regarding the victim organization, its infrastructure, or its staff and personnel. The adversary can leverage this information to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

Phishing for information technique is categorized under **reconnaissance** tactic with the ID T1598 and four other sub-techniques with IDs T1598.001, T1598.002, T1598.003, T1598.004¹⁸. Adversaries may send phishing communications to get sensitive information for use in targeting. Phishing for information is an attempt to make people disclose information, most commonly credentials or other actionable data. Phishing for information differs from phishing in that the goal is to collect data from the victim rather than to execute dangerous code. Phishing is a type of social engineering that is delivered electronically. Spear phishing is a type of targeted phishing. The adversary will target a specific individual, firm, or industry in spear phishing. Adversaries can also engage in non-targeted phishing, such as mass credential harvesting efforts. Adversaries may also attempt to collect information directly by exchanging emails, instant messaging, or other forms of electronic communication. Victims may also receive phishing messages instructing them to contact a phone number where the adversary will attempt to obtain sensitive information. Social engineering techniques, such as acting as a source with a need to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending several, urgent communications, are widely used in information phishing. Another method is to forge or spoof the sender's identity, which can be used to trick both the human recipient and automated security technologies. Phishing for information may also employ deceptive techniques such as removing or modifying emails or metadata/headers from hacked accounts.

Home > Techniques > Enterprise > Phishing for Information

Phishing for Information

Sub-techniques (4)	
ID	Name
T1598.001	Spearphishing Service
T1598.002	Spearphishing Attachment
T1598.003	Spearphishing Link
T1598.004	Spearphishing Voice

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from Phishing in that the objective is gathering data from the victim rather than executing malicious code.

ID: T1598
 Sub-techniques: T1598.001, T1598.002, T1598.003, T1598.004
 ① Tactic: Reconnaissance
 ① Platforms: PRE
 Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Robert Simmons, @MalwareUtkonos; Scott Cook, Capital One; Sebastian Salla, McAfee
 Version: 1.3
 Created: 02 October 2020
 Last Modified: 08 September 2023

Figure 12 - Phishing for Information tactic

¹⁷ Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0043/>

¹⁸ Phishing for information, technique T1598 - Enterprise | MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/techniques/T1598/>

Lab Architecture & Installation

For the needs of the current thesis regarding phishing and social engineering techniques it is important to have a sample environment in which the experiments will be conducted such as techniques and security controls that are going to be used. For that reason, a dedicated lab was created both on local home network and on Azure infrastructure. During the lab creation, there were technical problems such as ISP provider's limitations on the first 1000 ports and the Azure outbound 25 SMTP connections. Having those problems, I have built the server on the cloud and specifically on Microsoft's Azure.

The final constructed laboratory is hosted on the Microsoft Azure cloud platform, featuring an intricately designed architecture that encompasses a Mail Security Gateway (MSG) solution by Proxmox and a dedicated private Mail Server. Positioned within the Azure infrastructure, the lab serves as a virtualized environment, providing the necessary scalability and flexibility for an in-depth examination of social engineering and phishing in the context of email security. The Mail Security Gateway, strategically deployed at the network perimeter, functions as the initial defense layer against cyber threats. Leveraging Azure's robust security features, it employs advanced threat detection mechanisms to scrutinize incoming and outgoing emails, thwarting potential phishing attacks, and neutralizing malicious attachments. Simultaneously, the private Mail Server operates as the central communication hub, securely managing legitimate email traffic within the Azure environment. This Azure-based lab not only meets the specific needs outlined in the MSc thesis but also harnesses the advantages of cloud infrastructure, offering a secure and scalable platform for the comprehensive analysis of social engineering tactics and phishing strategies within the realm of email security.

Below screenshot shows the lab architecture that has been built on a high level. More specifically, a lab has been created on Azure behind an Application Gateway which includes two hosts. The first host is the Proxmox Mail Gateway security solution which acts as a proxy between the internet and the second host which is the private mail server. Finally, several hosts could be added on the architecture which will be used to evaluate Elastic SIEM against phishing attacks.

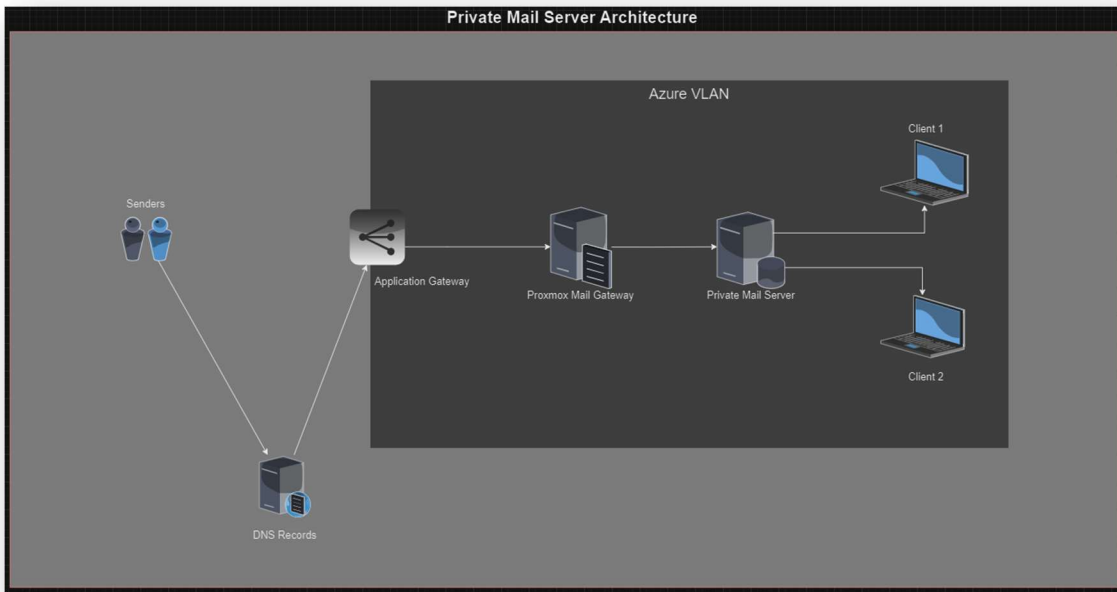


Figure 13 - Private mail server architecture

Lab Limitations

Embarking on the construction of a private mail server lab proved to be a nuanced endeavor, fraught with distinctive challenges that demanded resourcefulness and a deep understanding of networking dynamics. A notable constraint arose from the Internet Service Provider's (ISP) policy, which reserved the initial 1000 ports for their own use. This necessitated port allocation and strategic planning to ensure the seamless functioning of the private mail server within the confines of the available port range. Furthermore, the ISP's implementation of an SMTP (Simple Mail Transfer Protocol) block added a layer of complexity to the configuration process. Given the standard nature of SMTP for email communication, circumventing this block required either the implementation of unconventional configurations or the utilization of non-standard ports, introducing an additional layer of intricacy to the server setup. In parallel, another significant limitation emerged in the form of cloud service providers imposing restrictions on outbound SMTP traffic. This measure, while justified as an initiative-taking defense mechanism against phishing campaigns, posed a considerable hurdle in achieving the desired functionality of the private mail server. Negotiating these limitations mandated a thorough comprehension of the respective cloud provider's policies, necessitating a careful alignment of configurations to overcome the outbound SMTP block and ensure the unimpeded flow of emails from the private server. The intricate dance between ISP port reservations and cloud provider security protocols underscored the need for a nuanced approach, adaptability, and an in-depth grasp of networking intricacies when venturing into the construction of a private mail server within a dynamic and regulated network environment.

Lab Components

Constructing a private mail server lab involves integrating a range of essential components to ensure seamless functionality and security. The primary hardware components typically include a

dedicated server or a virtual machine with sufficient computing resources such as processing power, memory, and storage. This server serves as the foundation for hosting the mail server software and managing protocols.

On the software side, the core of the private mail server is often built using popular mail server applications like Postfix¹⁹ for SMTP, Dovecot²⁰ for IMAP and POP3. These applications collectively manage the sending, receiving, and storage of emails while also implementing security measures. To enhance security, SSL/TLS certificates are crucial for encrypting the communication between the mail server and clients. Additionally, components such as firewalls, intrusion detection/prevention systems, and secure authentication mechanisms play pivotal roles in safeguarding the mail server from external threats.

For effective management and monitoring, a web-based control panel like Webmin or a command-line interface may be integrated. This facilitates administrative tasks, user management, and monitoring server performance. Logging and auditing tools also play a crucial role in tracking server activities and identifying potential issues. In the context of addressing limitations imposed by ISPs and cloud providers, the lab may involve the use of network address translation (NAT) or port forwarding to navigate port reservations. Techniques such as setting up alternative SMTP configurations or exploring non-standard ports may be employed to overcome outbound SMTP blocks.

Overall, the constructive collaboration of hardware, software, and security components forms the backbone of a private mail server lab, creating an environment conducive to experimentation, learning, and the development of skills related to mail server administration and network management.

Cloudflare Domain

To explore the mail delivery process across the internet a domain has been bought from Cloudflare to achieve that goal. Cloudflare's DNS (Domain Name System) services are also noteworthy. The company offers a fast and secure DNS resolution service that not only translates domain names into IP addresses but also helps in blocking malicious websites and providing a layer of privacy for users. A registered a domain name called **hubcyber.work** would help on the experiments that will be illustrated. The following screenshot serves as an example of how the DNS entries are being overseen from Cloudflare's user-friendly GUI.

¹⁹ The Postfix home page. (<https://www.postfix.org/>)

²⁰ Dovecot | The Secure IMAP server. (<https://www.dovecot.org/>)

Type	Name	Content	Proxy status	TTL	Actions
A	hubcyber.work	74.234.35.177	DNS only	Auto	Edit
A	mail	74.234.35.177	DNS only	Auto	Edit
MX	hubcyber.work	mail.hubcyber.work	10 DNS only	Auto	Edit

Figure 14 - Cloudflare DNS records for domain

More details regarding the connectivity of the above A records and the lab's mail installed solutions are going to be described on the next chapters.

Azure Debian 11 Virtual Machine

The resource group "mailserver_lab" is currently in a running status in North Europe, under "Azure subscription 1" with an assigned subscription ID. The virtual machine, named "pmg-client," operates on the Linux Debian 12 operating system and is configured with a Standard B2s size, featuring 2 vCPUs and 4 GiB of memory. The public IP address assigned to this virtual machine is 74.234.35.177, and it is associated with the LAN/default virtual network/subnet. The machine is not configured with a DNS name and currently has no health state information available. The virtual machine, running Debian 12, has an agent status of "Ready," utilizing Debian 11 as the base image. Security configurations are set to standard, and the machine is not configured for health monitoring. Networking details include a private IP address of 10.10.10.5 and a public IP address of 74.234.35.177 associated with the "pmg-client" network interface. The machine has Proxmox Mail Gateway solution installed. Overall, this resource group constitutes a functional environment for a Debian 12-based virtual machine within Azure, suitable for various computing tasks.

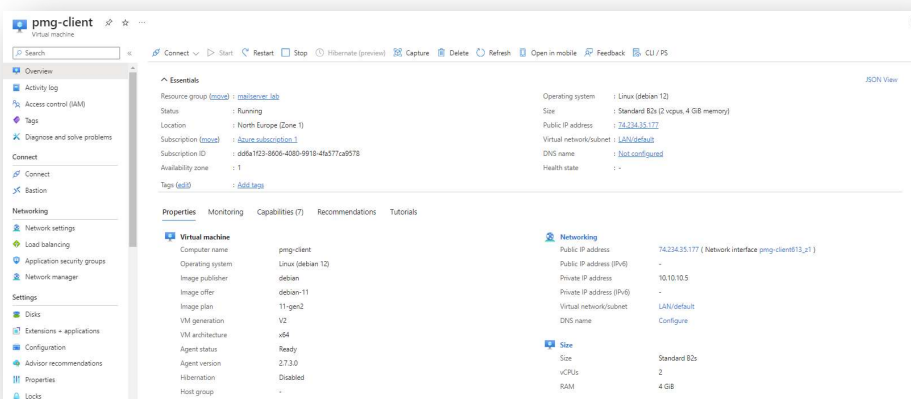


Figure 15 - PMG virtual machine on Azure

Azure Ubuntu Server 22.04 Virtual Machine

The resource group "mailserver_lab" is currently in a running status in the North Europe region under my subscription with an assigned subscription ID. The virtual machine within this resource group is operating on the Linux (Ubuntu 22.04) operating system, specifically utilizing a Standard B2s configuration with 2 vCPUs and 4 GiB of memory. The public IP address assigned to the virtual machine is 20.234.30.81, and it is associated with the LAN/default virtual network/subnet. The virtual machine is named "hubcyber.work" and is running with an agent status of "Ready," utilizing Ubuntu 22.04 as the base image. The machine has standard security configurations and is not currently configured for health monitoring. The networking details include a private IP address of 10.10.10.4 associated with the "ubuntu-mail-server" network interface. The virtual machine is not currently configured for Azure Spot instances, and no data disks or extensions/applications have been specified. Overall, the resource group constitutes a functional mail server lab environment within the Azure cloud infrastructure.

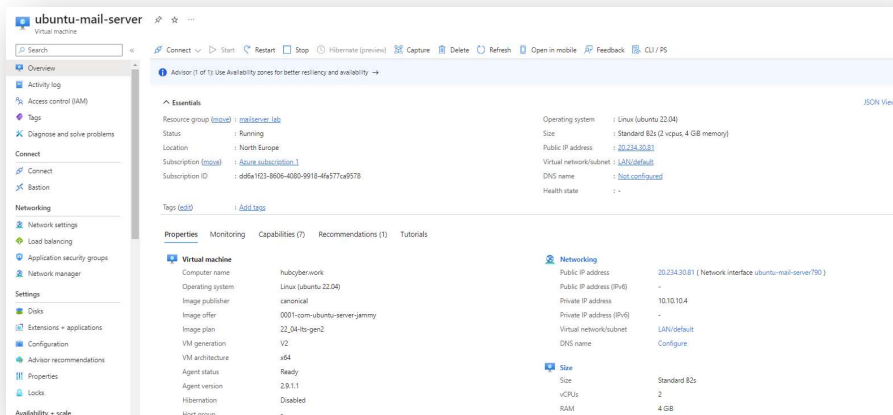


Figure 16 - Private mail server virtual machine on Azure

There is not yet any client machine implemented to view mails. In case it is necessary, a host with Windows or any Linux based operating system could be implemented.

Azure Windows 10 Virtual Machine

The resource group "mailserver_lab" is currently in a running status in the North Europe region under my subscription with an assigned subscription ID. The virtual machine within this resource group is operating on the Windows 10 operating system, specifically utilizing a Standard B2s configuration with 2 vCPUs and 4 GiB of memory. The public IP address assigned to the virtual machine is 74.234.40.223, and it is associated with the LAN/default virtual network/subnet. The virtual machine is running with an agent status of "Ready," utilizing Windows 10 as the base image. The machine has standard security configurations and is not currently configured for health monitoring. The networking details include a private IP address of 10.10.10.6 associated with the "windows-client" network interface. Overall, the resource group constitutes a functional mail server lab environment within the Azure cloud infrastructure.

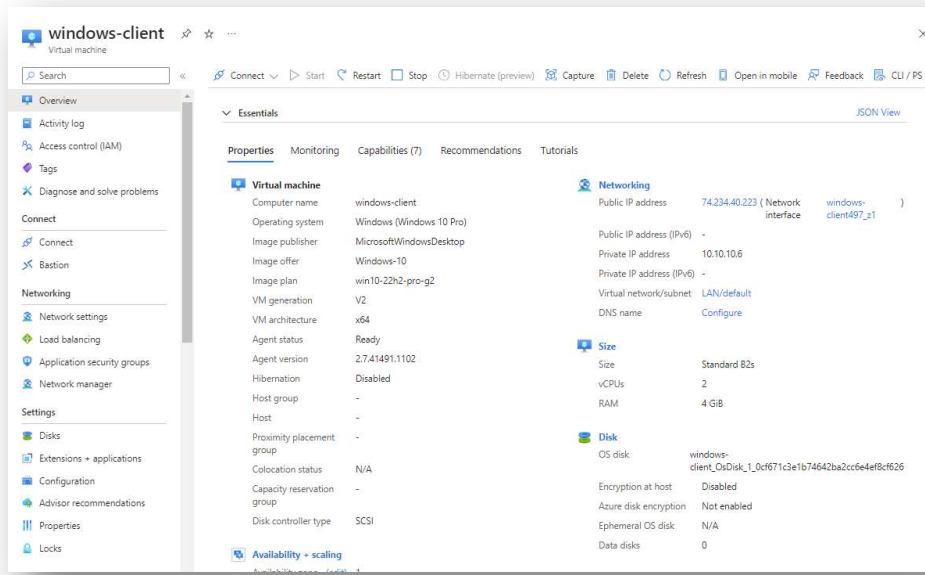


Figure 17 - Windows client virtual machine on Azure

Lab Installation

Starting out with the lab implementation it is important to set up each host with the software, tools and networking needed which is required for the components altogether.

Proxmox Mail Gateway Installation

First step is to prepare the host where the Proxmox Mail Gateway will be hosted. On Azure the steps that must be followed are:

1. On Virtual Machines window, go to Create. On the new menu enter details such as Virtual Machine name, Resource Group (if it is needed), Region - the lab has to be under the same region – especially if the hosts will be under the same VLAN, Zones, Operating System – in our case would be Debian 11 – since the Proxmox documentation suggests that Size requirements and finally the port that the administrator can login.
2. Proceed to Disks and select 64GB with Standard SSD.
3. On Networking add the host to the created VLAN. Also assign a public IP address. Proxmox Mail Gateway solution will proxy, filter and relay emails to the mail server.
4. Finally, enter any other details based on the lab architecture that you want to apply the PMG. In our case there is no immediate need for extra settings.
5. On Review + Create tab, check for the provided configurations. Confirm and continue to the host generation by selecting Create.

Resource group (move) : mailserver_lab	Operating system : Linux (debian 12)
Status : Running	Size : Standard B2s (2 vcpus, 4 GiB memory)
Location : North Europe (Zone 1)	Public IP address : 74.234.35.177
Subscription (move) : Azure subscription 1	Virtual network/subnet : LAN/default
Subscription ID : dd6a1f23-8606-4080-9918-4fa577ca9578	DNS name : Not configured
Availability zone : 1	Health state : -
Tags (edit) : Add tags	

Figure 18 - Mail Server lab details

Once the installation of the Virtual Machine running Debian 11 has been completed it is the time to try and install the required updates and finally the Proxmox Mail Gateway security solution²¹. Knowing the public IP address and the port 22 open, can connect on the host with ssh using the username and the password provided during the installation. Once connected to the machine it is required to do the package upgrades needed.

```
C:\Users\mike>ssh mike@108.143.195.192
The authenticity of host '108.143.195.192 (108.143.195.192)' can't be established.
ED25519 key fingerprint is SHA256:Jcxs7vn2HEX3HHKgBIN4f3jQ/vVvm7C8NQCuPRUB+U.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '108.143.195.192' (ED25519) to the list of known hosts.
mike@108.143.195.192's password:
Linux pmg-client 5.10.0-26-cloud-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

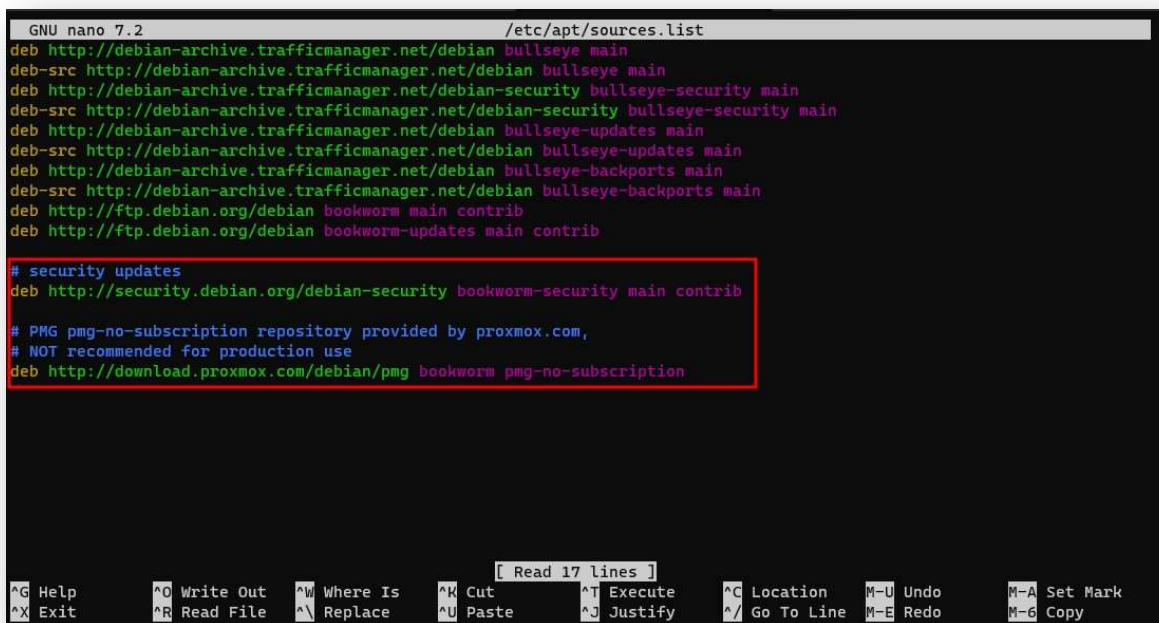
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
mike@pmg-client:~$ apt-get dist-upgrade
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?
mike@pmg-client:~$ sudo su
root@pmg-client:/home/mike# apt-get dist-upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  libnhttp2-14 tzdata
2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 364 kB of archives.
```

Figure 19 - Proxmox installation through sources

Once the Debian upgrade has been completed; the process can be continued. The packages that PMG need to be installed on the host do not exist on the default deb apt package manager. For that reason, it is necessary to add the provided URLs from the Proxmox official documentation on file “sources.list”

²¹ Proxmox Mail Gateway Documentation Index. (n.d.). <https://pmg.proxmox.com/pmg-docs/>

that exist under the path “/etc/apt.” To write on the sources.list²² file root privileges are required. In a sources.list file, each line specifies a package repository. It is essential to prioritize the preferred source by placing it first. Empty lines in the file are disregarded. Any line with a # character denotes the remainder of that line as a comment. To obtain available packages from a repository, one can execute the apt update command. Subsequently, updates can be installed directly through apt or via the graphical user interface (GUI) by navigating to Administration → Updates. The following paths must be added to the file as the screenshot illustrates below.



```
GNU nano 7.2 /etc/apt/sources.list
deb http://debian-archive.trafficmanager.net/debian bullseye main
deb-src http://debian-archive.trafficmanager.net/debian bullseye main
deb http://debian-archive.trafficmanager.net/debian-security bullseye-security main
deb-src http://debian-archive.trafficmanager.net/debian-security bullseye-security main
deb http://debian-archive.trafficmanager.net/debian bullseye-updates main
deb-src http://debian-archive.trafficmanager.net/debian bullseye-updates main
deb http://debian-archive.trafficmanager.net/debian bullseye-backports main
deb-src http://debian-archive.trafficmanager.net/debian bullseye-backports main
deb http://ftp.debian.org/debian bookworm main contrib
deb http://ftp.debian.org/debian bookworm-updates main contrib

# security updates
deb http://security.debian.org/debian-security bookworm-security main contrib

# PMG pmg-no-subscription repository provided by proxmox.com,
# NOT recommended for production use
deb http://download.proxmox.com/debian/pmg bookworm pmg-no-subscription
```

Figure 20 - Adding sources to Debian list

Once the Proxmox Mail Gateway paths have been added on the apt-based file repository, then it is required to install the keys provided by the vendor for the origin of the file that will be installed to be verified. APT uses GnuPG signatures to verify that the packages it downloads and installs are from a trusted source. If the Release file is signed with a valid GnuPG key, APT can be confident that the packages listed in the file have not been tampered with and are indeed from the expected source. To enable APT to verify the signatures, the public key used for signing is needed. Signature can manually install the key using the provided wget command. This command downloads the GnuPG key from a specified URL and saves it to the directory.

²² Darksody. (2023, July 28). Install proxmox mail gateway on debian on an Azure VM [Online forum post]. Proxmox Support Forum. <https://forum.proxmox.com/threads/install-proxmox-mail-gateway-on-debian-on-an-azure-vm.92786/>

```
root@pmg-client:/home/mike# wget https://enterprise.proxmox.com/debian/proxmox-release-bookworm.gpg -O /etc/apt/trusted.gpg.d/proxmox-release-bookworm.gpg
--2023-12-15 21:01:59-- https://enterprise.proxmox.com/debian/proxmox-release-bookworm.gpg
Resolving enterprise.proxmox.com (enterprise.proxmox.com)... 212.224.123.70, 2a01:7e0:0:424::249
Connecting to enterprise.proxmox.com (enterprise.proxmox.com)|212.224.123.70|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1187 (1.2K) [application/octet-stream]
Saving to: '/etc/apt/trusted.gpg.d/proxmox-release-bookworm.gpg'

/etc/apt/trusted.gpg.d/proxmox 100%[=====] 1.16K --.-KB/s in 0s

2023-12-15 21:01:59 (33.7 MB/s) - '/etc/apt/trusted.gpg.d/proxmox-release-bookworm.gpg' saved [1187/1187]

root@pmg-client:/home/mike# apt update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-security InRelease
```

Figure 21 - Updating Debian to install sources

After the signature has been installed an apt update is required for the host to resolve the application packages provided in the previous steps. The ifupdown Network connectivity module is uninstalled, and it is required for the Proxmox Mail Gateway to finish the installation, otherwise the Azure Virtual Machine will lock out the users from the remote connection. For that reason, is mandatory to upgrade the machine and reboot the system. After the reboot process has been completed it is time to install PMG on the host. Proxmox Mail Gateway can also operate within a Debian-based Linux Container (LXC) instance. To ensure a minimal set of installed software and reduce the need for updates, the proxmox-mailgateway-container meta-package can be employed. This does not depend on any Linux kernel, firmware, or components used for booting from bare metal, like grub2, thus it is the perfect fit for the lab architecture on Azure. With the command apt install proxmox-mailgateway-container. The command for the installation is *apt install proxmox-mailgateway-container*. During the installation, a Postfix module will be installed, and the user will be prompted to enter the configuration. In this lab architecture it is not required since the mail relay configuration will be done later. Once the installation, is finished the web interface of the PMG will run on the port 8006. A user can enter this web panel by executing a local port forwarding command on the port and the public IP address of the host. More specifically, illustrates a ssh connection on the public IP of the host and a local port forwarding of what is running on port 8006 of the host to user's 8080 port. The following image serves as a proof of concept.

```
PS C:\Users\mike> ssh mike@108.143.195.192 -L 8080:10.0.0.4:8006
mike@108.143.195.192's password:
Linux pmg-client 6.1.0-16-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.67-1 (2023-12-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 15 21:08:19 2023 from 188.4.177.79
```

Figure 22 - Port forwarding to access PMG interface

Now the user can perform a GET request on any preferred browser to successfully access the web graphic interface.

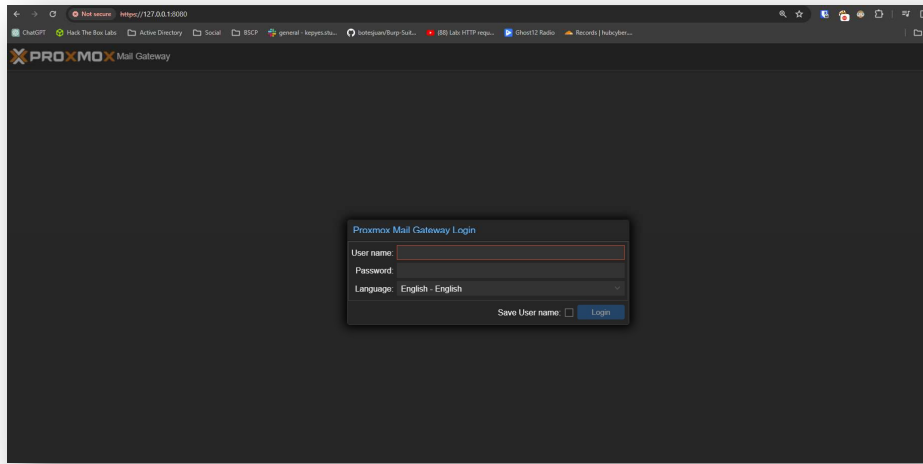


Figure 23 - Proxmox Mail Gateway Login interface

The first form that the user needs to fill in is the Login form. Now the user needs to put its root credentials to login. If no root password has been provided, then it is required to initiate one on the host. After filling in the credentials a successful session will begin, and the Proxmox Mail Gateway interface will be shown.

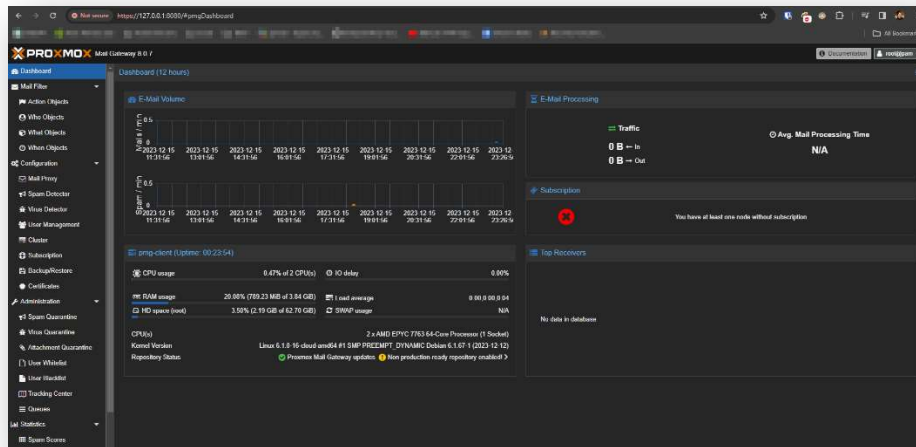


Figure 24 - Proxmox Mail Gateway graphic user interface

Once the installation of the Proxmox Mail Gateway has been finished some extra configurations are missing. To fulfill these, it is first necessary to deploy the private mail server. To continue with the private mail server installation, it is important to deploy, firstly, an Azure virtual machine.

Private Mail Server Installation

On Azure the steps that must be followed are:

1. On Virtual Machines window, go to Create. On the new menu enter details such as Virtual Machine name, Resource Group (if it is needed), Region - the lab must be under the same region – especially if the hosts will be under the same VLAN, Zones, Operating System – in our case would Ubuntu Server 22.04.
2. Proceed to Disks and select 64GB with Standard SSD.
3. On Networking add the host to the created VLAN. Also assign a public IP address which will be used temporarily for the configuration.
4. Finally, enter any other details based on the lab architecture that you want to apply. In our case there is no immediate need for extra settings.
5. On Review + Create tab, check for the provided configurations. Confirm and continue to the host generation by selecting Create.

After the successful deployment of the Azure Virtual Machine hosting Ubuntu, the process of creating the private mail server can be continued. First things first, a remote connection is needed using ssh on the virtual machine. Afterwards, run the basic `sudo apt update && upgrade` command to install the latest packages available for Ubuntu Server. Then to start with the installation I am going to install Postfix with the command `sudo apt install postfix`.

Postfix is a popular and widely used mail transfer agent (MTA) – a software component responsible for sending, receiving, and routing emails between different mail servers. It was developed by Wietse Venema and is designed to be secure, efficient, and easy to configure.

Key features and aspects of Postfix include²³:

1. **SMTP Server:** Postfix primarily operates as an SMTP (Simple Mail Transfer Protocol) server, handling the transmission of emails between servers on the Internet. SMTP is the protocol used for sending emails.
2. **Security:** Postfix places a strong emphasis on security. It implements various security measures to protect against common vulnerabilities and attacks, making it a reliable choice for secure email communication.
3. **Modularity:** Postfix is designed with a modular architecture, allowing administrators to extend its functionality using plugins and custom configurations. This modularity contributes to flexibility and customization.
4. **Configurability:** The configuration of Postfix is done through a set of human-readable text files, making it straightforward for system administrators to understand and modify settings. This approach contrasts with other mail servers that might use more complex configuration systems.
5. **Reliability:** Postfix aims to be dependable and robust. It includes features such as content filtering, access controls, and a queue management system to handle email delivery efficiently even in the face of network or system issues.
6. **Compatibility:** Postfix is compatible with various Unix-like operating systems, including Linux and BSD variants. It is commonly used on servers to handle email services for both small-scale setups and large-scale, enterprise-level deployments.

²³ Dent, K. D. (2004). Postfix: The Definitive Guide. "O'Reilly Media, Inc."

Postfix is often chosen as the default mail server for Linux distributions due to its reputation for security, ease of configuration, and efficient performance. Many administrators use Postfix in conjunction with other email-related software components, such as Dovecot (for handling incoming mail and user mailboxes). During the Postfix installation the user is prompted to apply some configurations. The first panel asks for the system mail name.

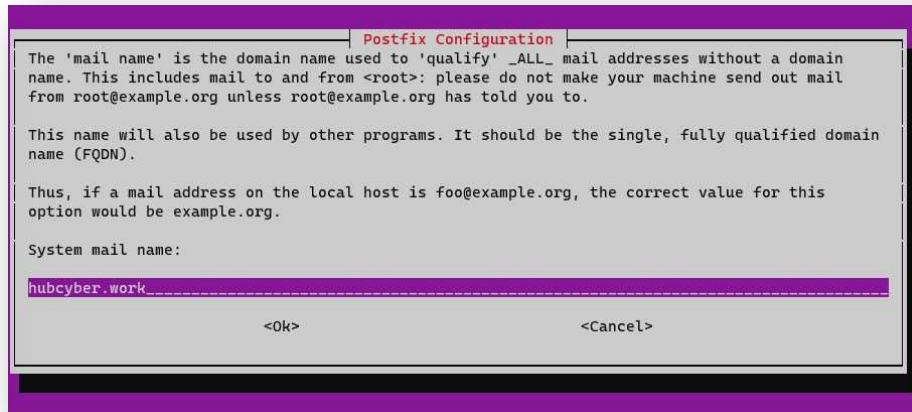


Figure 25 - Adding system mail name

In the realm of email communication, Postfix destinations represent the designated addresses and domains where the Postfix mail server is authorized to accept incoming messages. This configuration defines the specific locations to which the server is responsible for delivering emails, ensuring efficient and secure mail handling. Postfix destinations are set in the server's configuration files, typically specified in the main.cf file. Administrators define the accepted domains, email addresses, and recipient lists, allowing Postfix to recognize and process incoming emails destined for these specific locations. This designation is pivotal for controlling the flow of messages and ensuring that the server accurately routes emails to the intended recipients.

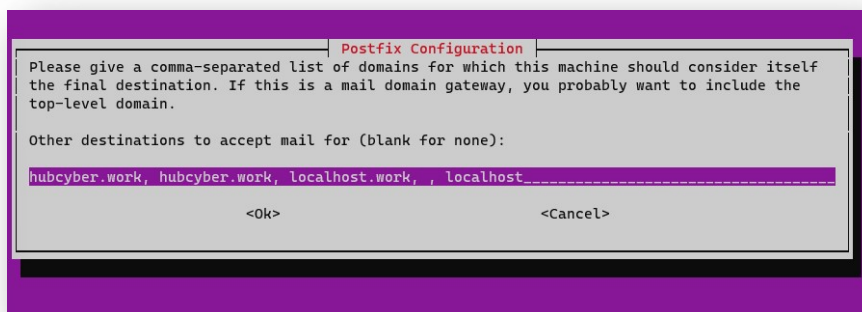


Figure 26 - Accept mail destinations

While Postfix is asynchronous, certain configurations, especially in the context of content filtering or policy decisions, might introduce more synchronous behavior. For example, if you use content filters or filters that perform real-time checks on incoming messages, these checks might introduce some level of synchronous processing.

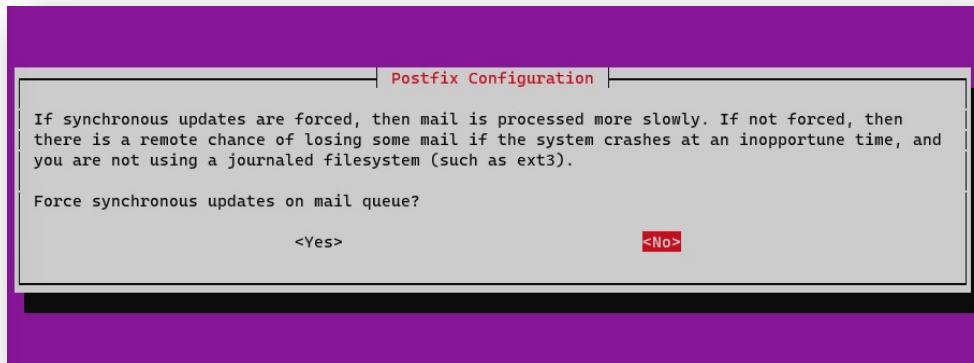


Figure 27 - Updates on synchronous queue

In the context of Postfix, the relay of mail involves the process of forwarding emails from one mail server to another. This is often used when an email server acts as a relay host to forward emails on behalf of other servers or clients. Main Configuration File (main.cf) is the main configuration file of Postfix (usually located at /etc/postfix/main.cf), where the need to configure Postfix to act as a relay host. Key parameters include relayhost which specifies the next-hop destination for non-local email and mynetworks which defines the network addresses that are allowed to relay through the server.

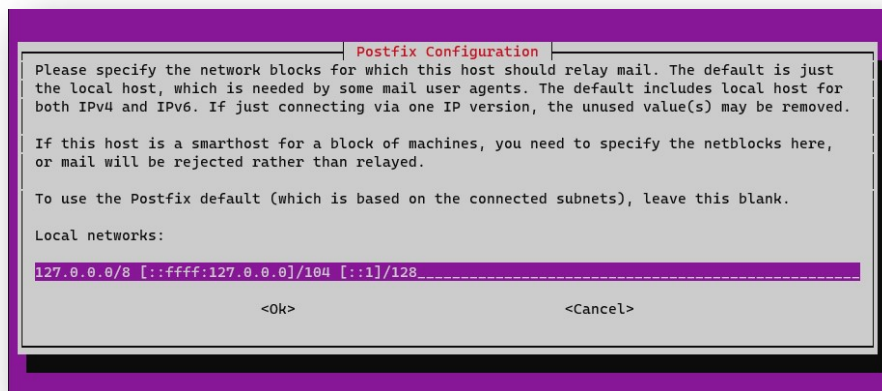


Figure 28 - Setting up local networks

To install Dovecot which will conduct a role on the mail server. Dovecot is a popular open-source email server software that provides both IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol version 3) services, offering efficient and secure access to users' email messages.

Dovecot's IMAP service allows users to access their email messages stored on a mail server. Unlike POP3, IMAP retains emails on the server, enabling users to organize, manage, and synchronize their messages across multiple devices. IMAP is particularly advantageous for users who want to access their emails from different locations and devices while maintaining a consistent view of their mailbox. Dovecot's IMAP implementation ensures a seamless and interactive experience, providing features such as folder management, message flags, and server-side search capabilities. Dovecot's POP3 service is designed for users who prefer to download their email messages to a local device, typically a computer or email client. When using POP3, emails are retrieved from the server and stored locally, and the server copy may be deleted based on user preferences. While POP3 is considered less flexible than IMAP in terms of managing emails across multiple devices, it can be suitable for users with specific requirements, such as a desire to store emails locally and reduce server storage usage. Dovecot's POP3 implementation ensures a reliable and straightforward email retrieval process, allowing users to access their messages with standard email clients.

In summary, Dovecot's IMAP and POP3 services cater to different user preferences and needs regarding email access and management. IMAP offers a more versatile and synchronized approach, while POP3 provides a straightforward method for downloading and storing emails locally. Dovecot's robust implementation of both protocols contributes to its widespread use as an email server solution in various environments.

```
root@hubcyber:/var/mail# sudo apt-get install dovecot-imapd dovecot-pop3d
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dovecot-core libexttextcat-2.0-0 libexttextcat-data liblua5.3-0
Suggested packages:
  dovecot-gssapi dovecot-ldap dovecot-lmtpd dovecot-lucene dovecot-managesieved dovecot-mysql
  dovecot-pgsql dovecot-sieve dovecot-solr dovecot-sqlite dovecot-submissiond ntp
The following NEW packages will be installed:
  dovecot-core dovecot-imapd dovecot-pop3d libexttextcat-2.0-0 libexttextcat-data liblua5.3-0
0 upgraded, 6 newly installed, 0 to remove and 3 not upgraded.
```

Figure 29 - Installing dovecot software

Finally, it needed to open the Dovecot configuration file and edit the line of protocols to accept pop3, pop3s, imap and imaps (where 's' related to secure version protocol) as values on parameters.

```

## Dovecot configuration file

# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration

# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.

# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace "

# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Enable installed protocols
!include_try /usr/share/dovecot/protocols.d/*.protocol

# Protocols to be supported by Dovecot
protocols = pop3 pop3s imap imaps

```

Figure 30 - Setting protocols on Dovecot configuration file

Now it is time to add users on the host to check whether each user receives emails from the internet. ***It is important to note that outbound SMTP is not provided on Azure.***

The next step of the lab installation is to configure some network settings regarding the hosts that have been created. The configurations that are needed to be implemented are based on the ports. The following table shows the rules.

Proxmox Mail Gateway Network Configurations

	Protocol	Name	Port	Source	Destination
Inbound	TCP	SSH	22	Any	Any
	TCP	SMTP	25	Any	Any
Outbound	TCP	SMTP	25	Any	Any
	TCP	AuthSMTP	587	Any	Any

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnySMTPInbound	25	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (4)						
320	AllowAnySMTPOutbound	25	TCP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Ubuntu Mail Server Network Configurations

	Protocol	Name	Port	Source	Destination
Inbound	TCP	SSH	22	Any	Any
	TCP	SMTP	25	Any	Any
	TCP	POP3	110	Any	Any
	TCP	IMAP	143	Any	Any
Outbound	TCP	SMTP	25	Any	Any
	TCP	POP3	110	Any	Any

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (10)						
300	SSH	22	TCP	Any	Any	Allow
320	RDP	3389	TCP	Any	Any	Allow
330	AllowAnyCustom25Inbound	25	TCP	Any	Any	Allow
340	AllowAnySSHInbound	22	TCP	Any	Any	Allow
360	AllowAnyPOP3Inbound	110	TCP	Any	Any	Allow
370	AllowAnyPOP3Inbound	995	TCP	Any	Any	Allow
390	AllowAnyIMAPInbound	143	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (5)						
350	AllowAnySMTPOutbound	25	TCP	Any	Any	Allow
380	AllowAnyPOP3Outbound	110	TCP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

At this point, it must be noted that the network configuration can be done also using built-in software such as `ufw` and `iptables` on Unix based operating systems and Firewall settings on Windows operating systems.

After utilizing both hosts that are needed for the experiments and the testing exercises that are going to be explained in detail on the next chapters it is time to configure the email proxy and relay of the Proxmox Mail Gateway Server. On the following screenshot, Mail Proxy is displayed. Under this tab there are the main configurations that are needed for the connectivity between the Mail Gateway and the private Mail Server.

The provided configuration settings are related to mail delivery in the context of the Proxmox Mail Gateway (PMG). PMG is a mail proxy and filter system designed to enhance the security and manageability of email traffic in a network. Below is an explanation of the configuration keys mentioned in the provided information:

- **Relay:** This setting specifies the default mail delivery transport for incoming mails. It corresponds to the equivalent Postfix configuration parameter in `main.cf`. The `<string>` value should represent the mail delivery transport, such as `smtp` or `lmtp`.
- **Relaynomx:** This setting, when set to `1`, disables MX lookups for the default relay. MX lookups are typically used to find the mail exchange servers for a domain. Disabling MX lookups can be useful in scenarios where you want to bypass DNS MX records and directly deliver emails to a specified relay server.
- **Relayport: (default = 25):** This setting specifies the port number for the SMTP/LMTP protocol when delivering mails to the relay host. The `<integer>` value should be within the valid port range (1 - 65535).
- **Relayprotocol: (default = smtp):** This setting determines the transport protocol used for delivering mails to the relay host. It can be either `lmtp` or `smtp`. LMTP (Local Mail Transfer Protocol) and SMTP (Simple Mail Transfer Protocol) are both common protocols used for email delivery.
- **Smarthost:** When set, this configuration specifies a smarthost to which all outgoing mails are delivered. The `<string>` value should represent the hostname or IP address of the smarthost. This corresponds to the Postfix option `default_transport`.
- **Smarthostport: (default = 25):** This setting specifies the SMTP port number for the smarthost. It corresponds to the Postfix option `default_transport`. The `<integer>` value should be within the valid port range (1 - 65535).

These configuration keys provide a way to customize how mail is delivered, whether it is for incoming mails using the default relay, or for outgoing mails through a specified smarthost. The values can be adjusted based on specific network and delivery requirements. In the structured lab architecture can provide the following settings. Most important settings will be under the Transport tab which will be explained in the next steps.

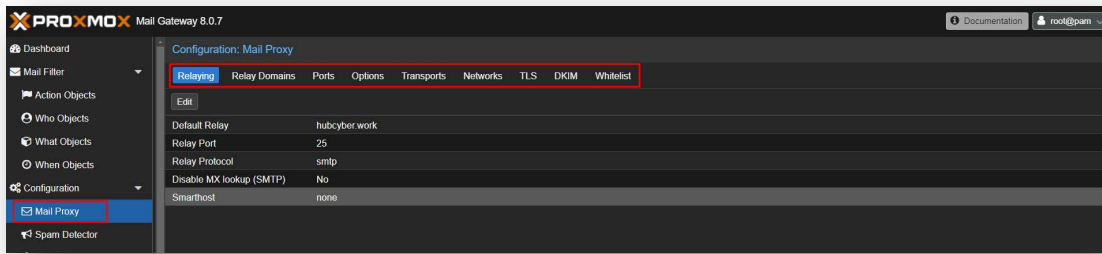


Figure 31 - PMG mail proxy configuration

Relayed mail domains, that is, what destination domains this system will relay mail to. The system will reject incoming mails to other domains.

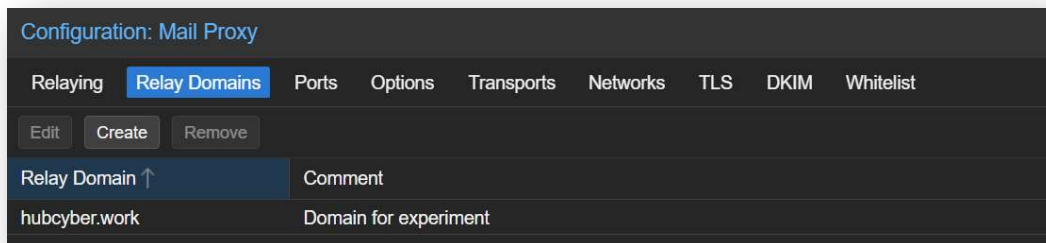


Figure 32 - Relay domains on PMG

This specification will do not proxy any other incoming mails for different email domains. Ports tab is the configurations in which external and internal SMTP ports can be configured. External port must be set on 25 since that is the way in which SMTP protocol will work for the incoming mails. Internal port works for outgoing mails from the mail proxy to the private mail server. On the Options tab there are many configurations that can be set.

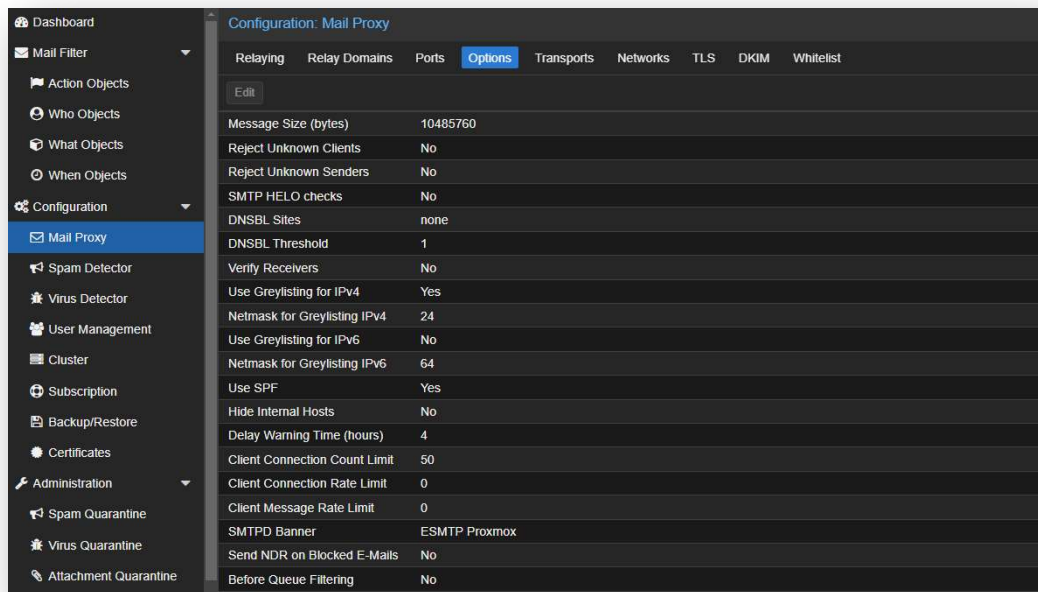


Figure 33 - Mail Proxy options

- **banner:** <string> (default = ESMTP Proxmox): ESMTP banner.
- **before_queue_filtering:** (default = 0): Enable before queue filtering by pmg-smtp-filter
- **conn_count_limit:** (default = 50): How many simultaneous connections any client is allowed to make to this service. To disable this feature, specify a limit of 0.
- **conn_rate_limit:** (default = 0): The maximal number of connection attempts any client is allowed to make to this service per minute. To disable this feature, specify a limit of 0.
- **dnsbl_sites:** Optional list of DNS white/blacklist domains (postfix option postscreen_dnsbl_sites).
- **dnsbl_threshold:** (default = 1) The inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score (postfix option postscreen_dnsbl_threshold).
- **dwarning:** (default = 4): SMTP delay warning time (in hours). (postfix option delay_warning_time)
- **greylist:** (default = 1): Use Greylisting for IPv4.
- **greylist6:** (default = 0): Use Greylisting for IPv6.
- **helotests:** (default = 0): Use SMTP HELO tests. (postfix option smtpd_helo_restrictions)
- **hide_received** (default = 0): Hide received header in outgoing mails.
- **maxsize** (default = 10485760) Maximum email size. Larger mails are rejected. (postfix option message_size_limit)
- **rejectunknown:** (default = 0) Reject unknown clients. (postfix option reject_unknown_client_hostname)
- **rejectunknownsender:** (default = 0) Reject unknown senders. (postfix option reject_unknown_sender_domain)
- **smtputf8:** <boolean> (default = 1) Enable SMTPUTF8 support in Postfix and detection for locally generated mail (postfix option smtputf8_enable)
- **spf:** <boolean> (default = 1) Use Sender Policy Framework.

- **verifyreceivers: <450 | 550>**: Enable receiver verification. The value specifies the numerical reply code when the Postfix SMTP server rejects a recipient address. (postfix options, reject_unknown_recipient_domain, reject_unverified_recipient, and unverified_recipient_reject_code)

The most important configuration that needs to be set on the lab is the addition of transporting an email under the tab Transports. After mail gateway manages to proxy an incoming email, it needs to provision it to the private mail server, if the email successfully manages to pass the email security controls. On the image below, a relay domain rule has been created for that specific reason. Every time a proxied email passes the security controls it can be provisioned to the mail server’s relay domain “hubcyber.work” which is being hosted on the LAN with private IP 10.10.10.4 using SMTP protocol. The SMTP protocol will work under the port 587 which is used for authenticated relay since Azure blocks all outgoing SMTP communications as a measure to prevent spamming.

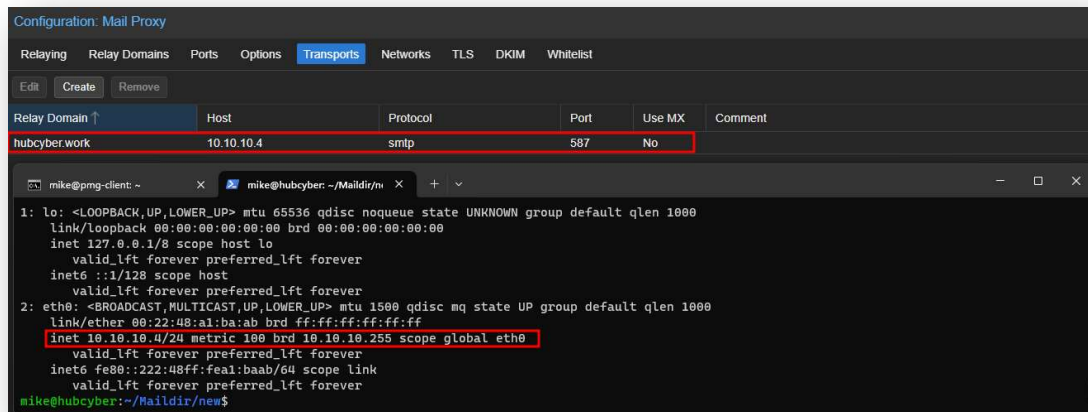


Figure 34 - Mail transport configuration

On the networks tab it is important to add the LAN where the Mail Gateway and the rest hosts are available. Documentation shares the information about not to provide the internal network IP since it would get recognized by default. For the precision, can proceed by providing the LAN created for the Azure lab. Proxmox Mail Gateway (PMG) provides administrators with dedicated tabs for configuring DKIM, TLS, and Whitelist settings. The DKIM tab facilitates the management of DomainKeys Identified Mail, allowing for the generation and association of cryptographic keys with domains, as well as enabling DKIM signing for outgoing emails. In the TLS tab, administrators can configure Transport Layer Security settings for secure email communication, specifying certificates, private keys, and security protocols for both incoming and outgoing connections. Additionally, the Whitelist tab serves as a mechanism for managing trusted senders or domains, enabling administrators to add specific email addresses or entire domains to the whitelist. Emails from whitelisted entities undergo fewer security checks, ensuring their delivery without additional scrutiny.

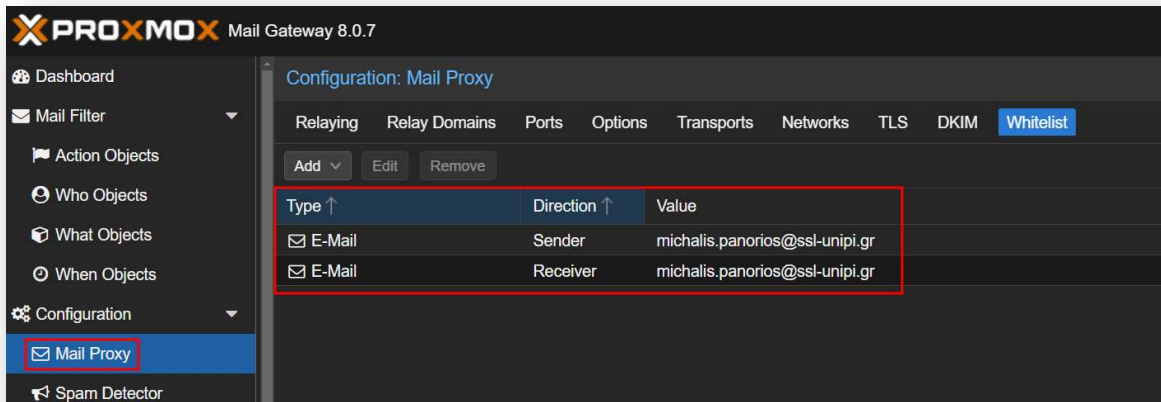


Figure 35 - Email whitelist options

After the above configuration of mail gateway and the private mail server it is also important to configure a client which will receive the emails on his mailbox. For that reason, a client running daily tasks on a Windows machine with Thunderbird mailbox installed is required. To fulfill these requirements, it is first necessary to deploy a virtual machine running Windows 10. To continue with the installation, it is important to deploy an Azure virtual machine.

Client Thunderbird Installation

On Azure the steps that must be followed are:

1. On Virtual Machines window, go to Create. On the new menu enter details such as Virtual Machine name, Resource Group (if it is needed), Region - the lab must be under the same region – especially if the hosts will be under the same VLAN, Zones, Operating System – in our case would be Windows 10.
2. Proceed to Disks and select 127GB with Standard SSD.
3. On Networking add the host to the created VLAN. Also assign a public IP address which will be used temporarily for the configuration.
4. Finally, enter any other details based on the lab architecture that you want to apply. In our case there is no immediate need for extra settings.
5. On Review + Create tab, check for the provided configurations. Confirm and continue to the host generation by selecting Create.

After the successful deployment of the Azure Virtual Machine hosting Windows, the process of creating the client's mailbox will be continued. First things first, a remote connection is needed using RDP on the virtual machine. An RDP session must be initiated to prepare the first configurations of the Windows host. Afterwards, a mailbox could be installed. There are many choices that can be made here such as Outlook or Thunderbird²⁴. In this lab Thunderbird will be used for the testing purposes. Once the installation of Thunderbird has been made, it is time to configure it. On Account Settings, the incoming

²⁴ Installing Thunderbird on Windows | Thunderbird Help. <https://support.mozilla.org/en-US/kb/installing-thunderbird-windows>

server of emails can be configured manually by selecting the mail server's IP and the protocol that would be initiated for the fetch of the emails.

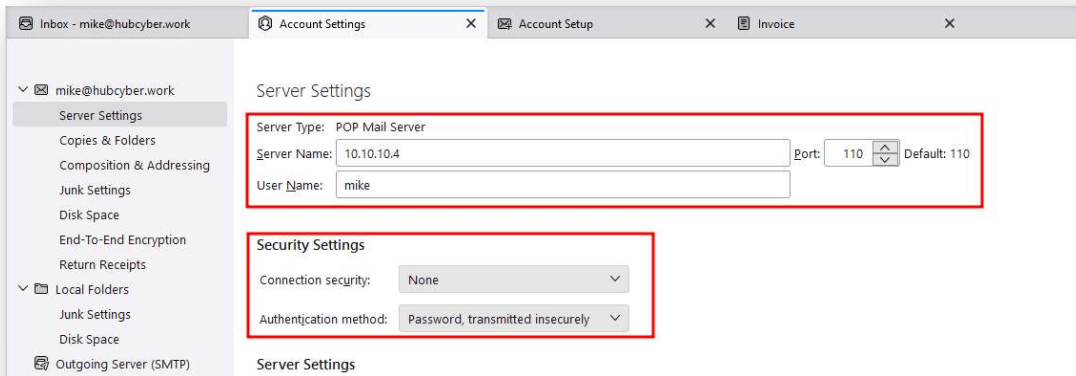


Figure 36 - POP3 Thunderbird options

More specifically, via Dovecot software private mail server has been configured to work with both IMAP, IMAPS, POP3 and POP3s. In this case POP3 default mail server will do the work. As defined in the introductory chapters POP3 runs on port 110. The IP of the private mail server and POP3's port will make the Thunderbird to fetch the emails. For username, the account created for the private mail server can be provided with the security setting just being a password. There are plenty of safer options such as SSL/TLS that can be used.

Elastic Installation

Elastic SIEM (Security Information and Event Management) is a part of the Elastic Stack, a set of open-source tools for searching, analyzing, and visualizing data. Elastic SIEM is designed to help organizations with security monitoring, threat detection, and response²⁵.

Here are some key features and components of Elastic SIEM:

- **Data Ingestion:** Elastic SIEM can ingest and analyze data from various sources, including logs, network traffic, and endpoint data. It supports a wide range of data formats and protocols.
- **Data Analysis:** Elastic SIEM uses the power of the Elasticsearch search and analytics engine to enable fast and efficient analysis of security data. It allows users to search and correlate data, identify patterns, and detect anomalies.
- **Detection Rules:** Elastic SIEM includes a rule-based detection engine that allows users to define custom rules for identifying potential security threats. These rules can be based on specific events, patterns, or behaviors.
- **Visualizations and Dashboards:** The solution provides pre-built visualizations and dashboards for monitoring and analyzing security data. Users can customize these dashboards to meet their specific needs.
- **Threat Intelligence Integration:** Elastic SIEM supports the integration of threat intelligence feeds, allowing organizations to enrich their security data with external threat intelligence information. Incident
- **Response:** The platform facilitates incident response by providing tools for investigating and responding to security incidents. This includes the ability to track and manage incidents within the platform.
- **Scalability:** Elastic SIEM is designed to scale horizontally, allowing organizations to handle large volumes of security data efficiently.
- **Open Source:** Elastic SIEM is built on open-source components, making it accessible to a broad community of users. The Elastic Stack components, including Elasticsearch, Logstash, and Kibana, are open-source projects.

By leveraging Elastic SIEM, organizations can enhance their ability to detect and respond to security threats in a timely and efficient manner. Security operations teams and SOC (Security Operations Center) analysts often use it to improve the overall security posture of an organization²⁶.

Elastic SIEM including Kibana, Fleet, Endpoint Security and Windows Log Collection is going to be installed primarily on the Ubuntu 22.04 virtual machine of the lab. Elasticsearch components are not available in the normal Ubuntu package repositories. However, they can be installed using APT after adding Elastic's package source list. To safeguard the system against package spoofing, all the packages are signed with the Elasticsearch signing key. The package management will consider packages that have been authenticated with the key to be trusted. To install Elasticsearch, this will import the Elasticsearch

²⁵ Athick, A. (2022). Getting Started with Elastic Stack 8.0: Design Powerful and Scalable Data Platforms to Search, Observe, and Secure Your Enterprise. Packt Publishing.

²⁶ Gormley, C., & Tong, Z. (2015). Elasticsearch: The Definitive Guide. O'Reilly & Associates Incorporated.

public GPG key and add the Elastic package source list in this step²⁷. Then the agent which will connect the SIEM with the clients would be installed on each client. First things first, it is needed to install the verification key. Next, add the Elastic source list to the sources.list.d directory, where apt will search for new sources. The [signed-by=/usr/share/keyrings/elastic.gpg] portion of the file instructs apt to use the key that you downloaded to verify repository and file information for Elasticsearch packages. Next update the packages and install elasticsearch package. The following image illustrates the commands that have been used selectively.

```
mike@hubcyber:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
mike@hubcyber:~$ echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
mike@hubcyber:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10.4 kB]
Get:6 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [77.8 kB]
Fetched 317 kB in 1s (400 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
mike@hubcyber:~$ sudo apt install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 631 MB of archives.
After this operation, 1317 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.11.3 [631 MB]
17% [1 elasticsearch 132 MB/631 MB 21%]
```

Figure 37 - Installing Elasticsearch on Ubuntu

During the installation, it is critical to note the token as it is given once the installation has been finished.

```
----- Security autoconfiguration information -----
Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.
The generated password for the elastic built-in superuser is : ██████████
If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.
```

Figure 38 - Security autoconfiguration information

The main path for configuring the Elastic is on /etc/elasticsearch/elasticsearch.yml. This .yml file includes all the configuration properties. Now it is time to start the elasticsearch service. Once the component has been initialized then it is important to configure elastic to run once the host is up. With that setting Elastic will not need to start manually everytime.

²⁷ Paro, A. (2022). Elasticsearch 8.X Cookbook - Fifth Edition: Over 180 Recipes to Perform Fast, Scalable, and Reliable Searches for Your Enterprise.

```
root@hubcyber:/etc/elasticsearch# systemctl start elasticsearch
root@hubcyber:/etc/elasticsearch# systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@hubcyber:/etc/elasticsearch# curl -X GET "localhost:9200"
curl: (52) Empty reply from server
root@hubcyber:/etc/elasticsearch#
```

Figure 39 - Elasticsearch system service restart

After that trying to send a request using curl on the homepage an empty response will be given. That occurs because the page has not been yet trusted with secure http. The option `-k` will help in that case to ignore the certificates and continue the process. After that, a curl request with browser-based authentication bearer, with the token provided on Elastic, will successfully respond. That confirms that Elastic Database is up and running.

```
root@hubcyber:/etc/elasticsearch# curl -X GET -k https://elastic:elastic@localhost:9200/
{
  "name" : "hubcyber.work",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "P...",
  "version" : {
    "number" : "8.11.3",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "64...",
    "build_date" : "2023-12-08T11:33:53.634979452Z",
    "build_snapshot" : false,
    "lucene_version" : "9.8.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figure 40 - Response from Elasticsearch

According to the official documentation, Kibana²⁸, which is used as the user interface of Elastic database, should be installed only after installing Elasticsearch. Installing in this order ensures that the components each product depends on are correctly in place. Already added Elastic package source in the previous step, it can just install the remaining components of the Elastic Stack using apt (`sudo apt install kibana`). Now a generated token is needed to be configured on Kibana which will be used as an authentication mechanism between Kibana and Elasticsearch.

```
mike@hubcyber:~$ sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
eyJ:
NDM(
zMzNzc2
nNnIn0=
```

Figure 41 - Creating an Elastic enrollment token

²⁸ Kibana: Explore, Visualize, Discover Data | Elastic. (n.d.). Elastic. <https://www.elastic.co/kibana>

Now, the generated token must be submitted on Kibana to be successfully configured. On the binaries of Kibana a setup tool exists named kibana-setup. Once this tool runs it will ask for the input of user. There the JWT token must be submitted as follows:

```
mike@hubcyber: /usr/share/kibana/bin$ sudo ./kibana-setup
? Enter enrollment token: eyJ2ZXIiOiI4LjExLjMiLCJhZHIiOiI0LsiMTAuMTAuMTAuNDU5MjAwIiwiaWF0IjE6IjIwZTljMwYyQ2Q4ZGI1Y2
NjN2MyZTEyNWw3MjQ1ZmZnc2NDM0MGI5MzVmZW1Y2QzMmI2NDk3ZDg4NDYyIiwiaWF0IjE6IjIwZTljMwYyQ2Q4ZGI1Y2Q4ZGI1Y2
hQULRIS0Y0NzVrak9HZnNnIn0=

✓ Kibana configured successfully.

To start Kibana run:
  bin/kibana
mike@hubcyber: /usr/share/kibana/bin$
```

Figure 42 - Enrollment token creation

As Elastic this time Kibana will be also required to be active from when the host is up.

```
mike@hubcyber: /usr/share/kibana/bin$ sudo systemctl start kibana
mike@hubcyber: /usr/share/kibana/bin$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.
mike@hubcyber: /usr/share/kibana/bin$
```

Figure 43 - Kibana installation

To verify that Kibana service has started localhost should now listen on port 5601.

```
mike@hubcyber: /usr/share/kibana/bin$ ss -lntp
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port    Process
LISTEN     0          128        *:*                   *:*                   tcpd
LISTEN     0          100       0.0.0.0:995           0.0.0.0:*             sshd
LISTEN     0          100       0.0.0.0:993           0.0.0.0:*             sshd
LISTEN     0          4096      127.0.0.53%lo:53      0.0.0.0:*             ntpd
LISTEN     0          100       0.0.0.0:587           0.0.0.0:*             sshd
LISTEN     0          100       0.0.0.0:143           0.0.0.0:*             sshd
```

Figure 44 - Verification of Kibana running on port 5601

For security reasons, a web server must be installed for Kibana to be behind of the web server. In this case nginx web server is going to be installed. Once the nginx web server ²⁹installed on the default file of the configuration a proxy pass will be added onto location. That ensures that whenever a request is coming on localhost on port 80 (root page of nginx) the request will be proxied on Kibana.

²⁹ Songer, A. (2021, April 19). Install and configure Nginx for Elasticsearch, Logstash, Kibana. Austin Songer. <https://www.songer.pro/install-and-configure-nginx-for-elasticsearch-logstash-kibana/>

```
location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    proxy_pass http://127.0.0.1:5601;
}
```

Figure 45 - Setting up nginx proxy pass

Afterwards, nginx service must be restarted for the web server to be initiated with the new settings. Once the above has been completed the procedure can continue by simply initializing a remote connection of the Ubuntu Server using ssh with a dynamic port forwarding. (that means that everything running on the remote host is available on the remote user on the requested specific port). The user can now navigate on localhost and submit the elastic credentials on the login form.

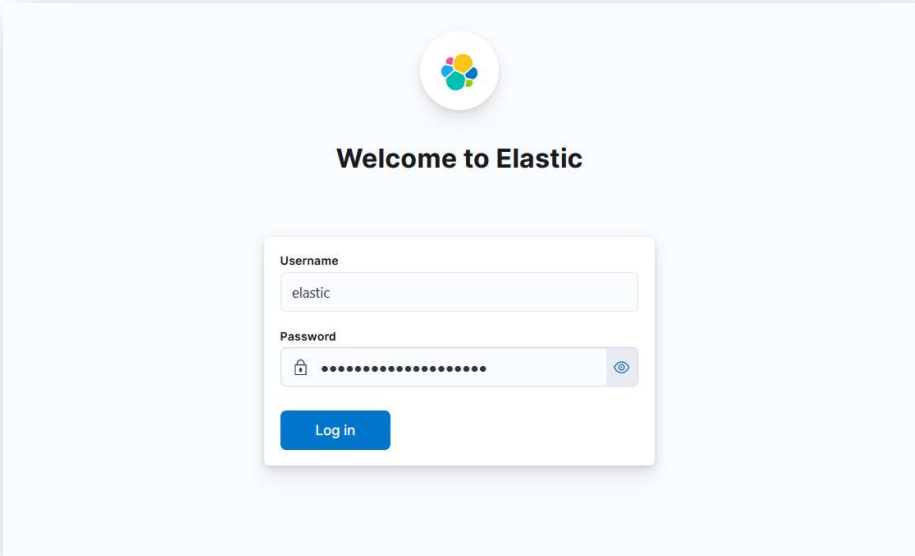


Figure 46 - Elasticsearch login page

Once the user successfully logs in to Elastic the options “Add Integrations” must be chosen. The first package that is going to be installed is Fleet Server which is a component of the Elastic Stack used to centrally manage Elastic Agents. It is initiated as a component of an Elastic Agent on a host designated to function as a server. A single Fleet Server process can manage multiple Elastic Agent connections. Its responsibilities include updating agent policies, gathering status information, and coordinating actions among Elastic Agents.

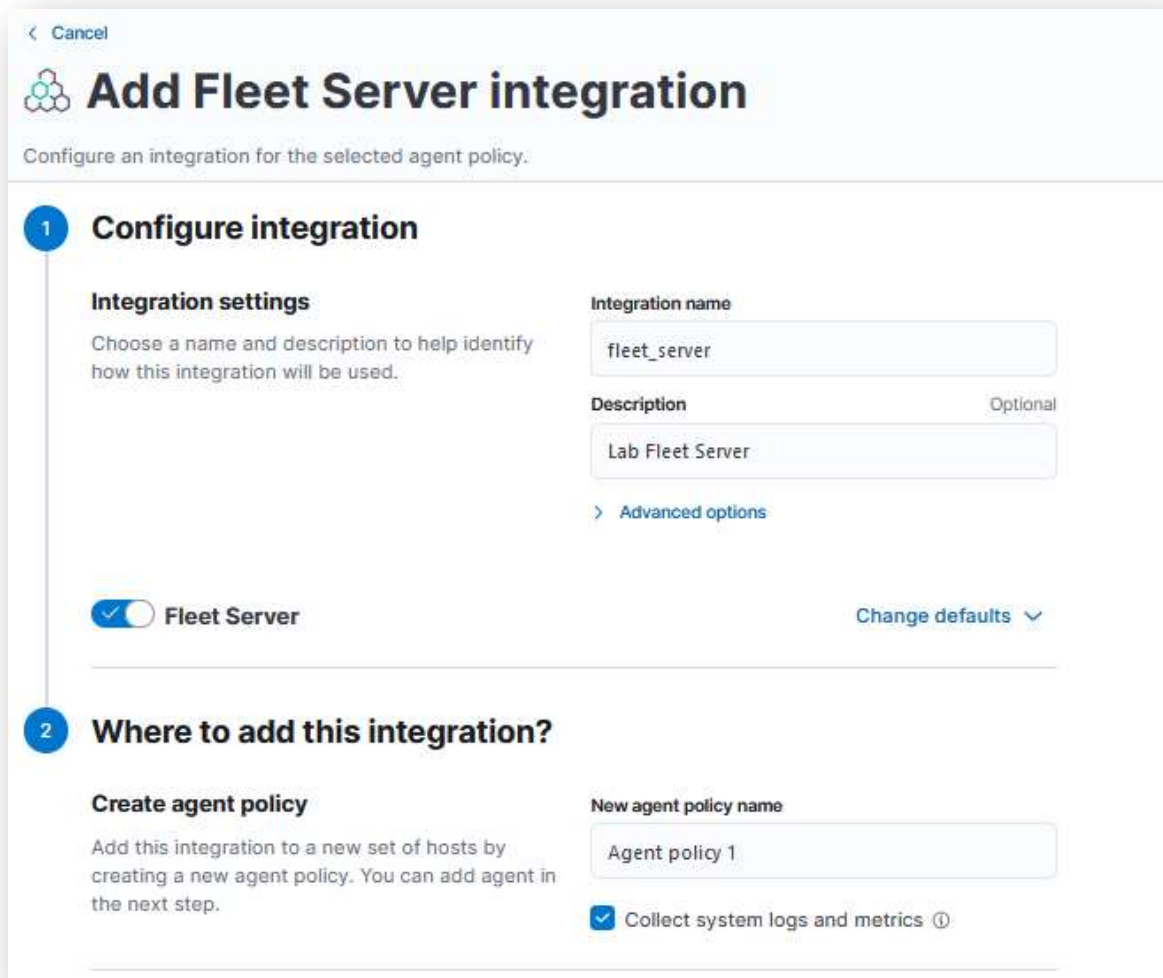


Figure 47 - Fleet server installation

Since the lab has been created for testing purposes the Fleet server can belong on the same host that is being used as a server (mail server, elastic stack etc). Fleet will collect the logs of all the machines that are enrolled with Fleet's agent³⁰. A step-by-step guide of the installation is available by Elastic's interface. To proceed to the installation a generated command will be provided to the user showing which has to be installed on the machine that will host the fleet server. In the lab's case that will be Ubuntu Server.

³⁰ Deploy on-premises and self-managed | Fleet and Elastic Agent Guide [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/fleet/current/add-fleet-server-on-prem.html>

```

mike@hubcyber:~/elastic-agent-8.11.3-linux-x86_64$ sudo ./elastic-agent install --fleet-server-es=https://10.10.10.4:9200 --fleet-server-service-token
=AAEAAWVsYXN8aWVzZXlZcXQtc2VydWVyL3Rva2VuLTE3MDM5NTMyODI1Mjg6dXdkdXdaEdCVWlUX1NaYlBMDRDRPekVmQQ --fleet-server-policy=fleet-server-policy --fleet-server-e
s-ca-trusted-fingerprint=20e9c1f0cd8db5ccc7c2e125c72457337764340b935fec5cd32b6497d8841ab2 --fleet-server-port=8220 --insecure
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:Y
Copying files.....
..... DONE
Installing service..... DONE
Starting service... DONE
Enrolling Elastic Agent with Fleet.....{"log.level":"info","@timestamp":"2023-12-30T16:37:44.877Z","log.origin":{"file.name":"cmd/enroll_cmd.go","f
ile.line":411},"message":"Generating self-signed certificate for Fleet Server","ecs.version":"1.6.0"}
.....{"log.level":"info","@timestamp":"2023-12-30T16:37:47.828Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":807},"message":"Fleet Ser
ver - Starting: spawned pid '50760'", "ecs.version":"1.6.0"}
.....{"log.level":"info","@timestamp":"2023-12-30T16:37:51.831Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":788},"message":"Fl
eet Server - Running on policy with Fleet Server integration: fleet-server-policy; missing config fleet.agent.id (expected during bootstrap process)","ecs
.version":"1.6.0"}
.....{"log.level":"warn","@timestamp":"2023-12-30T16:37:51.832Z","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":107},"messa
ge":"SSL/TLS verifications disabled.", "ecs.version":"1.6.0"}
.....{"log.level":"info","@timestamp":"2023-12-30T16:37:52.762Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":479},"message":"Starting enrollme
nt to URL: https://hubcyber.work:8220/", "ecs.version":"1.6.0"}
.....{"log.level":"warn","@timestamp":"2023-12-30T16:37:52.987Z","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":107},"mess
age":"SSL/TLS verifications disabled.", "ecs.version":"1.6.0"}
.....{"log.level":"info","@timestamp":"2023-12-30T16:37:54.788Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":277},"message":"Successfully
triggered restart on running Elastic Agent.", "ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
DONE
Elastic Agent has been successfully installed.

```

Figure 48 - Installing Fleet server on the host

✓

Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. For additional guidance, see our [installation docs](#).

Linux Tar

Mac

Windows

RPM

DEB

```

curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.3-lin
tar xzvf elastic-agent-8.11.3-linux-x86_64.tar.gz
cd elastic-agent-8.11.3-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://10.10.10.4:9200 \
  --fleet-server-service-token=AAEAAWVsYXN8aWVzZXlZcXQtc2VydWVyL3Rva2VuLTE3MDM5NTMyODI1Mjg6dXdkdXdaEdCVWlUX1NaYlBMDRDRPekVmQQ \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=20e9c1f0cd8db5ccc7c2e125c72457337764340b935fec5cd32 \
  --fleet-server-port=8220

```

✓

Fleet Server connected

You can now continue enrolling agents with Fleet.

Figure 49 - Fleet server installation generated command

Fleet Server has been successfully configured. In that step, Fleet agent can be installed on the hosts of the lab, especially on Windows box which would be a client. After the above setup finishes a new widget regarding the Agents will appear. In this section, a utility to choose between different operating systems will be given to the user. In this case, the lab includes a client running a Windows 10. In each case a script will be provided for the installation of Fleet agent. The script below is getting executed as a PowerShell script.

```
P5 C:\Users\mike\elastic-agent-8.11.3-windows-x86_64> $ProgressPreference = 'SilentlyContinue'
>> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.3-windows-x86_64.zip -OutFile elastic-agent-8.11.3-windows-x86_64.zip
>> Expand-Archive .\elastic-agent-8.11.3-windows-x86_64.zip -DestinationPath .
>> cd elastic-agent-8.11.3-windows-x86_64
>> .\elastic-agent.exe install --url=https://10.10.10.4:8220 --enrollment-token=0DFianY0d0JaY25KC --insecure
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
Copying files.....
```

Figure 50 - Adding Windows host on Fleet Server

Once the installation finishes successfully, the widget will reach its end with a mark indicating the successful enrollment of the agent.

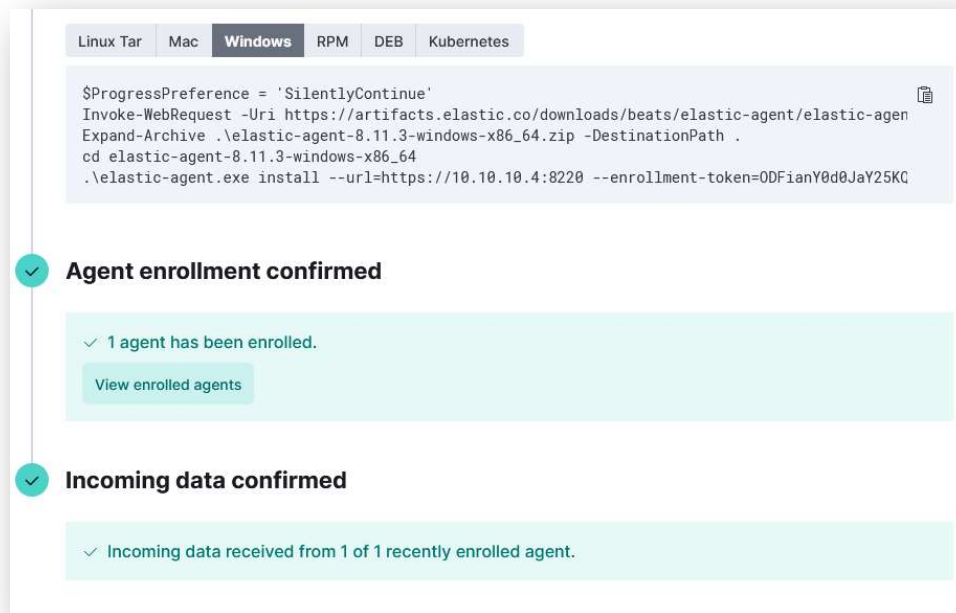


Figure 51 - Fleet Server success installation message

Fleet Server has been created to manage all the machines of the lab from a centralized host. That means that each agent is feeding the Fleet Server with their logs. These logs can be handled also individually. Besides that, updates are being handled from the fleet server and will instantly take place on each agent without any more user interaction. After installing Fleet server, it is time to install an integration which will help to monitor the logs from security side. For that reason, Elastic Defend integration³¹ is going to be installed. This provides the known full package with Elastic EDR Detection & Response software that is being used from Cyber Security Analysts around the world. The following configurations are being provided during the installation.

³¹ Install and configure the Elastic Defend integration | Elastic Security Solution [8.12] | Elastic. <https://www.elastic.co/guide/en/security/current/install-endpoint.html>

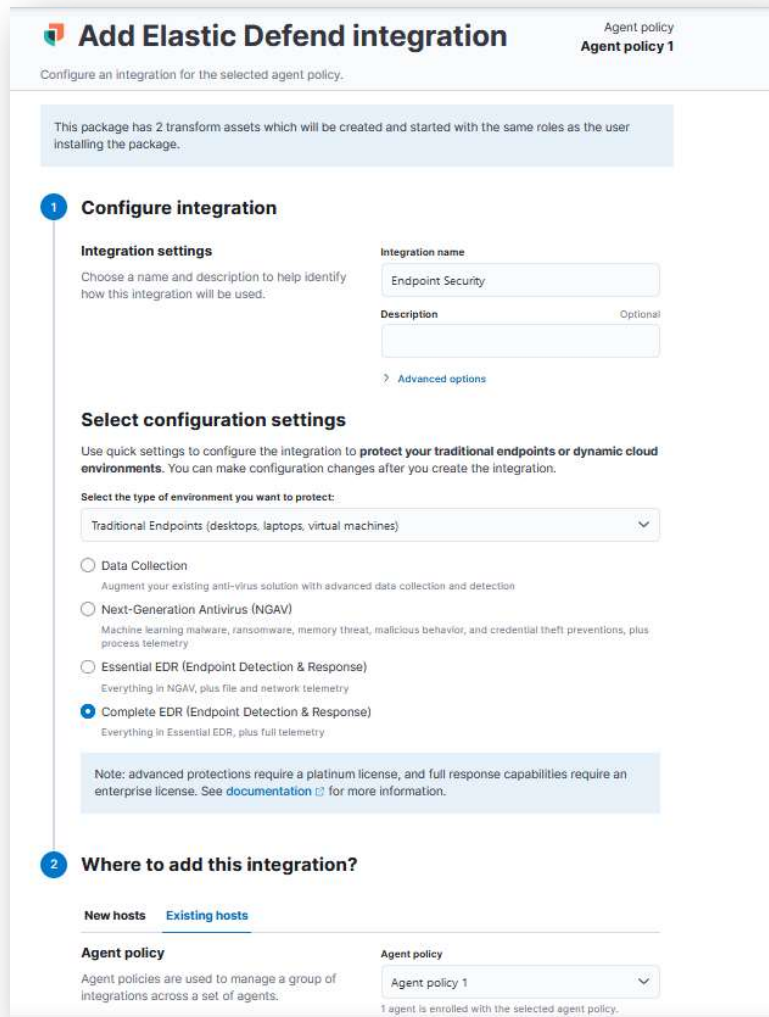


Figure 52 - Setting up Elastic Defend integration

To verify that the installation has finished without any problems it is possible to check if the Endpoint folder has been installed on the enrolled client of the Fleet server. The screenshot below shows that the EDR package has been successfully installed. For further information, installation log files can be seen on the folder.

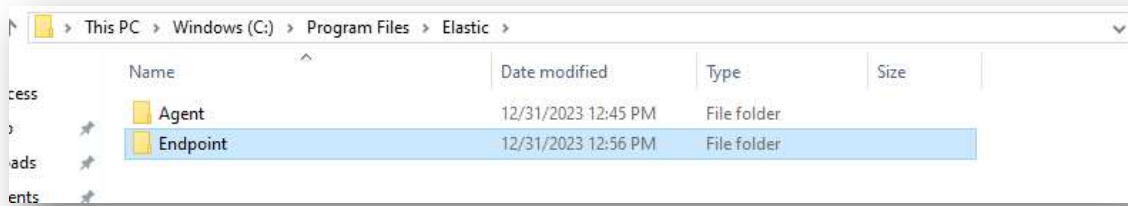


Figure 53 - Folders of Elastic on Windows host

By navigating to Elastic Defend menu an error message will appear regarding the API key that has not been installed yet. To continue the proper installation, the generation of an API key is necessary.

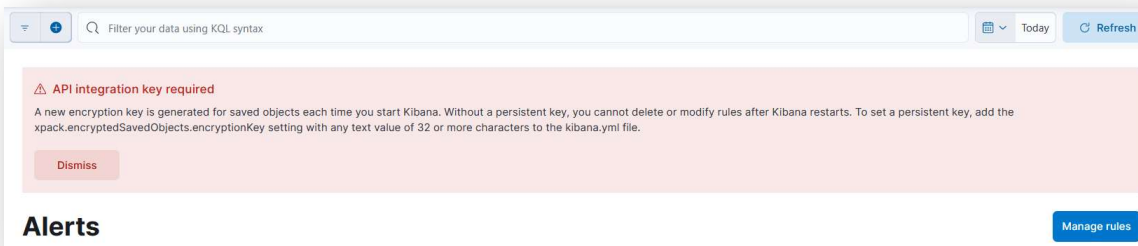


Figure 54 - Missing API integration key

On the Ubuntu host where the elasticsearch and kibana packages have been installed it is possible to generate the required API key. More specifically, on kibana binary folder the script “kibana-encryption-keys” will generate three encrypted keys that can be used on the kibana.yml configuration file.

```
mike@hubcyber:~/usr/share/kibana/bin$ sudo ./kibana-encryption-keys generate
## Kibana Encryption Key Generation Utility

The 'generate' command guides you through the process of setting encryption keys for:

xpack.encryptedSavedObjects.encryptionKey
  Used to encrypt stored objects such as dashboards and visualizations
  https://www.elastic.co/guide/en/kibana/current/xpack-security-secure-saved-objects.html#xpack-security-secure-saved-objects

xpack.reporting.encryptionKey
  Used to encrypt saved reports
  https://www.elastic.co/guide/en/kibana/current/reporting-settings-kb.html#general-reporting-settings

xpack.security.encryptionKey
  Used to encrypt session information
  https://www.elastic.co/guide/en/kibana/current/security-settings-kb.html#security-session-and-cookie-settings

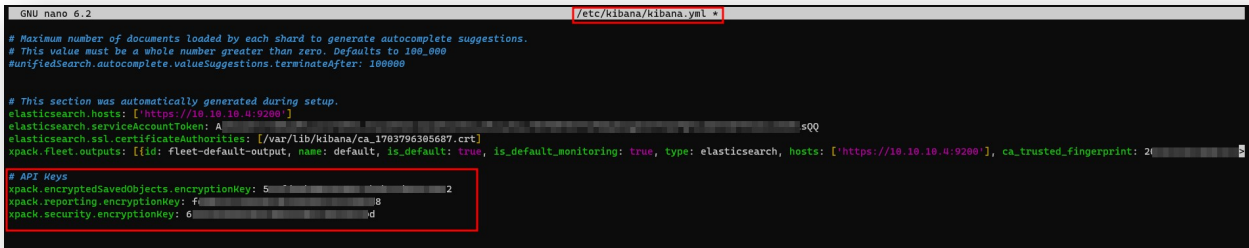
Already defined settings are ignored and can be regenerated using the --force flag. Check the documentation links for instructions on how to rotate encryption keys.
Definitions should be set in the kibana.yml used configure Kibana.

Settings:
xpack.encryptedSavedObjects.encryptionKey: 51[redacted]2
xpack.reporting.encryptionKey: f6[redacted]8
xpack.security.encryptionKey: 6e[redacted]d

mike@hubcyber:~/usr/share/kibana/bin$
```

Figure 55 - Generating Kibana encryption keys

The above screenshot illustrates the generation of the keys for many packages like reporting and security which are specifically used by the Elastic Defend integration. Writing kibana.yml file with the keys the installation then can proceed.



```
GNU nano 6.2 /etc/kibana/kibana.yml
# Maximum number of documents loaded by each shard to generate autocomplete suggestions.
# This value must be a whole number greater than zero. Defaults to 100_000
#unifiedSearch.autocomplete.valueSuggestions.terminateAfter: 100000

# This section was automatically generated during setup.
elasticsearch.hosts: ['https://10.10.10.4:9200']
elasticsearch.serviceAccountToken: A...500
elasticsearch.ssl.certificateAuthorities: [/var/lib/kibana/ca_1703796305687.crt]
xpack.fleet.outputs: [{"id": fleet-default-output, name: default, is_default: true, is_default_monitoring: true, type: elasticsearch, hosts: ['https://10.10.10.4:9200'], ca_trusted_fingerprint: 2...}

# API Keys
xpack.encryptedSavedObjects.encryptionKey: 5...2
xpack.reporting.encryptionKey: f...8
xpack.security.encryptionKey: 6...d
```

Figure 56 - Adding encryption keys on yaml file

The encryption keys have been enrolled successfully. Now it is time to proceed with the utilities the Elastic Defend package provides. One of the most important utilities is the Rules. The term "Defend Rules"³² could refer to predefined or custom rules within Elastic Security. These rules are used to identify specific patterns or behaviors in log and event data that may indicate security threats or anomalies. When certain conditions defined by these rules are met, alerts are generated to notify security teams of potential issues.

Rule Types

- **Prebuilt Rules:** Elastic Security comes with a set of prebuilt rules that cover common security use cases. These rules are designed to detect known attack patterns or suspicious activities.
- **Custom Rules:** Organizations can create custom rules tailored to their specific security requirements. These rules are often based on the organization's knowledge of its own infrastructure and the types of threats it is likely to face.

Use Cases

- **Threat Detection:** Rules can be configured to detect specific threats, such as known malware signatures, unauthorized access attempts, or patterns indicative of a security incident.
- **Anomaly Detection:** Some rules may focus on detecting anomalous behavior within the network or system, helping identify potential insider threats or unusual patterns that could signify a security issue.
- **Compliance Monitoring:** Rules can be designed to check for compliance with security policies and standards.

Incident Response

When a rule generates an alert, Elastic Security provides tools for incident response. Security teams can investigate alerts, gather additional context, and take appropriate action to mitigate the impact of security incidents.

³² Anson, S. (2020). Applied incident response. John Wiley & Sons.

The package provides some prebuilt rules for many operating systems such as Windows and Linux based. It is possible to download them by clicking on the red underlined button as the screenshot indicates:

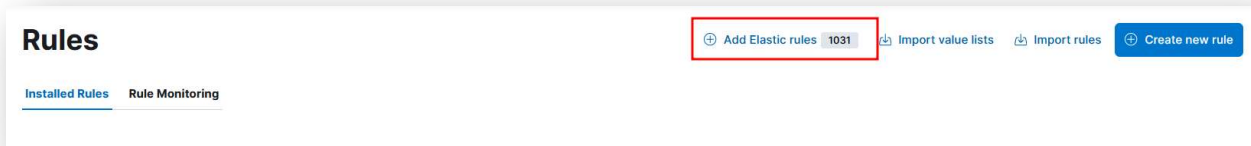


Figure 57 - Predefined Elastic Rules

The rules have been successfully installed on the stack and they can be enabled whenever they might seem useful from the user controlling the Elastic SIEM.

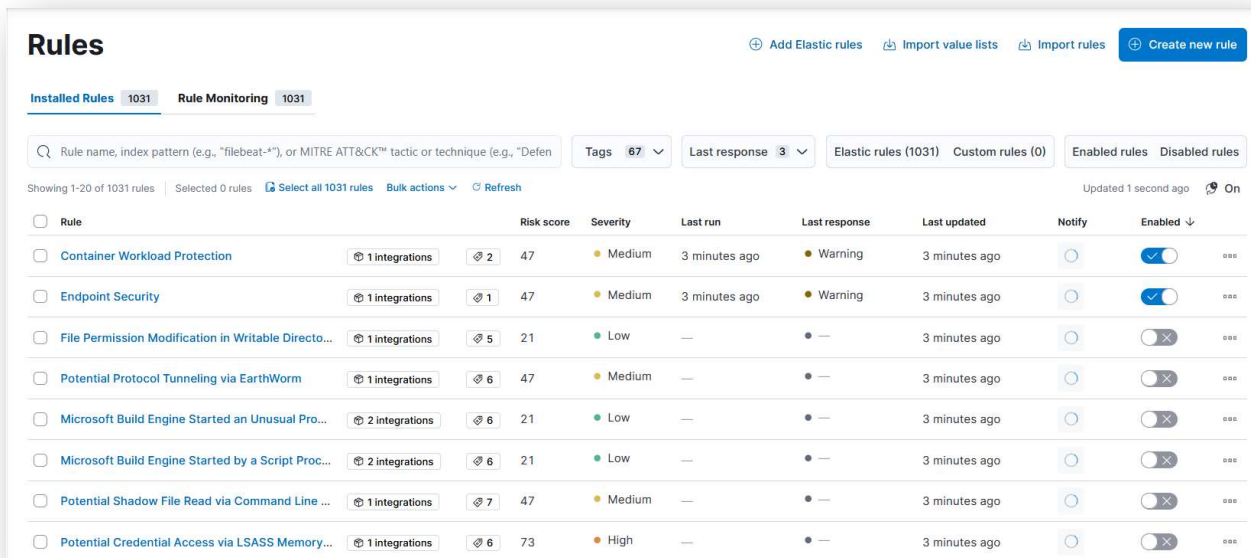


Figure 58 - Table of Elastic's default rules

Windows does not provide logs in certain useful formation. For that reason, Windows integration includes many data streams, and it is being used from the SIEM to adjust the logs on certain format that can be easily handled.

Sysmon, which stands for System Monitor, is a Windows system service and device driver designed to record system activity to the Windows event log. It is developed by Microsoft and is designed to provide detailed information about various events on a Windows system, offering enhanced visibility and improved security. Sysmon provides more detailed and granular logging compared to standard Windows event logs. It captures information about process creations, network connections, file creations, registry changes, and other critical system activities.

Sysmon is often used as part of a comprehensive security monitoring strategy. It helps organizations detect and respond to suspicious or malicious activities on their systems by providing a deeper level of insight into system events. By monitoring a wide range of activities, Sysmon can aid in the early detection of security incidents. Security teams can use Sysmon logs to identify potential threats, investigate incidents, and respond promptly to security events.

Security professionals and threat hunters use Sysmon to proactively search for indicators of compromise or abnormal behavior within a system. By analyzing Sysmon logs, security teams can identify patterns that may indicate the presence of advanced threats. Sysmon logs can be easily integrated into Security Information and Event Management (SIEM) solutions. This integration allows organizations to aggregate and correlate Sysmon data with other security events, providing a more comprehensive view of the security landscape. Sysmon is configurable, allowing administrators to fine-tune the types of events they want to monitor. This customization enables organizations to focus on specific aspects of system activity relevant to their security requirements.

Sysmon is freely available and widely adopted in the security community. Its open-source nature encourages collaboration and the sharing of custom configurations and rulesets to enhance its effectiveness. Sysmon operates in real-time, continuously monitoring system activity. This proactive approach allows organizations to identify and address security issues as they occur.

In summary, Sysmon is a powerful tool that contributes to a robust security posture by providing detailed visibility into Windows system activities. Its use is particularly valuable in security monitoring, incident detection and response, and overall system visibility.

The following Windows integration is available on the Elastic and can be downloaded. To integrate with the current stack, it is necessary to configure it on the policy that the client host has been initialized.

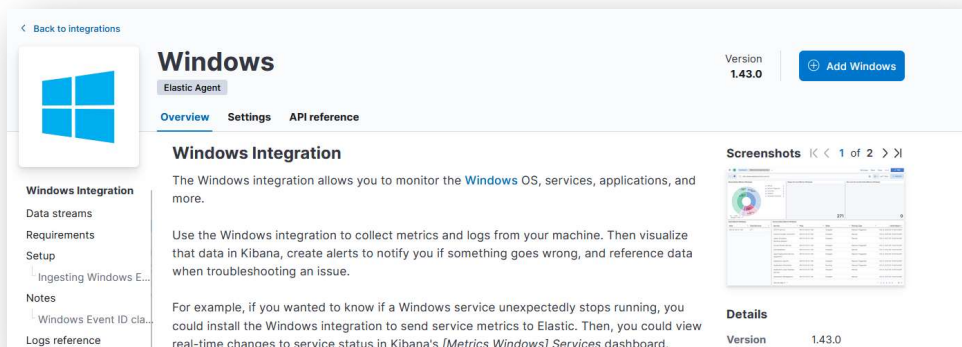


Figure 59 - Windows sysmon integration module

For Sysmon data stream to apply on the Windows host, must make sure that the Sysmon is installed on the host. Sysmon can be downloaded from the Microsoft's official page <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>. The screenshot below illustrates the installation command that has been used for installing Sysmon.


```
PS C:\Users\mike\Desktop\Sysmon> .\Sysmon64.exe -i -n

System Monitor v15.11 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Figure 60 - Installing sysmon executable on Windows

After installing Sysmon the Windows integration requires some specific configurations.

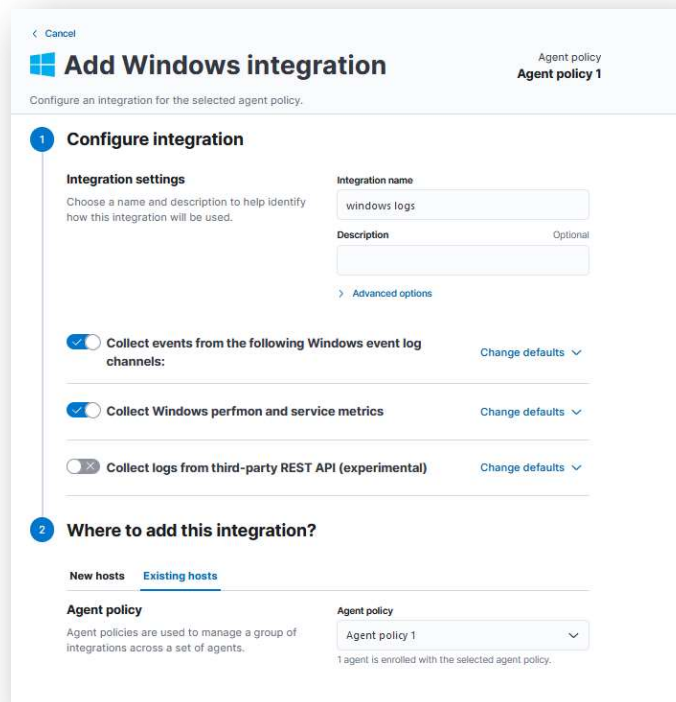


Figure 61 - Configuration of Windows integration

After installing the following, create a data stream regarding the Sysmon logs coming from the Windows 10 host. On **Analytics > Discover** press the blue button next to the search bar and select Create a new data view. A new widget will be displayed showing the indexes of the sources that are available to choose from. On the new data view the following configurations must be applied.

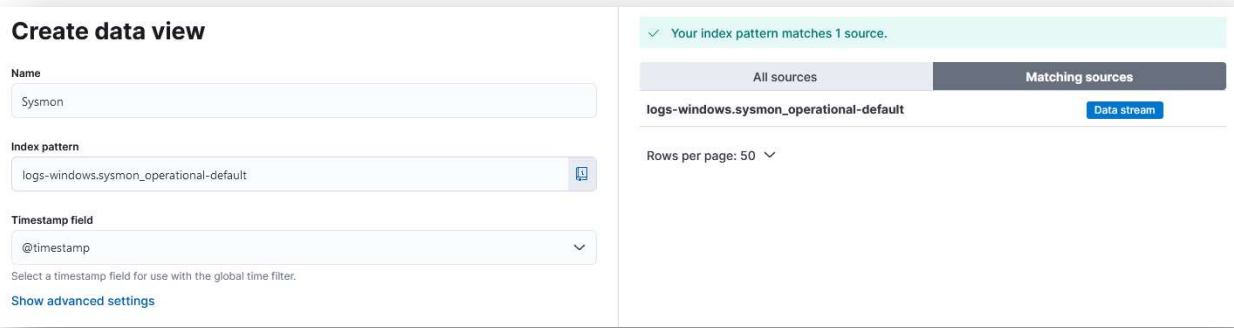


Figure 62 - Creating a data view

Below screenshot show that Elastic is managing ton of logs that are being generated. They are displayed with timestamp and document columns. Any other field can be chosen for the logs to also display the required column.

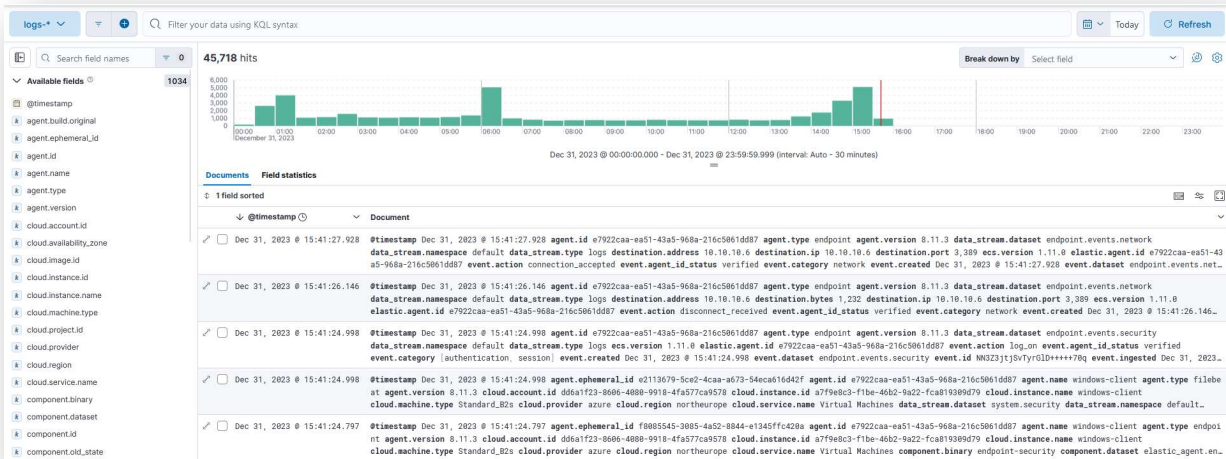


Figure 63 - Log collection panel

In the orchestrated testing scenario, a leveraged controlled environment to emulate a user-triggered event on a Windows host. The specific action involved initiating the calculator application (calc.exe) to simulate a process execution event. This deliberate activity aimed to replicate a scenario that could potentially be indicative of a user interacting with the system or an attacker attempting to execute arbitrary processes. Following the execution, Elastic SIEM assess its responsiveness and accuracy in logging the event. Within the SIEM interface, scrutinized the associated event.id, which serves as a unique identifier for the logged event. This step was crucial in verifying the system's ability to differentiate and classify diverse events accurately. Furthermore, an examined Elastic SIEM's capacity to capture any PowerShell commands associated with the executed process. This aspect is particularly relevant given the prevalent use of PowerShell in modern cyber threats for its scripting capabilities and potential misuse by adversaries.

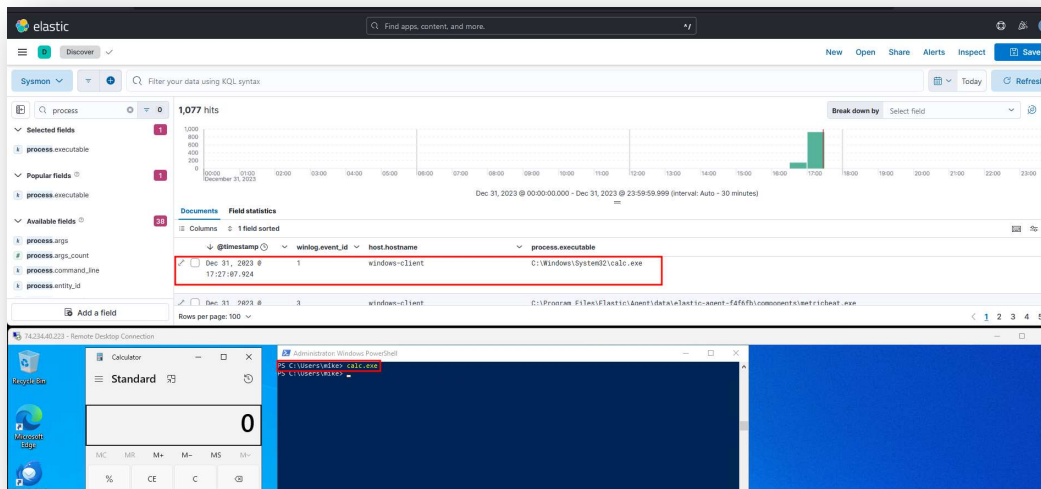


Figure 64 - Elastic detection of calc.exe test

The successful integration of Elastic SIEM with the testing environment, combined with its ability to log promptly and accurately the event.id and relevant PowerShell commands, displays its effectiveness in real-time event monitoring, threat detection, and incident response. This empirical validation contributes valuable insights to the broader discourse on the reliability and practical application of Elastic SIEM in enhancing cybersecurity postures.

Lab Testing

After the above step-by-step installation of all the hosts and software needed it is time to test if the hosts manage to work together. For the lab to work the following steps need to be executed one by one.

1. Sending an email from external domain to the specified mail domain **hubcyber.work** and specifically to the recipient "mike."
2. Proxmox Mail Gateway must proxy the email, which can be checked on the Tracking Center of PMG and relay the email on the private mail server. That can be also checked on the logs.
3. On the user's mail directory (Maildir) check for the incoming mail that Postfix managed to catch and save.
4. Check if the client running Thunderbird mailbox can fetch the incoming mails from the private mail server.

The following email is going to be the example which the lab expected to handle for the end-to-end delivery process. After sending the below email, it is expected for the Proxmox Mail Gateway to handle it.

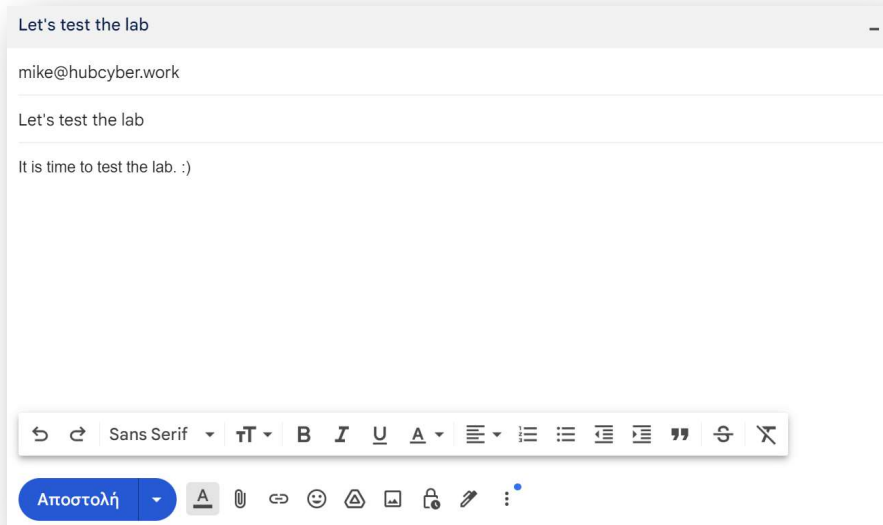


Figure 65 - Test email for transfer

On the Tracking Center of the Mail Gateway where the emails that are proxied can be tracked the email send is handled correctly.

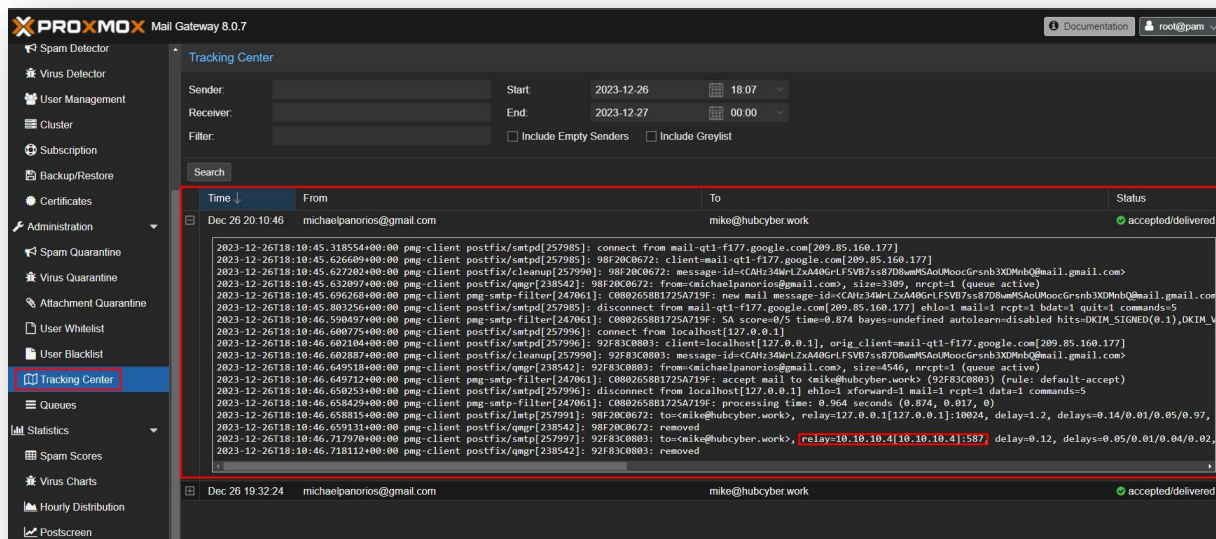


Figure 66 - Proxmox Tracking Center of the above email

In the provided logs from the Proxmox Mail Gateway (PMG), a series of events related to email transmission are recorded. The logs include details about the connection from the sender, identified as "mail-qt1-f177.google.com" with IP address 209.85.160.177, to the PMG client's SMTP server. The logs

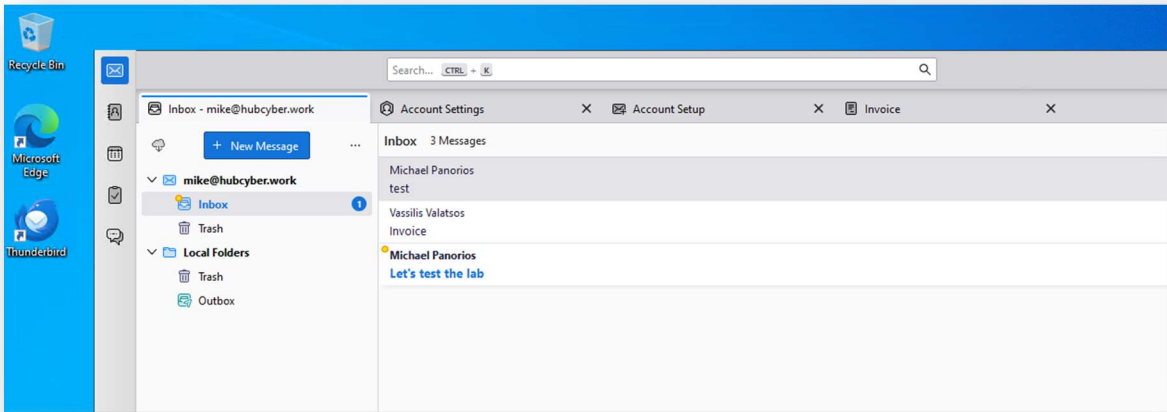


Figure 68 - Thunderbird sync with mail server

The email has been successfully retrieved from the mailbox and the user mike can view the contents of the email provided.

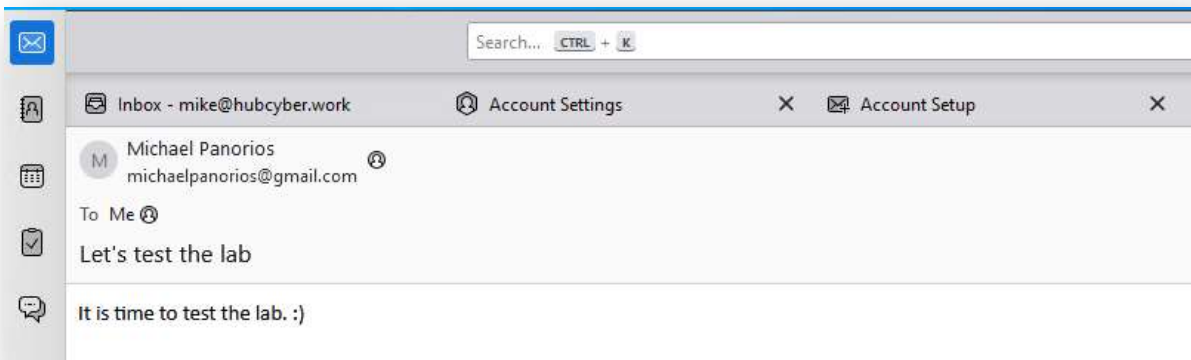


Figure 69 - Email reached the destination

Finally, the lab has been successfully installed and tested.

Phishing Techniques & Detection Methods

This dissertation is dedicated to the exploration of phishing detection and prevention, with a focus on harnessing the capabilities of Elastic. Phishing, a persistent cyber threat exploiting human vulnerabilities, necessitates advanced technological solutions for timely identification and mitigation. Elastic's robust framework, widely recognized for its scalability and real-time data analytics, stands out as a promising solution to address the dynamic nature of phishing attacks. The research objective lies in the seamless integration of Elastic's search and analytics functionalities to develop a comprehensive system adept at detecting and preventing phishing attempts. The strategic incorporation of machine learning algorithms and anomaly detection techniques within the Elastic ecosystem is anticipated to significantly augment the accuracy and responsiveness of phishing detection mechanisms. This study aspires to make a substantive contribution to fortifying cybersecurity defenses against the pervasive threat of phishing, leveraging the powerful features and capabilities inherent in Elastic. Elastic, as a powerful and versatile search and analytics platform, can play a significant role in addressing various aspects of phishing detection and prevention. While it may not directly mitigate every specific phishing technique, Elastic can contribute to the overall cybersecurity strategy. There are many phishing strategies being used by adversaries for stealing critical information and evade into enterprise networks. Behind every successful phishing attack, a threat actor has studied user behavior to identify the easiest route to stealing information and data. Nearly every type of phishing attack requires a user to click a link or open a file to provide entry into a system or automatically download malicious software. Cybercriminals have become experts at crafting seemingly harmless, targeted attacks to exploit unsuspecting users³³.

COMMON PHISHING TECHNIQUES

<i>URL SPOOFING</i>	Shortened links	Non-domain email addresses	File Attachments	
<i>SPEAR PHISHING</i>	Unsolicited emails	Links to shared drives	Unusual requests	Single or blank attachments
<i>WHALING</i>	Incorrect domain address	Use of personal email	Single or blank attachments	-
<i>BEC</i>	Sense of urgency	Unusual behaviors	CEO Fraud	-
<i>VISHING</i>	Sensitive Information needed	Pay small fees	Debt to be paid	-
<i>CLONE PHISHING</i>	Duplicate emails	Misspelled email addresses	Hyperlinked text	Cloned websites
<i>SMS PHISHING</i>	Unsolicited texts	Unknown numbers	Authentication request	-
<i>POP-UP PHISHING</i>	Browser notifications	New tab or window	Urgent messages	-
<i>SOCIAL MEDIA</i>	Offers or online discounts.	Surveys or contests	Friend requests	Comments videos photos

³³ 19 Most common types of phishing attacks in 2024 | UpGuard <https://www.upguard.com/blog/types-of-phishing-attacks>

EVIL TWIN	Duplicate Wi-Fi hotspots	Unsecure warnings	-	-
WEBSITE SPOOFING	Homograph attacks	URL misspellings	Website errors	-

URL Spoofing

Phishing emails are at the top of the list because they are one of the oldest and most popular forms of frauds. Most attempts employ emails to target individuals while seeming to be from a reliable source. Dedicated hackers will mimic an email format from a respectable corporation and add a malicious link, picture file that will deceive the victim into "confirming" their personal information or will automatically download dangerous code. Legitimate companies will never request sensitive details through email. Be wary of urgent notifications, as scammers often employ tactics like account breach alerts, payment failures, login verifications, or copyright infringement notices to deceive recipients. Avoid clicking on any links and instead verify information directly on the official website. Shortened links, commonly used to mask malicious URLs, pose a threat, so exercise caution, especially with services like Bitly or TinyURL³⁴.

Clue in the URL	Example
Includes redirection	http://3104.nnu4urys.info?http://c43n34.com?35u3b
The path contains a URL of a known organization	http://108.179.216.140/~bankofamerica/
Confused URL with non-valid pattern	http://sparkleyourcake.com/www.paypal.fr/
Special characters “-“ in the host name	http://yj4yb6hmb3.x-cant-bank-you-here-of-my-money.cn/yj4yb6hmb3/Oraliao_show_23Y
Long domain name	http://31837.9hzaseruijintunhfeugandeikisn.com/5/54878
Hostname is Encoded	http://www.%64isc%72%65%74%2done-%6ei%67h%74.%63o%6d
IP is Encoded	http://0x42.0x1D.0x25.0xC2/
E-mail Address in URL	http://username@hotmail.com.fddcol.com

Figure 70 - URL Spoofing examples

Watch out for non-domain email addresses, as scammers may use third-party providers or variations of legitimate domains. Always verify the sender's email address by hovering over it to ensure it matches the user or company name. Lastly, be cautious of spelling and grammar mistakes, which are red flags that can indicate a fraudulent email, particularly when originating from non-English speaking countries.

³⁴ Nakutavičiūtė, J, (2024, January 9). What is URL Spoofing? 2024 Explanation. NordVPN. <https://nordvpn.com/blog/url-spoofing/>

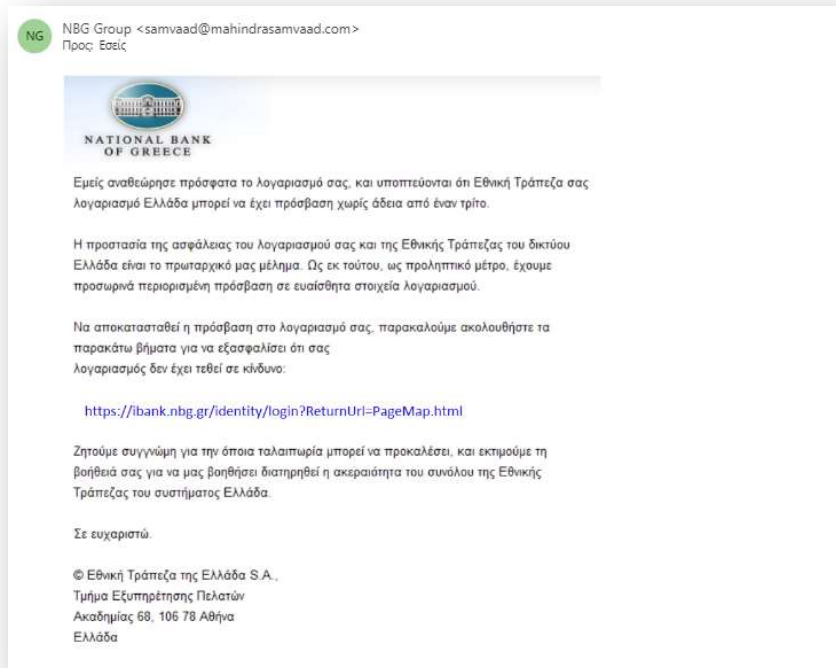


Figure 71 - URL Spoofing of National Bank of Greece

Spear Phishing

Spear phishing attacks³⁵ are highly focused versions of email phishing that target specific persons and organizations. Criminals can obtain publicly available information and attack whole corporations or departments using open-source intelligence (OSINT). Due to access to personal information, they may mislead readers into believing the email is an internal message or from a reliable source. Receiving requests for credentials beyond someone is pay grade within your company, reach out to the individual directly through an alternative communication channel to confirm the legitimacy of the request. This precaution becomes especially crucial in the event of a hacked email.

³⁵ Hadnagy, C., & Fincher, M. (2015). Phishing dark waters: The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons.

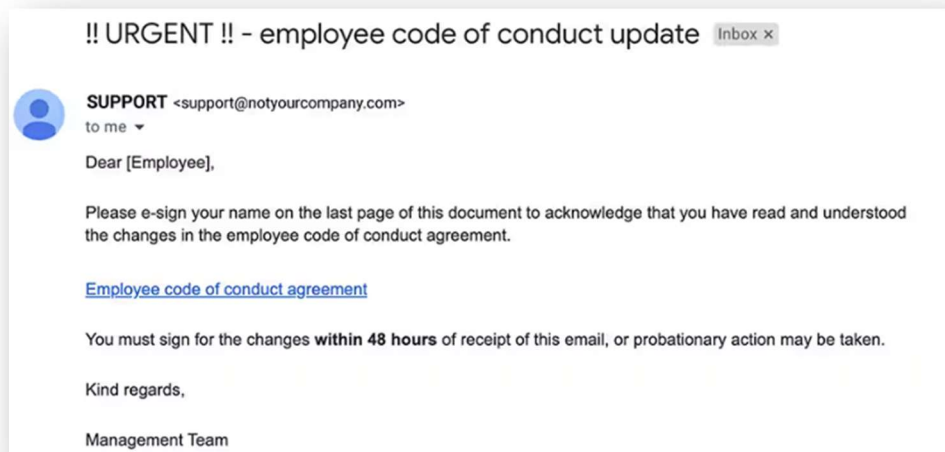


Figure 72 - Spearphishing example

Avoid sharing links to shared drives if the request appears to be from an internal or trustworthy source, as scammers may use corrupted links to redirect you to fake websites. Be cautious of unsolicited emails offering "important documents" for download; if did not request such files, it could be a fake email. Always verify the sender's identity before opening any attachments. Additionally, be wary of emails containing specific mentions of personal details, as scammers may use this information to falsely establish trust. Any obvious attempts to gain your trust should be met with suspicion, and verification of the sender's authenticity is paramount. Stay vigilant against these tactics to enhance your overall cybersecurity.

Whaling

If spear phishing emails target specific groups or individuals, whaling is the practice of targeting high-level executives. Also known as CEO fraud, whaling attacks are typically much more sophisticated, relying on OSINT, plenty of research into the company's business practices, and even a deep dive into social media accounts. Because the goal is to successfully dupe the executive, the emails are usually extremely fluent in business communications with near-perfect English. Whaling attacks, like spear phishing incidents, pose a heightened challenge for detection compared to typical phishing attacks due to their personalized nature, targeting specific individuals within an organization. While less sophisticated whale phishing relies on social engineering to deceive targets, cybercriminals executing whaling attacks often invest significantly in making the attack

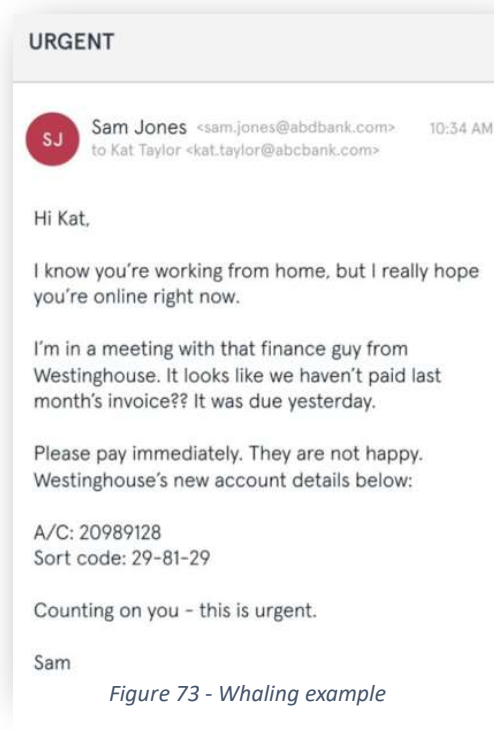


Figure 73 - Whaling example

appear exceptionally legitimate, driven by the potential for substantial returns. These attacks involve meticulous steps such as extracting information from publicly available social media profiles like Facebook, Twitter, and LinkedIn. Cybercriminals engage with the organization through email to grasp the email address structure and signature format, while also collecting general company details, including job titles, colleague names, third-party vendors, and any information exposed in prior data breaches. Moreover, if the targeted organization lacks robust email security measures, attackers may employ email spoofing techniques to create emails that seem to originate from a trusted source within the organization³⁶, further complicating detection efforts. Even in cases where the target organization has effective email security, attackers may exploit vulnerabilities in a third-party vendor's cybersecurity, enabling them to launch the cyber-attack using the vendor's domain or by acquiring a similar typo squatted domain name.

Business Email Compromise

A Business Email Compromise (BEC) is almost same as whaling³⁷ in that it impersonates the executive rather than trying to mislead them. Criminals will imitate or get access to a decision-making executive email account and send internal requests to lower-level workers. Scoular, an Omaha-based agribusiness firm, was the victim of a BEC assault in 2014. Keith McMurtry, the corporate controller, got an email from his CEO requesting an instant wire transfer to buy a Chinese-based firm. The email specified a lawyer who would handle the transaction, and McMurtry wired \$17.2 million to an offshore account. However, the email turned out to be false, including phony phone numbers and email addresses. When encountering communication related to large transactions or significant business deals, it is essential to be wary of a sense of urgency, as such processes typically undergo thorough scrutiny involving multiple individuals before finalization. If the communication appears unusually urgent and involves only a limited number of recipients (typically less than 2 or 3), it should trigger caution. Additionally, sophisticated Business Email Compromise (BEC) attacks may strive to maintain a professional tone, but subtle variations in language or personality could serve as indicators. If an executive's communication deviates from their usual style, it is prudent to remain vigilant for other signs of a potential phishing attack. Moreover, the absence of legal correspondence in business dealings raises concerns about legitimacy and legality. In such cases, it is crucial to involve a legal team or lawyer. If an email lacks legal representation, it is advisable to independently verify its legitimacy through the appropriate channels within the company's chain of command.

Vishing

Voice phishing, also known as "vishing," involves scammers attempting to extract information or money by placing a call to your phone number³⁸. With the advent of sophisticated technology, these criminals can now manipulate caller IDs to appear as if they are calling from a trusted source. Typically, the caller employs tactics that create a sense of urgency, aiming to appear authoritative and impede clear thinking on the recipient's part. Common vishing attack scenarios include falsely claiming a family member is in distress and needs financial assistance, asserting that the IRS requires your social security number for tax return confirmation, demanding payment for a non-existent prize or vacation, stating

³⁶ National Cyber Security Centre of UK, Whaling: how it works, and what your organization can do about it. <https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it>

³⁷ What is Business Email Compromise (BEC)? | Microsoft Security. <https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>

³⁸ Atkins, C. (2018). Phishing attacks: Advanced Attack Techniques. Createspace Independent Publishing Platform.

that a warrant has been issued for your arrest, suggesting your vehicle qualifies for an extended warranty, indicating suspicious activity on your bank account, promising guaranteed returns on investment opportunities, or asserting the presence of a large sum of debt that needs immediate payment. To identify voice phishing attempts, be cautious of calls from blocked or unidentified numbers, as phishing calls often originate from such sources. If you answer and the caller raises suspicion, it is advisable to hang up immediately. Moreover, remain vigilant against requests for sensitive information or money over the phone, as legitimate government organizations conduct official business through mail and will never solicit personal information through a phone call.

Clone Phishing

Clone phishing deviates from the traditional method of sending fake emails by duplicating a legitimate email sent by an individual or company to create a nearly identical version³⁹. This replicated email is then resent to the target, often with a new corrupted attachment or link. The email will give the impression of being a resend and may prominently display at the top of the victim's inbox. In more advanced cases, the phisher may use a fake but similar email, while sophisticated hackers will go a step further by spoofing the email address to make it appear as if sent from a genuine domain. To identify clone phishing attempts, closely examine your recent emails for duplicates. If a duplicate is spotted, scrutinize the newer version for any newly introduced links, which may indicate a phishing attempt. Always verify the correct link by comparing it to previous email communications. Another potential red flag is misspelled email addresses; even minor errors may be present in fake emails, though they may go unnoticed by an untrained eye. Additionally, pay attention to hyperlinked text. When hovering over a link, browsers typically reveal the actual address at the bottom left of the screen. If the URL does not match the linked text, it could be a sign of phishing. It is crucial to exercise caution and verify the legitimacy of links. Moreover, be wary of cloned websites that may mimic the appearance of legitimate sites to deceive users. Always validate the authenticity of communication and links to enhance your cybersecurity.

SMS Phishing

SMS phishing, commonly known as "smishing," operates similarly to phishing, but instead of phone calls, scammers employ SMS text messages containing links or attachments to deceive individuals⁴⁰. Due to the perceived privacy of personal phone numbers, people tend to trust text messages more, making them susceptible to smishing attacks. However, contemporary smartphones make it just as convenient for hackers to exploit text message URLs and compromise personal data. To recognize SMS phishing attempts, be cautious of unsolicited texts, especially those offering free coupons, incredible deals on unrelated products, or



Figure 74 - SMS Phishing example

³⁹What is clone phishing? Check Point Software. (2023, November 25). <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/what-is-clone-phishing/>

⁴⁰ What is Smishing and How to Defend Against it. (2023, November 20). [www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it](https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it)

requests to confirm account information, check order status, or verify medical details, particularly if you did not sign up for such alerts directly. Another red flag is receiving messages from unknown numbers requesting information.

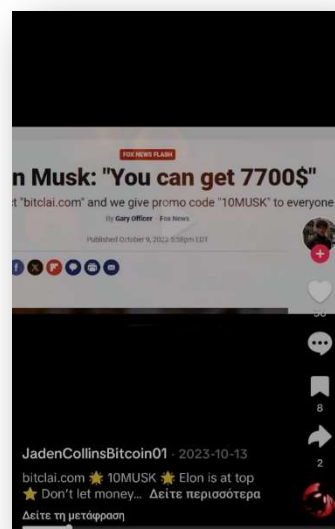
Utilizing free number lookup services or contacting related individuals for verification can help ascertain the legitimacy of the message. Generally, refrain from clicking on any provided links in the text and avoid engaging with the sender. Additionally, be wary of unauthorized authentication requests. If you receive such a request, someone may be attempting to access one of your accounts. It is crucial to change your password immediately to prevent further unauthorized access. Staying vigilant and following these precautions can help safeguard against the risks associated with SMS phishing.

Pop-up Phishing

Although most people have an ad or pop-up blocker installed on their web browsers, hackers can still embed malware on websites. Notification boxes or look like legitimate ads on a web page. Anyone that clicks on these pop-ups or ads will become infected with malware⁴¹. To identify pop-up phishing attempts and safeguard online security, users should be wary of certain indicators. When prompted by browsers like Chrome or Safari to "Allow" or "Decline" notifications on a new site, exercise caution, as browsers may not filter out spam notifications, potentially leading to the automatic download of malicious code. Surfing the web without pop-up blockers, particularly on mobile devices, can trigger unexpected new tabs or windows containing links to download malware, posing a significant threat. Additionally, be cautious of urgent messages in pop-ups claiming the need to update antivirus software or renew a subscription, as these are clear signs of phishing. It is essential to address legitimate updates, renewals, payments, or account-related issues directly on the official website rather than through pop-ups on unrelated or suspicious sites. By remaining vigilant and recognizing these indicators, users can enhance their protection against the potential risks associated with pop-up phishing.

Social Media Phishing

In addition to email, social media has become a prominent avenue for phishing attacks due to the vast amount of personal information shared on platforms like Facebook, Instagram, Snapchat, and LinkedIn. The widespread use of these networks for networking purposes has increased the susceptibility to social engineering attacks, aiming to exploit sensitive data. Phishing tactics on social media often involve deceptive links leading to malicious websites or scammers posing as individuals in distress to extract money. Common methods include offers, online discounts, surveys, contests, friend requests, fake videos, and comments on posts. Recognizing social media phishing requires vigilance, particularly in assessing suspicious links, even if seemingly sent by friends, and being cautious of messages or friend requests from unknown individuals with minimal activity, often indicative of potential phishing attempts. Staying alert



⁴¹ Hardy, J. (2023, May 1). What you need to know about Pop-Up Phishing — Affinity Technology Partners. Affinity Technology Partners. <https://www.affinitytechpartners.com/3n1blog/2018/5/3/scam-alert-what-you-need-to-know-about-pop-up-phishing>

and exercising caution on social media platforms are crucial to safeguard against evolving phishing threats and ensure online safety⁴².

Evil Twin

An evil twin phishing attack creates an unsecured Wi-Fi hotspot access point that baits unsuspecting users into connecting⁴³. Once connected, all inbound and outbound data can be intercepted, including personal data or financial information. Hackers can also prompt the users to visit a fake website portal in hopes the user will provide valuable authentication details. Evil twin phishing attacks are most common in public areas with free Wi-Fi, like coffee shops, libraries, airports, or hotels. The best way to prevent becoming an evil twin phishing target is to use a virtual private network (VPN) while using public Wi-Fi.

Website Spoofing

In the realm of cyber threats, website spoofing poses a significant risk as attackers craft entirely fake websites to deceive users and pilfer personal information. Notably, finance, healthcare, and social media platforms are frequent targets due to the wealth of critical data they house⁴⁴. A well-executed fake website mirrors the original's logos, text, colors, and functionality. To discern website spoofing, users should scrutinize URLs for subtle misspellings, often employed through homograph attacks, such as replacing "rn" with "m" or using "vv" instead of "w." Additionally, authentic websites are rarely perfectly replicated, so vigilant users may spot small errors like pixelated logos or misaligned text. It is paramount to halt website interaction if any discrepancies arise, particularly when accessed through links in emails or messages. Maintaining bookmarks for original websites serves as a helpful reference to ensure safe online navigation and mitigate the risk of falling prey to deceptive website spoofing attempts. There are many plugins and tools such as SingleFile that let potential attackers to clone an identical user interface. That interface is a part of the website spoofing process.

⁴² Cofense (2024, January 11). Social media phishing: What you need to know | Cofense. Cofense. <https://cofense.com/knowledge-center/social-media-phishing-what-you-need-to-know/>

⁴³ Evil twin attacks and how to prevent them. (2023, April 19). [www.kaspersky.com. https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks](https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks)

⁴⁴ Wikipedia contributors. (2023d, November 17). Website spoofing. Wikipedia. https://en.wikipedia.org/wiki/Website_spoofing

Elastic Detection

After discussing the phishing methods that are being used from the most threat actors it is time to check whether the Elastic can catch some phishing attempts. Elastic has the detection engine to create and manage rules and view the alerts these rules create. Rules periodically search indices (such as logs-* and filebeat-*) for suspicious source events and create alerts when a rule's conditions are met. When an alert is created, its status is Open.

To help track investigations, an alert's status can be set as Open, Acknowledged, or Closed. That rules are being applied to specific systemic rules such as process creation which is based on Event IDs. As discussed, on the installation chapter, Elastic Security package comes with 1032 predefined rules that can be enabled and used immediately. Also, Elastic Security give the opportunity to the administrators to prepare, configure and run their own queries. On the specific environment with Thunderbird installed as a mailbox only certain rules that catch processes can run and alert the administrators. There are some predefined rules regarding phishing attempts such as *O365 Email Reported by User as Malware or Phish* and *Microsoft 365 User Restricted from Sending Email*. Specifically, a user within the O365 environment flagged an email as potentially malicious or indicative of phishing activity.

The reported email is currently under investigation for potential security threats. The user's proactive reporting is a crucial element of our security measures, as it allows our team to promptly assess and address any potential risks. Our security experts are diligently examining the reported email to identify and mitigate any potential threats to the Elastic network. We appreciate the user's vigilance in helping maintain a secure digital environment and will take all necessary actions to safeguard our systems and data against potential cyber threats.

A Microsoft 365 user is currently restricted from sending emails as part of a security or policy enforcement measure. This restriction may be a result of various factors, including but not limited to suspicious activity, policy violations, or the user's account being flagged for potential risks. By temporarily limiting the user's ability to send emails, our organization aims to mitigate potential security threats and protect sensitive information. The IT security team is actively investigating the issue to determine the cause and ensure that the user's account is secure.

Once the necessary security measures have been taken, the user's email sending capabilities will be reinstated, and appropriate steps will be communicated to the user to prevent any recurrence of the issue. We appreciate the user's understanding and cooperation as we work to maintain a secure and resilient email environment within Microsoft 365.

O365 Email Reported by User as Malware or Phish

The screenshot shows the configuration page for a rule in Elastic SIEM. The page is divided into several sections:

- About:** Describes the rule's purpose: "Detects the occurrence of emails reported as Phishing or Malware by Users. Security Awareness training is essential to stay ahead of scammers and threat actors, as security products can be bypassed, and the user can still receive a malicious message. Educating users to report suspicious messages can help identify gaps in security controls and prevent malware infections and Business Email Compromise attacks." It lists the author as Elastic, severity as Medium, and a risk score of 47. Reference URLs include a Microsoft support article and a link to legitimate files reported by users. MITRE ATT&CK categories include Initial Access (TA0001), Phishing (T1566), Spearphishing Attachment (T1566.001), and Spearphishing Link (T1566.002). The timestamp override is event.ingested, and tags include Domain: Cloud, Data Source: Microsoft 365, and Tactic: Initial Access.
- Definition:** Shows the index patterns as filebeat-* and logs-o365*. The custom query is: `event.dataset:o365.audit and event.provider:SecurityComplianceCenter and event.action:AlertTriggered and rule.name:"Email reported by user as malware or phish"`. The rule type is Query. Related integrations show O365 as not installed. Required fields are event.action, event.dataset, event.provider, and rule.name. The timeline template is None.
- Schedule:** The rule runs every 5m with an additional look-back time of 25m.

Microsoft 365 User Restricted from Sending Email

The screenshot shows the configuration page for a rule in Elastic SIEM. The page is divided into several sections:

- About:** Describes the rule's purpose: "Identifies when a user has been restricted from sending email due to exceeding sending limits of the service policies per the Security Compliance Center." It lists the author as Austin Songer, severity as Medium, and a risk score of 47. Reference URLs include Microsoft documentation on cloud app security anomaly detection and policy template reference. A false positive example is provided: "A user sending emails using personal distribution folders may trigger the event." The license is Elastic License v2. MITRE ATT&CK categories include Initial Access (TA0001) and Valid Accounts (T1078). The timestamp override is event.ingested, and tags include Domain: Cloud, Data Source: Microsoft 365, Use Case: Configuration Audit, and Tactic: Initial Access.
- Definition:** Shows the index patterns as filebeat-* and logs-o365*. The custom query is: `event.dataset:o365.audit and event.provider:SecurityComplianceCenter and event.category:web and event.action:"User restricted from sending email" and event.outcome:success`. The rule type is Query. Related integrations show O365 as not installed. Required fields are event.action, event.category, event.dataset, event.outcome, and event.provider. The timeline template is None.
- Schedule:** The rule runs every 5m with an additional look-back time of 25m.

Elastic has enhanced its security capabilities by incorporating extensive coverage for MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, specifically focusing on phishing techniques. This strategic integration allows Elastic to comprehensively detect and defend against a broad spectrum of phishing attacks, aligning with MITRE's industry-recognized knowledge base⁴⁵. Leveraging advanced analytics and machine learning, Elastic's security solutions provide real-time monitoring and response to phishing attempts within the organization. This proactive approach enables swift identification of malicious activities associated with phishing techniques, contributing to a robust

⁴⁵ Detection rules | Elastic Security Solution [8.12] | Elastic. Elastic.
<https://www.elastic.co/guide/en/security/current/ts-detection-rules.html>

defense posture against cyber threats. By continually updating its defenses based on the latest MITRE ATT&CK insights, Elastic ensures that its users benefit from a dynamic and adaptive security ecosystem in the ever-evolving landscape of phishing attacks.

- Suspicious Explorer Child Process
- Suspicious MS Office Child Process
- Execution of File Written or Modified by Microsoft Office
- Suspicious MS Outlook Child Process
- Suspicious PDF Reader Child Process
- Windows Script Executing PowerShell
- Possible Consent Grant Attack via Azure-Registered Application
- Okta FastPass Phishing Detection
- Potential Process Injection from Malicious Document
- Creation of SettingContent-ms Files
- O365 Email Reported by User as Malware or Phish
- Microsoft 365 Exchange Anti-Phish Rule Modification
- Remote XSL Script Execution via COM
- Potential Remote File Execution via MSIEXEC
- Downloaded Shortcut Files
- File with Suspicious Extension Downloaded
- Microsoft 365 Exchange Safe Link Policy Disabled
- Microsoft 365 Exchange Anti-Phish Policy Deletion
- Downloaded URL Files
- Google Workspace Object Copied from External Drive and Access Granted to Custom Application
- Suspicious HTML File Creation
- Execution of File Written or Modified by PDF Reader
- Suspicious Execution via Microsoft Office Add-Ins
- Suspicious macOS MS Office Child Process
- Windows Script Interpreter Executing Process via WMI
- AWS Execution via System Manager

The security landscape presents a myriad of potential threats, and vigilance is paramount in identifying and mitigating these risks. Instances of suspicious explorer child processes, MS Office child processes, and the execution of files modified by Microsoft Office raise concerns about potential malicious activities. Further, the observation of suspicious child processes in MS Outlook and PDF readers warrants heightened scrutiny.

The detection of Windows scripts executing PowerShell commands and the possibility of a consent grant attack via an Azure-registered application underline the importance of monitoring and securing cloud-based environments. Notably, the Okta FastPass phishing detection capability aids in fortifying defenses against credential compromise attempts. Instances of potential process injection from malicious documents, creation of SettingContent-ms files, and the reported O365 email as malware underscore the need for robust email security measures and continuous monitoring. Any alterations to Microsoft 365 Exchange anti-phish rules or policies, as well as the deletion of such safeguards, pose a serious risk and necessitate immediate investigation and remediation.

The discovery of remote XSL script execution via COM, potential remote file execution via MSIEXEC, and the download of shortcut files and URLs highlight the evolving techniques employed by threat actors. Similarly, the creation of suspicious HTML files and execution of files modified by PDF readers emphasize the importance of securing diverse attack surfaces. The observation of suspicious activity involving Microsoft Office add-ins, macOS MS Office child processes, and Windows script interpreters executing processes via WMI necessitate a comprehensive approach to endpoint security.⁴⁶ Additionally, the execution of AWS commands via System Manager indicates the need for robust cloud security practices.

As organizations navigate the complex threat landscape, constant vigilance, proactive monitoring, and swift response mechanisms are essential to fortify defenses against emerging cyber threats and safeguard sensitive information and systems.

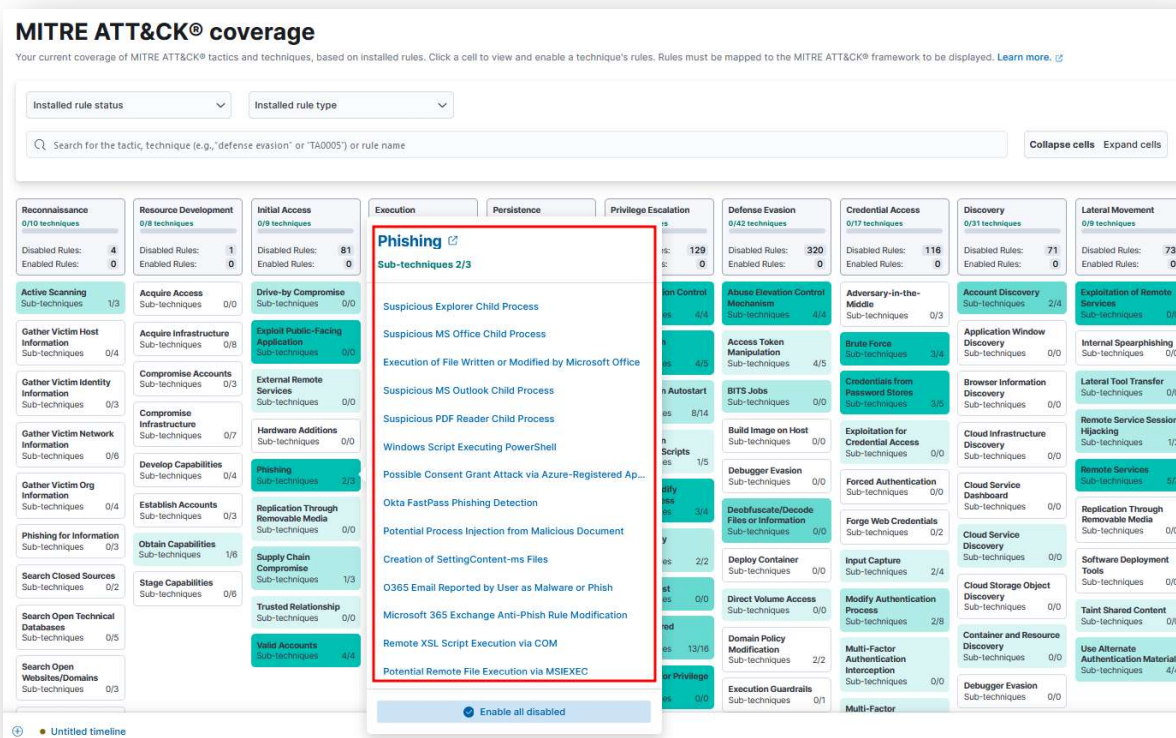


Figure 75 - Elastic MITRE ATT&CK Coverage of Phishing

Every SIEM has its own utilities where it can catch and alert for specific anomalies found within the network or individually in a host. More specifically, Elastic SIEM does not support any methodology on how to detect URL Spoofing or other browser-based detection mechanisms. Elastic Security can detect any exploitable process that can run on the host, alert, and prevent that from happening. Finally, isolation practices are supported.

⁴⁶ Erkailo, T., Ewing, P., Ignatovych, K., Sachidananda, S., & Settle, M. (2024, January 19). What's new in Elastic Security 8.10: Scale your defenses and outpace attackers. Elastic Blog. <https://www.elastic.co/blog/whats-new-elastic-security-8-10-0>

Phishing Rules Experiment with Elastic

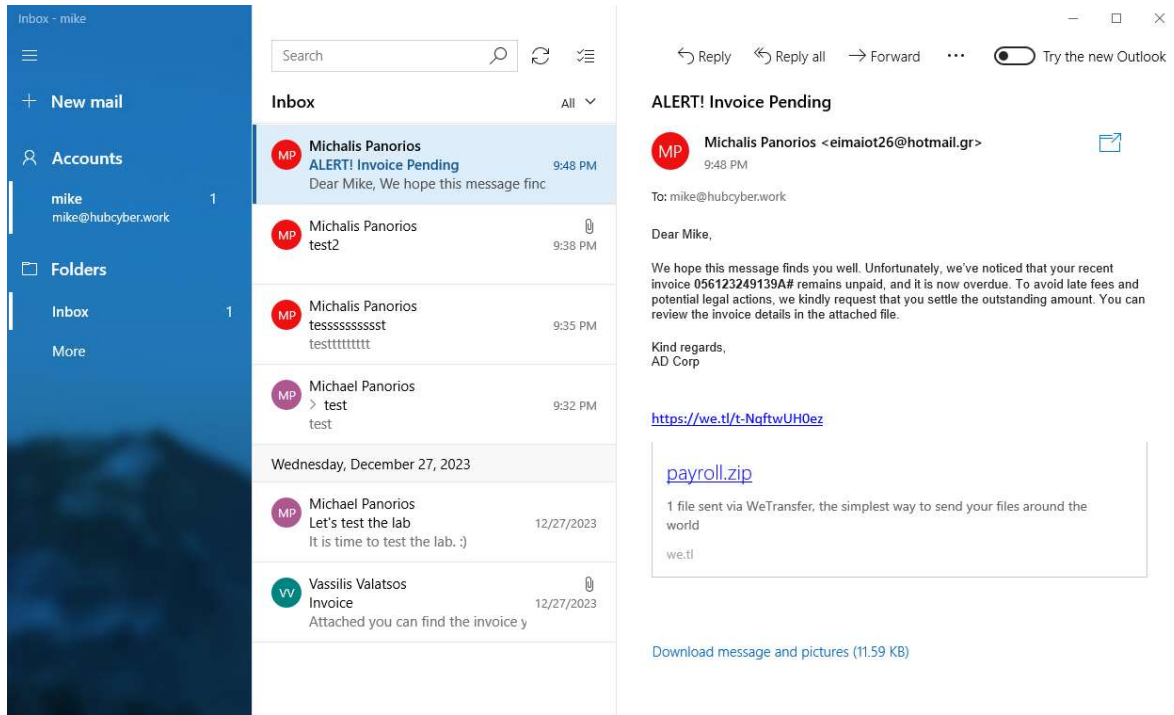


Figure 76 - Outlook phishing example

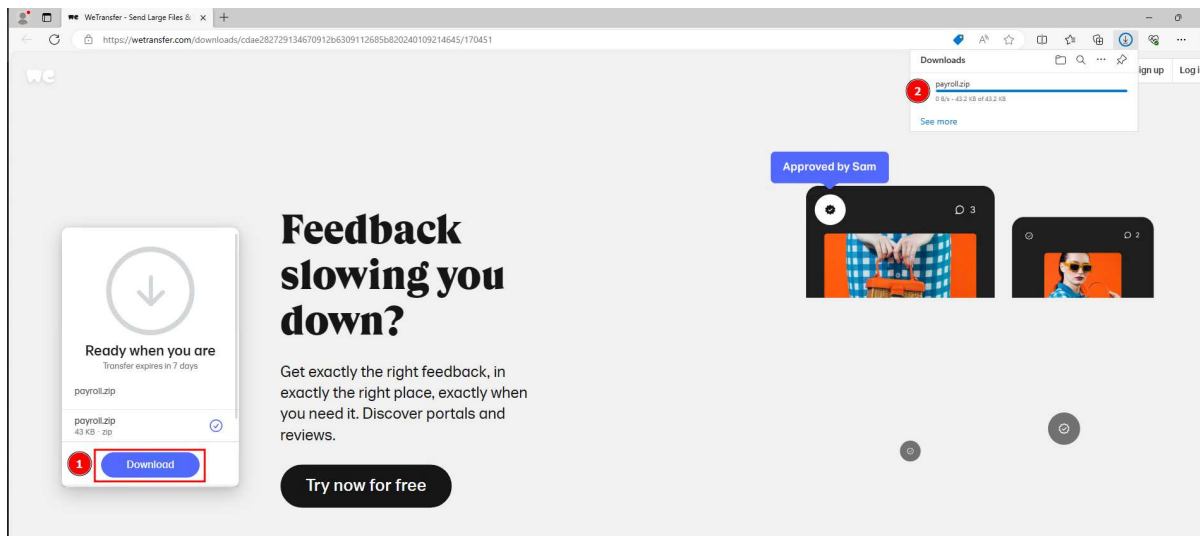


Figure 77 - Public drive phishing example

Potential Process Injection from Malicious Document

About

Identifies a suspicious Windows explorer child process. Explorer.exe can be abused to launch malicious scripts or executables from a trusted parent process.

Author
Elastic

Severity
Medium

Risk score
47

License
Elastic License v2

MITRE ATT&CK™

- Initial Access (TA0001)
 - Phishing (T1566)
 - Spearphishing Attachment (T1566.001)
 - Spearphishing Link (T1566.002)
- Execution (TA0002)
 - Command and Scripting Interpreter (T1059)
 - PowerShell (T1059.001)
 - Windows Command Shell (T1059.003)
 - Visual Basic (T1059.005)
 - System Binary Proxy Execution (T1218)
- Defense Evasion (TA0005)
 - System Binary Proxy Execution (T1218)

Timestamp override
event.ingested

Tags
Domain: Endpoint OS: Windows Use Case: Threat Detection
Tactic: Initial Access Tactic: Defense Evasion Tactic: Execution
Data Source: Elastic Endgame Data Source: Elastic Defend

Definition

Index patterns
logs-endpoint.events* | winlogbeat* | logs-windows* | endgame*

EQL query

```
process where host.os.type == "windows" and event.type == "start" and
{
  process.name : ("cscript.exe", "wscript.exe", "powershell.exe",
  "rundll32.exe", "cmd.exe", "mshta.exe", "regsvr32.exe") or
  process.pe.original_file_name in ("cscript.exe", "wscript.exe",
  "PowerShell.EXE", "RUNDLL32.EXE", "Cmd.Exe", "MSHTA.EXE",
  "REGSVR32.EXE")
} and
/* Explorer started via DCOM */
process.parent.name : "explorer.exe" and process.parent.args :
"-Embedding" and
not process.parent.args :
{
  /* Noisy CLSID.SeparateSingleProcessExplorerHost Explorer COM
  Class IDs */
  "factory{5BDB9510-9434-43C2-8B6C-57852CC8A120}",
  "factory{ceff45ee-c862-41de-aae2-a022c81eda92}"
}
}
```

Rule type
Elastic Defend Installed: enabled

Related integrations
Windows Installed: enabled

Required fields

- event.type
- host.os.type
- process.name
- process.parent.args
- process.parent.name
- process.pe.original_file_name

Timeline template
None

Figure 78 - Potential Process Injection from Malicious Document query

This query is crafted for Windows systems to identify specific processes initiated under certain conditions. It targets processes started with a "start" event on Windows hosts and focuses on executable names, including common command-line interpreters and utilities such as **cscript.exe**, **wscript.exe**, **powershell.exe**, **rundll32.exe**, **cmd.exe**, **mshta.exe**, and **regsvr32.exe**. Additionally, it considers the original file names associated with these processes. The query further refines its search by examining the parent process, ensuring it is "**explorer.exe**" with the argument "**-Embedding**". Finally, it excludes cases where the parent process arguments contain specific COM Class IDs associated with Explorer that are deemed noisy or undesirable, providing a more precise and context-aware analysis of process initiation on Windows systems.⁴⁷

⁴⁷ Potential Process Injection from Malicious Document | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/potential-process-injection-from-malicious-document.html>

Windows Script Executions

About

Identifies child processes of frequently targeted Microsoft Office applications (Word, PowerPoint, Excel) with unusual process arguments and path. This behavior is often observed during exploitation of Office applications or from documents with malicious macros.

Author

Building block

Severity

Risk score

License

MITRE ATT&CK™

- Defense Evasion (TA0005) Process Injection (T1055)
- Privilege Escalation (TA0004) Process Injection (T1055)
- Initial Access (TA0001) Phishing (T1566) Spearphishing Attachment (T1566.001)

Timestamp override

Tags

Domain: Endpoint OS: Windows Use Case: Threat Detection
Tactic: Defense Evasion Tactic: Privilege Escalation Tactic: Initial Access
Rule Type: BBP Data Source: Elastic Defend

Definition

Index patterns

EQL query

```
logs-endpoint.events.*
process where host.os.type == "windows" and event.action == "start" and
process.parent.name : ("excel.exe", "powerpnt.exe", "winword.exe") and
process.args_count == 1 and
process.executable : (
"?:\\Windows\\SysWOW64\\*.exe", "?:\\Windows\\system32\\*.exe"
) and
not process.executable : "?:\\Windows\\System32\\spool\\drivers\\x64\\" and
process.code_signature.trusted == true and not
process.code_signature.subject_name : "Microsoft *" and
not process.executable : (
"?:\\Windows\\Sys*\\Taskmgr.exe",
"?:\\Windows\\Sys*\\ctfmon.exe",
"?:\\Windows\\System32\\notepad.exe")
```

Rule type

Related integrations

Required fields

Timeline template

Event Correlation

Elastic Defend Installed: enabled

- event.action
- host.os.type
- process.args_count
- process.code_signature.subject_name
- process.code_signature.trusted
- process.executable
- process.parent.name

Figure 79 - Windows Script Executions query

The query focuses on processes initiated with a "start" action on Windows hosts. It specifically looks for processes with parent names such as "excel.exe," "powerpnt.exe," or "winword.exe". The target processes should have a single argument (**args_count == 1**) and be executed from locations within the Windows directories (**?:\\Windows\\SysWOW64*.exe** and **?:\\Windows\\system32*.exe**).

Exclusions are applied to filter out certain scenarios. It excludes processes executed from the **"?:\\Windows\\System32\\spool\\drivers\\x64\\"** path unless they are trusted (**process.code_signature.trusted == true**) and not signed by Microsoft (**not process.code_signature.subject_name : "Microsoft *"**). Additionally, it excludes processes with executable paths matching specific patterns related to Task Manager (**Taskmgr.exe**), CTFMon (**ctfmon.exe**), and Notepad (**notepad.exe**) in different Windows system directories.⁴⁸

In summary, the query aims to pinpoint the initiation of specific processes, particularly those associated with Microsoft Office applications, while excluding certain system processes and potential security concerns.

⁴⁸ Windows Script Executing PowerShell | Elastic Security Solution [8.12] | Elastic.
<https://www.elastic.co/guide/en/security/current/windows-script-executing-powershell.html>

Windows Script Executing PowerShell

About

Identifies a PowerShell process launched by either cscript.exe or wscript.exe. Observing Windows scripting processes executing a PowerShell script, may be indicative of malicious activity.

Author
Elastic

Severity
Low

Risk score
21

License
Elastic License v2

MITRE ATT&CK™

- Initial Access (TA0001)
 - Phishing (T1566)
 - Spearphishing Attachment (T1566.001)
- Execution (TA0002)
 - Command and Scripting Interpreter (T11059)
 - PowerShell (T11059.001)
 - Visual Basic (T11059.003)

Timestamp override

Tags

Domain: Endpoint | OS: Windows | Use Case: Threat Detection
Tactic: Initial Access | Tactic: Execution | Resource: Investigation Guide
Data Source: Elastic Endgame | Data Source: Elastic Defend

Definition

Index patterns
wlogbeat-* | logs-endpoint.events.* | logs-windows.* | endgame-*

EQL query

```
process where host.os.type == "windows" and event.type == "start" and process.parent.name : ("cscript.exe", "wscript.exe") and process.name : "powershell.exe"
```

Rule type
Elastic Defend Installed: enabled
Windows Installed: enabled

Related integrations

Required fields

- event.type
- host.os.type
- process.name
- process.parent.name

Timeline template
None

Schedule

Runs every
5m

Additional look-back time
4m

Figure 80 - Windows Script Executing PowerShell query

This EQL query focuses on identifying processes on Windows systems based on specific criteria. It looks for processes with the following characteristics:

- The host operating system should be of type **"windows"**.
- The event type should be a process **start (event.type == "start")**.
- The parent process name should be either **"cscript.exe"** or **"wscript.exe"**.
- The process name itself should be **"powershell.exe"**.

In summary, this query is designed to find instances where PowerShell (powershell.exe) is started, specifically when the parent process is either CScript or WScript. This type of query can be useful for detecting PowerShell execution initiated from script hosts like CScript or WScript, which may be indicative of certain scripting or automation activities on a Windows system.

Suspicious MS Office Child Process

About

Identifies suspicious child processes of frequently targeted Microsoft Office applications (Word, PowerPoint, Excel). These child processes are often launched during exploitation of Office applications or from documents with malicious macros.

Author
Elastic

Severity
Medium

Risk score
47

Reference URLs
<https://www.elastic.co/blog/vulnerability-summary-follina>

License
Elastic License v2

MITRE ATT&CK™

- Initial Access (TA0001)
 - Phishing (T1566)
 - Spearphishing Attachment (T1566.001)
- Execution (TA0002)
 - Command and Scripting Interpreter (T11059)
 - PowerShell (T11059.001)
 - Windows Command Shell (T11059.003)
- Defense Evasion (TA0005)
 - System Binary Proxy Execution (T1218)

Timestamp override

Tags

Domain: Endpoint | OS: Windows | Use Case: Threat Detection
Tactic: Initial Access | Tactic: Defense Evasion | Tactic: Execution
Resources: Investigation Guide | Data Source: Elastic Endgame
Data Source: Elastic Defend

Definition

Index patterns
wlogbeat-* | logs-endpoint.events.* | logs-windows.* | endgame-*

EQL query

```
process where host.os.type == "windows" and event.type == "start" and process.parent.name : ("eghcd32.exe", "excel.exe", "fltr.exe", "msaccess.exe", "mspub.exe", "powerpoint.exe", "winword.exe", "wordbook.exe") and process.name : ("Microsoft.Workflow.Compiler.exe", "arp.exe", "atbroker.exe", "dgnlo.exe", "dsadmin.exe", "icb.exe", "certutil.exe", "cmd.exe", "compg.exe", "control.exe", "cscript.exe", "csisave", "dlnx.exe", "dsgot.exe", "dsquery.exe", "forfiles.exe", "fsutil.exe", "ipconfig.exe", "hostname.exe", "ieexec.exe", "iexpress.exe", "installutil.exe", "ipconfig.exe", "mhta.exe", "mscat.exe", "notepad.exe", "not.exe", "net.exe", "netsh.exe", "notepad.exe", "notepad.exe", "odbcconf.exe", "ping.exe", "powershell.exe", "pskill.exe", "process.exe", "quser.exe", "qwinsta.exe", "rsl.exe", "reg.exe", "regasm.exe", "regsvcs.exe", "regsvr32.exe", "sc.exe", "scintask.exe", "systeminfo.exe", "tasklist.exe", "tracert.exe", "whoami.exe", "wmic.exe", "wscript.exe", "wizard.exe", "explorer.exe", "rundll32.exe", "hh.exe", "msdt.exe")
```

Rule type
Elastic Defend Installed: enabled
Windows Installed: enabled

Related integrations

Required fields

- event.type
- host.os.type
- process.name
- process.parent.name

Timeline template
None

Figure 81 - Suspicious MS Office Child Process query

This query is designed to identify processes on Windows systems that meet specific criteria related to process initiation⁴⁹. Here is a summary:

- The query is focused on processes initiated on Windows hosts (**host.os.type == "windows"**) with a "start" event (**event.type == "start"**).
- The parent process should have one of the specified names, including **"eqnedt32.exe," "excel.exe," "ftldr.exe," "msaccess.exe," "mspub.exe," "powerpnt.exe," "winword.exe,"** and **"outlook.exe."**
- The child process (the one being started) should have a name matching any of the listed executable names. These include a variety of common system utilities and tools, such as **"cmd.exe," "powershell.exe," "regsvr32.exe," "explorer.exe"** and many others.

In essence, this query is tailored to identify instances where specific processes are started on a Windows system, particularly focusing on a predefined set of parent processes and a comprehensive list of allowed child processes. This type of query can be useful for monitoring and detecting the execution of specific utilities or tools on a Windows environment.

Suspicious Explorer Child Process

The screenshot displays the configuration for the 'Suspicious Explorer Child Process' query in the Elastic Security Solution. The interface is split into two main sections: 'About' and 'Definition'.

About Section:

- Author:** Elastic
- Severity:** Medium
- Risk score:** 47
- License:** Elastic License v2
- MITRE ATT&CK:**
 - Initial Access (TA0001)
 - Phishing (T1566)
 - Spearphishing Attachment (T1566.001)
 - Spearphishing Link (T1566.002)
 - Execution (TA0002)
 - Command and Scripting Interpreter (T1059)
 - PowerShell (T1059.001)
 - Windows Command Shell (T1059.003)
 - Visual Basic (T1059.005)
 - Defense Evasion (TA0003)
 - System Binary Proxy Execution (T1218)
- Timestamp override:** event.ingested
- Tags:** Domain: Endpoint, OS: Windows, Use Case: Threat Detection, Tactic: Initial Access, Tactic: Defense Evasion, Tactic: Execution, Data Source: Elastic Ingestions, Data Source: Elastic Defend

Definition Section:

- Index patterns:** log-* endpoint.events-* winlogbeat-* log-* windows-* endgame-*
- EQL query:**

```
process where host.os.type == "windows" and event.type == "start" and
{
  process.name in ("cscript.exe", "wscript.exe", "powershell.exe",
"rundll32.exe", "cmd.exe", "mshta.exe", "regsvr32.exe") or
  process.pe.original_file_name in ("cscript.exe", "wscript.exe",
"PowerShell.EXE", "RUNDLL32.EXE", "Cmd.Exe", "MSHTA.EXE",
"REGSVR32.EXE")
} and
{! Explorer started via DCOM }
process.parent.name == "explorer.exe" and process.parent.args
!-Embedding" and
not process.parent.args:
{
  ! Noisy CLSID_SeparateSingleProcessExplorerHost Explorer COM
Class ID: "{
"Factory,{5BD95610-9434-43C2-886C-57852CC8A120}",
"Factory,{ceff45ee-c862-41de-aae2-a022c81eda92}"
}
```
- Rule type:** Elastic Defend
- Related integrations:** Elastic Defend (Installed: enabled), Windows (Installed: enabled)
- Required fields:** event.type, host.os.type, process.name, process.parent.args, process.parent.name, process.pe.original_file_name
- Timeline template:** None

Figure 82 - Suspicious Explorer Child Process query

This query is designed to filter and identify specific processes on Windows systems. It focuses on processes initiated with a "start" event on Windows hosts. The query targets processes with names like **"cscript.exe," "wscript.exe," "powershell.exe," "rundll32.exe," "cmd.exe," "mshta.exe,"** and **"regsvr32.exe,"** or those with specific original file names. Additionally, it checks if the parent process is **"explorer.exe"** invoked via **DCOM ("Embedding" argument)** and excludes cases where the parent process arguments match certain COM Class IDs (**"{5BD95610-9434-43C2-886C-57852CC8A120}"**) and

⁴⁹ Suspicious MS Office Child Process | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/suspicious-ms-office-child-process.html>

"{ceff45ee-c862-41de-ae2-a022c81eda92}"). This query is tailored for detecting specific process relationships and configurations, often useful in security and monitoring contexts⁵⁰.

Execution of File Written or Modified by Microsoft Office

Figure 83 - Execution of File Written or Modified by Microsoft Office query

This sequence is designed to analyze and correlate events related to the execution of specific executable files on Windows systems. In the first part, it focuses on file events, excluding deletions, where the file extension is ".exe." The target executables are associated with processes like **WINWORD.EXE**, **EXCEL.EXE**, **OUTLOOK.EXE**, **POWERPNT.EXE**, **eqnedt32.exe**, **ftldr.exe**, **MSPUB.EXE**, and **MSACCESS.EXE**. That information is organized by the unique host ID and file path. The second part of the sequence examines process events for Windows systems, specifically looking for process start events. It excludes instances where the process is named "**NewOutlookInstaller.exe**" and is signed by "**Microsoft Corporation**" while being trusted. Results from this part are grouped by the host ID and the executable path of the process. The entire sequence is executed within a maximum span of 2 hours, allowing for the correlation of file and process events over this time limit. Such sequences are valuable for detecting and responding to potential security threats or suspicious activities within a Windows environment⁵¹.

⁵⁰ Raman, D. (2020, July 15). Detecting suspicious child processes using ee-outliers and Elasticsearch. Nviso Labs. <https://blog.nviso.eu/2018/12/21/detecting-suspicious-child-processes-using-ee-outliers-and-elasticsearch/>

⁵¹ Execution of file written or modified by Microsoft Office | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/execution-of-file-written-or-modified-by-microsoft-office.html>

Suspicious MS Outlook Child Process

Identifies suspicious child processes of Microsoft Outlook. These child processes are often associated with spear phishing activity.

Author Elastic

Severity Low

Risk score 21

License Elastic License v2

MITRE ATT&CK™

- Initial Access (TA0001) [🔗](#)
 - Phishing (T1566)
 - Spearphishing Attachment (T1566.001)
- Execution (TA0002) [🔗](#)
 - Command and Scripting Interpreter (T1059)
 - PowerShell (T1059.001)
 - Windows Command Shell (T1059.003)
- Defense Evasion (TA0005) [🔗](#)
 - System Binary Proxy Execution (T1218)

Timestamp override event_ingested

Index patterns winlogbeat-* logs-endpoint.events.* logs-windows.* endgame-*

EQL query

```
process where host.os.type == "windows" and event.type == "start" and process.parent.name : "outlook.exe" and process.name : ("Microsoft.Workflow.Compiler.exe", "arp.exe", "atbroker.exe", "bginfo.exe", "bitsadmin.exe", "cdb.exe", "certutil.exe", "cmd.exe", "cmstp.exe", "cscript.exe", "csi.exe", "dnx.exe", "dsget.exe", "dsquery.exe", "forfiles.exe", "fsi.exe", "ftp.exe", "gpresult.exe", "hostname.exe", "ieexec.exe", "iexpress.exe", "installutil.exe", "ipconfig.exe", "mshta.exe", "msxsl.exe", "nbtstat.exe", "net.exe", "net1.exe", "netsh.exe", "netstat.exe", "nntest.exe", "odbcconf.exe", "ping.exe", "powershell.exe", "pwsh.exe", "qprocess.exe", "quser.exe", "qwinsta.exe", "rcsi.exe", "reg.exe", "regasm.exe", "regsvcs.exe", "regsvr32.exe", "sc.exe", "schtasks.exe", "systeminfo.exe", "tasklist.exe", "tracert.exe", "whoami.exe", "wmic.exe", "wscript.exe", "xwizard.exe")
```

Rule type Event Correlation

Figure 84 - Suspicious MS Outlook Child Process query

This EQL statement is designed to identify specific processes on Windows systems that are initiated with a "start" event. The query narrows down the focus by specifying that the parent process must be "outlook.exe." The query then lists a set of allowed child processes that can be started by Outlook, covering a range of commonly used Windows utilities and executables such as "cmd.exe," "powershell.exe," "regsvr32.exe," and others⁵². This type of query can be valuable for monitoring and analyzing the execution of specific processes associated with Outlook, which may be indicative of certain workflow patterns or potential security concerns within a Windows environment.

⁵² Suspicious MS Outlook Child Process | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/suspicious-ms-outlook-child-process.html>

Suspicious PDF Reader Child Process

About Details Investigation guide Setup guide

Identifies suspicious child processes of PDF reader applications. These child processes are often launched via exploitation of PDF applications or social engineering.

Author Elastic

Severity Low

Risk score 21

License Elastic License v2

MITRE ATT&CK™

- Execution (TA0002) [Exploitation for Client Execution \(T1203\)](#)
- Initial Access (TA0001) [Phishing \(T1566\)](#)
 - Spearphishing Attachment (T1566.001)

Timestamp override event.ingested

Tags

Domain: Endpoint OS: Windows

Use Case: Threat Detection Tactic: Execution

Tactic: Initial Access Resources: Investigation Guide

Data Source: Elastic Endgame Data Source: Elastic Defend

Definition

Index patterns winlogbeat-* logs-endpoint.events.* logs-windows.* endgame-*

EQL query

```
process where host.os.type == "windows" and event.type == "start" and process.parent.name : ("AcroRd32.exe", "Acrobat.exe", "FoxitPhantomPDF.exe", "FoxitReader.exe") and process.name : ("arp.exe", "dsquery.exe", "dsget.exe", "gpresult.exe", "hostname.exe", "ipconfig.exe", "nbtstat.exe", "net.exe", "net1.exe", "nets.exe", "netstat.exe", "nittest.exe", "ping.exe", "qprocess.exe", "quser.exe", "qwinsta.exe", "reg.exe", "sc.exe", "systeminfo.exe", "tasklist.exe", "tracert.exe", "whoami.exe", "bginfo.exe", "cdb.exe", "cmstp.exe", "csi.exe", "dnh.exe", "fsi.exe", "leexec.exe", "lexpress.exe", "installutil.exe", "Microsoft.Workflow.Compiler.exe", "msbuild.exe", "mshta.exe", "msxsl.exe", "odbcconf.exe", "rcsl.exe", "regsvr32.exe", "xwizard.exe", "atbroker.exe", "forfiles.exe", "schtasks.exe", "regasm.exe", "regsvcs.exe", "cmd.exe", "cscript.exe", "powershell.exe", "pwsh.exe", "wmic.exe", "wscript.exe", "bitsadmin.exe", "certutil.exe", "ftp.exe")
```

Figure 85 - Suspicious PDF Reader Child Process query

This EQL query is structured for identifying specific processes initiated with a **"start"** event on Windows systems. It focuses on processes whose parent process name belongs to a predefined set, which includes **"AcroRd32.exe," "Acrobat.exe," "FoxitPhantomPDF.exe,"** and **"FoxitReader.exe."** The query further narrows down the results by specifying a list of allowed child processes, encompassing various common Windows utilities and executables such as **"cmd.exe," "powershell.exe," "regsvr32.exe,"** and others. This type of query is useful for monitoring and analyzing the execution of specific processes associated with PDF reader applications, providing insights into potential workflow patterns or security considerations within a Windows environment⁵³.

⁵³ Suspicious PDF Reader Child Process | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/suspicious-pdf-reader-child-process.html>

Creation of SettingContent-ms Files

The screenshot shows the configuration page for the rule "Creation of SettingContent-ms Files". The "About" section on the left provides details about the rule's author, severity (Low), risk score (21), and reference URLs. The "Definition" section on the right shows the EQL query: `logs-endpoint.events.* |> file where host.os.type == "windows" and event.type == "creation" and file.extension : "settingcontent-ms"`. The "MITRE ATT&CK" section lists associated attack techniques: Execution (TA0002), User Execution (T1204), Malicious File (T1204.002), Initial Access (TA0001), Phishing (T1566), and Spearphishing Attachment (T1566.001).

Figure 86 - Creation of SettingContent-ms Files query

This EQL query is designed to identify files on Windows systems that have been created with a "creation" event and have the extension "settingcontent-ms".⁵⁴ The query specifically focuses on files with this extension, which is associated with setting content files on Windows. This type of query can be useful for monitoring and analyzing the creation of specific file types related to system settings or configurations, providing insights into changes made to these settings on Windows hosts.

O365 Email Reported by User as Malware or Phish

The screenshot shows the configuration page for the rule "O365 Email Reported by User as Malware or Phishing". The "About" section on the left describes the rule's purpose: detecting emails reported as Phishing or Malware by Users. The "Definition" section on the right shows the Custom query: `event.dataset:o365.audit and event.provider:SecurityComplianceCenter and event.action:AlertTriggered and rule.name:"Email reported by user as malware or phish"`. The "MITRE ATT&CK" section lists associated attack techniques: Initial Access (TA0001), Phishing (T1566), Spearphishing Attachment (T1566.001), and Spearphishing Link (T1566.002).

Figure 87 - O365 Email Reported by User as Malware or Phishing query

This rule detects the occurrence of emails reported as Phishing or Malware by Users. Security Awareness training is crucial for staying ahead of scammers and threat actors because even the most robust security products can be bypassed, and users may still encounter malicious messages. Educating users to report suspicious messages can help identify gaps in security controls and prevent malware

⁵⁴ Creation of SettingContent-MS Files | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/creation-of-settingcontent-ms-files.html>

infections and Business Email Compromise attacks. This EQL query is crafted to search for events in the "o365.audit" dataset where the provider is "SecurityComplianceCenter", the action is "AlertTriggered" and the specific rule name is "Email reported by user as malware or phish." This query is focused on identifying security-related events within Office 365 auditing data, specifically those triggered by alerts associated with user-reported emails identified as potential malware or phishing threats. It helps in monitoring and responding to security incidents within the Office 365 environment⁵⁵.

Microsoft 365 Exchange Anti-Phish Rule Modification

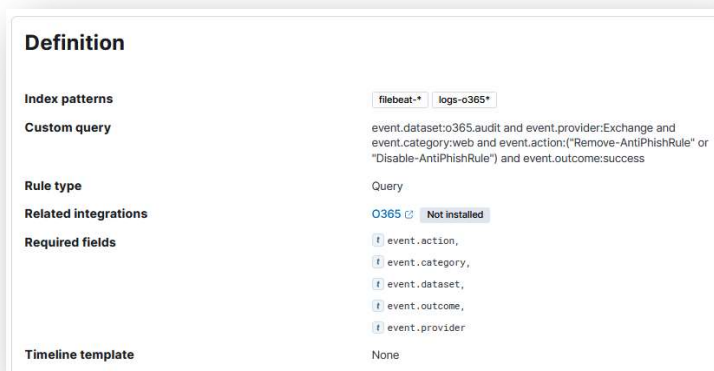


Figure 88 - Microsoft 365 Exchange Anti-Phish Rule Modification query

This rule identifies the modification of an anti-phishing rule in Microsoft 365. By default, Microsoft 365 includes built-in features that help protect users from phishing attacks. Anti-phishing rules increase this protection by refining settings to better detect and prevent attacks. This EQL statement is designed to query events within the "o365.audit" dataset related to Exchange in the Office 365 environment. The conditions specified include events categorized as "web," with actions either being "Remove-AntiPhishRule" or "Disable-AntiPhishRule" and having a successful outcome. This query is tailored to identify successful attempts to remove or disable anti-phishing rules in the Office 365 Exchange environment⁵⁶. Monitoring such events is crucial for maintaining the security of email systems and responding to any changes made to anti-phishing configurations.

⁵⁵ Robmazz. (2023, July 21). Microsoft 365 alert policies. Microsoft Learn. <https://learn.microsoft.com/en-us/purview/alert-policies>

⁵⁶ Microsoft 365 Exchange Anti-Phish Rule Modification | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/microsoft-365-exchange-anti-phish-rule-modification.html>

Remote XSL Script Execution via COM

The screenshot displays the 'Definition' page for a rule in the Elastic Security Solution. The page is divided into several sections:

- Index patterns:** logs-endpoint.events.*
- EQL query:**

```
sequence with maxspan=1m
[library where host.os.type == "windows" and dll.name : "msxml3.dll" and
process.name : ("winword.exe", "excel.exe", "powerpnt.exe", "mspub.exe")]
by process.entity_id
[process where host.os.type == "windows" and event.action == "start" and
process.parent.name : ("winword.exe", "excel.exe", "powerpnt.exe",
"mspub.exe") and
not process.executable :
("?:\\Windows\\System32\\WerFault.exe",
"?:\\Windows\\SysWow64\\WerFault.exe",
"?:\\Windows\\splwow64.exe",
"?:\\Windows\\System32\\conhost.exe",
"?:\\Program Files\\*.exe",
"?:\\Program Files (x86)\\*.exe")] by process.parent.entity_id
```
- Rule type:** Event Correlation
- Related integrations:** Elastic Defend Installed, enabled
- Required fields:**
 - dll.name,
 - event.action,
 - host.os.type,
 - process.entity_id,
 - process.executable,
 - process.name,
 - process.parent.entity_id,
 - process.parent.name
- Timeline template:** None

Figure 89 - Remote XSL Script Execution via COM query

This EQL query is designed to correlate events related to the **"msxml3.dll"** library on Windows systems within a one-minute time. In the first part, it focuses on library events where the **"msxml3.dll"** is loaded by processes such as WinWord, Excel, PowerPoint, and Publisher, organizing the results by the unique entity ID of the associated process. The second part concentrates on process start events where specific processes are launched, including WinWord, Excel, PowerPoint, and Publisher. The sequence excludes certain executables commonly associated with error reporting, console host, and files within specific directories like **"Program Files"** and **"Program Files (x86)"**. In essence, this sequence is useful for identifying instances where the **"msxml3.dll"** library is accessed by specific processes and analyzing the associated process start events, excluding certain common system executables. This type of sequence can be valuable for detecting potential misuse or irregularities in the usage of the specified library within a short time span. Results are grouped by the unique entity ID of the parent process. Overall, this sequence is valuable for detecting and analyzing instances of the **"msxml3.dll"** library being accessed within a short time span by specific processes, aiding in the identification of potential anomalies or misuse in the system⁵⁷.

⁵⁷ Remote XSL script Execution via COM | Elastic Security Solution [8.12] | Elastic. (n.d.-b). Elastic. <https://www.elastic.co/guide/en/security/8.12/remote-xsl-script-execution-via-com.html>

Potential Remote File Execution via MSIEXEC

Definition

Index patterns

EQL query

```
logs-endpoint.events.*
sequence with maxspan=1m
[process where host.os.type == "windows" and event.action == "start" and
 process.name : "msiexec.exe" and process.args : "/V" ] by process.entity_id
[network where host.os.type == "windows" and process.name : "msiexec.exe" and
 event.action == "connection_attempted" ] by process.entity_id
[process where host.os.type == "windows" and event.action == "start" and
 process.parent.name : "msiexec.exe" and user.id : ("S-1-5-21-*", "S-1-5-12-1-*") and
 not process.executable : ("?:\\Windows\\SysWOW64\\msiexec.exe",
 "?:\\Windows\\System32\\msiexec.exe",
 "?:\\Windows\\System32\\srtasks.exe",
 "?:\\Windows\\SysWOW64\\srtasks.exe",
 "?:\\Windows\\System32\\taskkill.exe",
 "?:\\Windows\\Installer\\MSI*.tmp",
 "?:\\Program Files\\*.exe",
 "?:\\Program Files (x86)\\*.exe",
 "?:\\Windows\\System32\\ie4uinit.exe",
 "?:\\Windows\\SysWOW64\\ie4uinit.exe",
 "?:\\Windows\\System32\\sc.exe",
 "?:\\Windows\\system32\\wbem\\mofcomp.exe",
 "?:\\Windows\\twain_32\\fjscan32\\SOP\\crtmprc.exe",
 "?:\\Windows\\SysWOW64\\taskkill.exe",
 "?:\\Windows\\SysWOW64\\schtasks.exe",
 "?:\\Windows\\system32\\schtasks.exe",
 "?:\\Windows\\System32\\sdbinst.exe") and
 not (process.code_signature.subject_name == "Citrix Systems, Inc." and
 process.code_signature.trusted == true) and
 not (process.name : ("regsvr32.exe", "powershell.exe", "rundll32.exe", "wscript.exe") and
 process.Ext.token.integrity_level_name == "high" and
 process.args : ("?:\\Program Files\\*", "?:\\Program Files (x86)\\(*)") and
 not (process.executable : ("?:\\Program Files\\*.exe", "?:\\Program Files (x86)\\*.exe") and
 process.code_signature.trusted == true) and
 not (process.name : "rundll32.exe" and process.args : "printui.dll,PrintUIEntry")
 ] by process.parent.entity_id
```

Figure 90 - Potential Remote File Execution via MSIEXEC query

This query is designed to scrutinize and correlate events related to the execution of the **"msiexec.exe"** process on Windows systems, focusing on a one-minute period. In the first part, it identifies instances where **"msiexec.exe"** is initiated with the **"/V"** argument, organizing the results by the unique entity ID of the process. The second part centers around network events where **"msiexec.exe"** attempts a connection, again grouping the results by the associated process entity ID. The final part investigates child processes of **"msiexec.exe"** with specific conditions, excluding certain executables commonly associated with system tasks, Citrix Systems, Inc. processes, and high-integrity level token processes. Additionally, it filters out processes with specific code signatures, names, arguments, and trusted execution, providing a comprehensive analysis of child processes spawned by **"msiexec.exe"** within the specified time limit. This sequence is valuable for detecting and assessing potential anomalies or malicious activities related to MSI installer executions on Windows systems⁵⁸.

⁵⁸ Potential Remote file execution via MSIEXEC | Elastic Security Solution [8.12] Elastic.
<https://www.elastic.co/guide/en/security/current/potential-remote-file-execution-via-msiexec.html>

Downloaded Shortcut Files

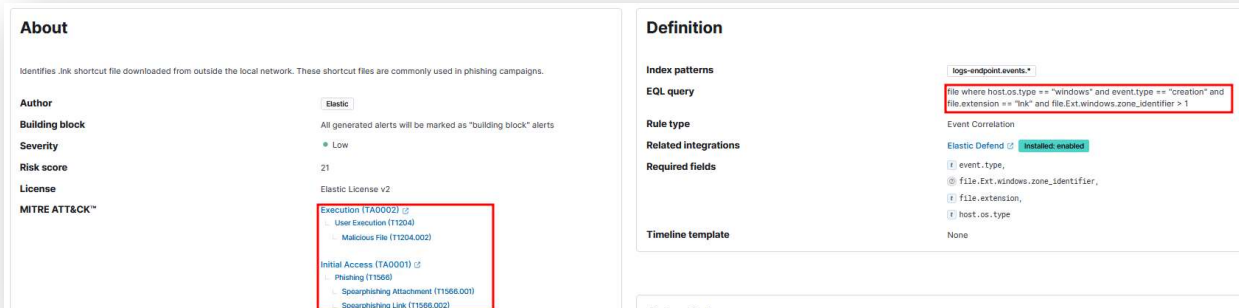


Figure 91 - Downloaded Shortcut Files query

This query is tailored to identify files on Windows systems that have been created with a **"creation"** event, possess the file extension **"Ink"** (shortcut), and have a Windows Zone Identifier greater than 1. The Windows Zone Identifier is a security feature used to determine the security zone of the file. A Zone Identifier greater than 1 typically indicates that the file originated from the internet or another potentially untrusted source. This query helps in pinpointing the creation of shortcut files with elevated security implications, enabling the detection of potential security risks or suspicious activities related to downloaded or external files on Windows hosts⁵⁹.

File with Suspicious Extension Downloaded

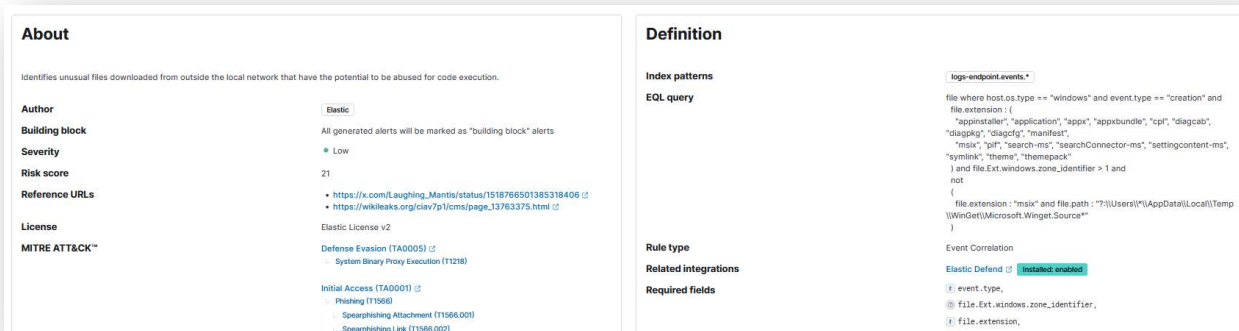


Figure 92 - File with Suspicious Extension Downloaded query

This EQL query is designed to identify specific files on Windows systems that have been created with a **"creation"** event. The query focuses on files with various extensions, including **"appinstaller," "application," "appx," "appxbundle," "cpl," "diagcab," "diagpkg," "diagcfg," "manifest," "msix," "pif," "search-ms," "searchConnector-ms," "settingcontent-ms," "symlink," "theme,"** and **"themepack"**. The additional condition checks for a Windows Zone Identifier greater than 1, indicating potential external or untrusted sources. To refine the results, the query excludes files with the extension **"msix"** located in

⁵⁹ Downloaded Shortcut Files | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/downloaded-shortcut-files.html>

specific paths within the user's temporary directory. This query is useful for detecting the creation of specific file types associated with various Windows functionalities, helping to monitor and identify potential security risks or suspicious activities on Windows hosts⁶⁰.

Microsoft 365 Exchange Safe Link Policy Disabled

Figure 93 - Microsoft 365 Exchange Safe Link Policy Disabled query

This query is crafted to search for events within the "o365.audit" dataset where the provider is "Exchange" the category is "web," the action is "Disable-SafeLinksRule" and the outcome is "success." Specifically, this query focuses on successful attempts to disable Safe Links rules within the Exchange environment, providing visibility into changes made to Safe Links configurations. Monitoring such events is crucial for maintaining the security of email systems and responding to any modifications in the Safe Links protection settings in the Office 365 environment⁶¹.

Microsoft 365 Exchange Anti-Phish Policy Deletion

Figure 94 - Microsoft 365 Exchange Anti-Phish Policy Deletion query

This query is formulated to search for events within the "o365.audit" dataset where the provider is "Exchange" the category is "web," the action is "Remove-AntiPhishPolicy" and the outcome is

⁶⁰ File with Suspicious Extension Downloaded | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/file-with-suspicious-extension-downloaded.html>

⁶¹ Microsoft 365 Exchange Safe Link Policy Disabled | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/microsoft-365-exchange-safe-link-policy-disabled.html>

"success." The query specifically targets successful attempts to remove Anti-Phishing policies within the Exchange environment. Monitoring such events is crucial for maintaining the security posture of email systems and responding to any changes made to Anti-Phishing configurations in the Office 365 environment.⁶²

Downloaded URL Files

About

Identifies .url shortcut files downloaded from outside the local network. These shortcut files are commonly used in phishing campaigns.

Author
Elastic

Building block
All generated alerts will be marked as "building block" alerts

Severity
Low

Risk score
21

License
Elastic License v2

MITRE ATT&CK™

- Execution (TA0002)
 - User Execution (T1204)
- Initial Access (TA0001)
 - Phishing (T1568)
 - Spearphishing Attachment (T1566.001)
 - Spearphishing Link (T1566.002)

Definition

Index patterns
logs-endpointEvents*

EQL query

```
file where host.os.type == "windows" and event.type == "creation" and file.extension == ".url" and file.Ext.windows_zone_identifier > 1 and not process.name : "explorer.exe"
```

Rule type
Event Correlation

Related integrations
Elastic Defend Installed: enabled

Required fields

- event.type
- file.Ext.windows_zone_identifier
- file.extension
- host.os.type
- process.name

Timeline template
None

Figure 95 - Downloaded URL Files query

This EQL query is designed to identify files on Windows systems that have been created with a **"creation"** event, have the file extension **"url"**, possess a Windows Zone Identifier greater than 1 (indicating potential external or untrusted sources), and were not created by the **"explorer.exe"** process. The query is focused on detecting the creation of URL files by processes other than Windows Explorer. This can be useful for monitoring and identifying potentially suspicious or malicious activities related to URL files on Windows hosts, particularly those not initiated by the system's native file explorer process.

⁶² Microsoft 365 Exchange Anti-Phish Policy Deletion | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/microsoft-365-exchange-anti-phish-policy-deletion.html>

Google Workspace Object Copied from External Drive and Access Granted to Custom Application

The screenshot displays the Elastic SIEM interface for a rule titled "Google Workspace Object Copied from External Drive and Access Granted to Custom Application".

About: This section describes the rule's purpose: detecting when a user copies a Google spreadsheet, form, document, or script from an external drive. It notes that sequence logic has been added to detect when a user grants a custom Google application permission via OAuth shortly after. An adversary may send a phishing email to the victim with a Drive object link where "copy" is included in the URL, thus copying the object to the victim's drive. If a container-bound script exists within the object, execution will require permission access via OAuth in which the user has to accept.

Author: Elastic

Severity: Medium

Risk score: 47

Reference URLs:

- <https://www.elastic.co/security-labs/google-workspace-attack-surface-part-one>
- <https://developers.google.com/apps-script/guides/bound>
- https://support.google.com/a/users/answer/13004165#share_make_a_copy_links

False positive examples:

- Google Workspace users typically share Drive resources with a shareable link where parameters are edited to indicate when it is viewable or editable by the intended recipient. It is uncommon for a user in an organization to manually copy a Drive object from an external drive to their corporate drive. This may happen where users find a useful spreadsheet in a public drive, for example, and replicate it to their Drive. It is uncommon for the copied object to execute a container-bound script either unless the user was intentionally aware, suggesting the object uses container-bound scripts to accomplish a legitimate task.

License: Elastic License v2

MITRE ATT&CK: Initial Access (TA0001) Phishing (T1566) Spearphishing Link (T1586.002)

Definition:

Index patterns: filebeat-* | logs-google_workspace*

EQL query:

```
sequence by source.user.email with maxspan=3m
[!file where event.dataset == "google_workspace.drive" and event.action == "copy" and

/* Should only match if the object lives in a Drive that is external to the user's GWS organization */
google_workspace.drive.owner_is_team_drive == "false" and
google_workspace.drive.copy_type == "external" and

/* Google Script, Forms, Sheets and Document can have container-bound scripts */
google_workspace.drive.file_type: ("script", "form", "spreadsheet", "document")]

[any where event.dataset == "google_workspace.token" and event.action == "authorize" and

/* Ensures application ID references custom app in Google Workspace and not GCP */
google_workspace.token.client_id: ["apps.googleusercontent.com"]]

Event Correlation

Google_workspace [Not installed]

[] event.action,
[] event.dataset,
[] google_workspace.drive.copy_type,
[] google_workspace.drive.file_type,
[] google_workspace.drive.owner_is_team_drive,
```

Figure 96 - Google Workspace Object Copied from External Drive and Access Granted to Custom Application query

This EQL sequence is constructed to analyze events related to file copying in Google Workspace Drive, specifically focusing on instances where files of certain types are copied externally and potentially involve container-bound scripts. The sequence is organized by the user's email address (source.user.email) and has a maximum span of 3 minutes (maxspan=3m)⁶³.

File Copy Events: This part focuses on events in the Google Workspace Drive dataset where file copying actions are detected. Specifically, it looks for copies of files that are external to the user's Google Workspace organization, with a file type matching "script," "form," "spreadsheet," or "document."

Authorization Token Events: The second part of the sequence involves events in the Google Workspace Token dataset where authorization actions are taken. The condition ensures that the client ID referenced in the token corresponds to a custom app within Google Workspace, rather than a generic Google Cloud Platform (GCP) app.

Overall, this sequence is valuable for identifying and analyzing file copying events involving specific file types, with a focus on external copies and potential container-bound scripts. The grouping by the user's email address allows for a user-centric view of these events within the specified time span.

⁶³ Google Workspace Object Copied from External Drive and Access Granted to Custom Application | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/google-workspace-object-copied-from-external-drive-and-access-granted-to-custom-application.html>

Suspicious HTML File Creation

About

Identifies the execution of a browser process to open an HTML file with high entropy and size. Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign HTML files.

Author
Elastic

Severity
Medium

Risk score
47

License
Elastic License v2

MITRE ATT&CK™

- Initial Access (TA0001)
 - Phishing (T1566)
 - Spearpishing Attachment (T1566.001)
 - Spearpishing Link (T1566.002)
- Defense Evasion (TA0005)
 - Deflected File or Internet (T1027)
 - HTML Smuggling (T1027.008)

Tags

Domain: Endpoint OS: Windows Use Case: Threat Detection
Tactic: Initial Access Data Source: Elastic Defend

Definition

Index patterns
EQL query

```
logsi-endpoint.events.*
sequence by user.id with maxspan=5m
[file where host.os.type == "windows" and event.action in ("creation", "rename") and
file.extension in ("htm", "html") and
file.path : ("?!(Users!(Downloads!(*)
?(Users!(Content.Outlook!(*)
?(Users!(AppData!(Local!(Temp!(Temp?_*
?(Users!(AppData!(Local!(Temp!(?z*
?(Users!(AppData!(Local!(Temp!(?a$*)) and
((file.entropy >= 5 and file.size >= 150000) or file.size >= 1000000))
(process where host.os.type == "windows" and event.action == "start" and
{
(process.name in ("chrome.exe", "msedge.exe", "brave.exe", "whale.exe",
"browser.exe", "dragon.exe", "vivaldi.exe", "opera.exe")
and process.args == "--single-argument") or
(process.name == "explorer.exe" and process.args_count >= 2) or
(process.name in ("firefox.exe", "waterfox.exe") and process.args ==
"-url")
}
) and process.args : ("?(Users!(Downloads!(?htm*
?(Users!(Content.Outlook!(?htm*
?(Users!(AppData!(Local!(Temp!(Temp?_*htm*
?(Users!(AppData!(Local!(Temp!(?z*htm*
?(Users!(AppData!(Local!(Temp!(?a$*htm*))]
```

Figure 97 - Suspicious HTML File Creation query

This EQL query is tailored to investigate and correlate events related to the creation or renaming of HTML files on Windows systems within a maximum span of 5 minutes. The sequence is organized by user ID and comprises two main components. Firstly, it identifies file events where HTML files are created or renamed, considering specific paths such as Downloads, Outlook content, and temporary directories. Additionally, the criteria include entropy and size constraints to filter for files meeting certain characteristics. The second part of the sequence focuses on process start events, particularly those involving popular browsers (Chrome, Edge, Brave, Whale, etc.), Internet Explorer, and Firefox derivatives. The processes are filtered based on specific arguments indicating the opening of HTML files from predefined paths. This comprehensive approach allows for the detection of user-centric activities related to HTML files and associated browser interactions, providing insights into potential user behavior and usage patterns within the specified time⁶⁴.

Execution of File Written or Modified by PDF Reader

About

Identifies a suspicious file that was written by a PDF reader application and subsequently executed. These processes are often launched via exploitation of PDF applications.

Author
Elastic

Severity
High

Risk score
73

License
Elastic License v2

MITRE ATT&CK™

- Execution (TA0002)
 - Phishing (T1566)
 - Spearpishing Attachment (T1566.001)
 - Spearpishing Link (T1566.002)

Definition

Index patterns
EQL query

```
logsi-endpoint.events.* | winlogsec.* | logsi-windows.* | endgame.*
sequence with maxspan=2h
[file where host.os.type == "windows" and event.type in ("deletion" and
file.extension : ".exe" and
(process.name : "AcroR32.exe" or
process.name : "rdrcef.exe" or
process.name : "FoxitPhantomPDF.exe" or
process.name : "FoxitReader.exe" and
not (file.name : "FoxitPhantomPDF.exe" or
file.name : "FoxitPhantomPDF.Updater.exe" or
file.name : "FoxitReader.exe" or
file.name : "FoxitReader.Updater.exe" or
file.name : "AcroR32.exe" or
file.name : "rdrcef.exe")
) by host.id, file.path
(process where host.os.type == "windows" and event.type == "start" by
host.id, process.executable]
```

Figure 98 - Execution of File Written or Modified by PDF Reader query

This query is designed to examine and correlate events related to the execution of certain executable files on Windows systems within a maximum span of 2 hours (maxspan=2h). The sequence is organized by host ID and comprises two main components:

⁶⁴ Suspicious HTML File Creation | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic.
<https://www.elastic.co/guide/en/security/current/prebuilt-rule-8-2-1-suspicious-html-file-creation.html>

- **File Events:** This section focuses on file events where executable files with specific extensions are involved. The criteria include the executable names of Acrobat Reader, Foxit PhantomPDF, and Foxit Reader, while excluding specific updater-related file names associated with these applications. The results are organized by host ID and file path.
- **Process Start Events:** The second part of the sequence concentrates on process start events on Windows systems, capturing details such as the executable involved. The results are grouped by host ID and the executable path of the launched process.

In essence, this sequence is valuable for identifying instances of specific executable files being executed on Windows hosts, offering insights into potential software usage patterns or security-related events within the specified period⁶⁵.

Suspicious Execution via Microsoft Office Add-Ins

This EQL statement focuses on identifying specific processes on Windows systems initiated through a "start" event. The criteria are as follows:

```
process where
  host.os.type == "windows" and event.type == "start" and
  process.name : ("WINWORD.EXE", "EXCEL.EXE", "POWERPNT.EXE", "MSACCESS.EXE",
"VSTOInstaller.exe") and
  process.args regex~ "".+\.(\w{1}|ppa|ppam|xla|xlam|vsto)"" and
  /* Office Add-in from suspicious paths */
  (process.args :
    ("?:(Users|\\Temp|7z*",
    "?:(Users|\\Temp|Rar$*",
    "?:(Users|\\Temp|Temp2_+",
    "?:(Users|\\Temp|BNZ_+",
    "?:(Users|\\Downloads|*",
    "?:(Users|\\AppData|Roaming|)",
    "?:(Users|Public|*",
    "?:(ProgramData|*",
    "?:(Windows|Temp|*",
    "\\Device|*",
    "http*") or
  process.parent.name : ("explorer.exe", "OpenWith.exe") or
  /* Office Add-in from suspicious parent */
  process.parent.name : ("cmd.exe", "powershell.exe") and
  /* False Positives */
  not (process.args : ".vsto" and
  process.parent.executable :
    ("?:(Program Files|Logitech|LogiOptions|PluginInstallerUtility*.exe",
    "?:(ProgramData|Logishrd|LogiOptions|Plugins|VSTO
\\*|VSTOInstaller.exe",
    "?:(Program Files|Logitech|LogiOptions|PluginInstallerUtility.exe",
    "?:(Program Files|LogiOptionsPlus|PluginInstallerUtility*.exe",
    "?:(ProgramData|Logishrd|LogiOptionsPlus|Plugins|VSTO
\\*|VSTOInstaller.exe",
    "?:(Program Files|Common Files|microsoft shared|VSTO
\\*|VSTOInstaller.exe") and
  not (process.args : "/Uninstall" and process.name : "VSTOInstaller.exe") and
  not (process.parent.name : "rundll32.exe" and
  process.parent.args : "?:(WINDOWS|Installer
\\MSI*.tmp.zzzzInvokeManagedCustomActionOutOfProc)" and
  not (process.name : "VSTOInstaller.exe" and process.args : "https://dl.getsidekick.com
/outlook/vsto/Sidekick.vsto")
```

Figure 99 - Suspicious Execution via Microsoft Office Add-Ins query

- The operating system should be Windows.
- The event type should be "start."
- The process name should match one of the following: "WINWORD.EXE," "EXCEL.EXE," "POWERPNT.EXE," "MSACCESS.EXE," or "VSTOInstaller.exe."
- The process arguments should match a regular expression pattern indicating files with extensions "wll," "xll," "ppa," "ppam," "xla," "xlam," or "vsto."
- The process should originate from suspicious paths, including temporary directories, user downloads, roaming folders, public folders, program data, Windows temporary directory, device paths, or those starting with "http*."
- The parent process should be either "explorer.exe" or "OpenWith.exe," or the parent's name should be either "cmd.exe" or "powershell.exe".
- Certain false positives are excluded, such as processes with arguments ending in ".vsto" launched by specific parent executables or those involving uninstallation ("/Uninstall") of VSTOInstaller.exe. Additionally, specific instances involving rundll32.exe and VSTOInstaller.exe with arguments are considered false positives and excluded.

This comprehensive EQL query aims to identify potentially suspicious processes associated with Microsoft Office applications and VSTOInstaller.exe, considering various criteria and excluding known false positives⁶⁶.

⁶⁵ Execution of file written or modified by PDF reader | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/execution-of-file-written-or-modified-by-pdf-reader.html>

Windows Script Interpreter Executing Process via WMI

The screenshot displays the Elastic Security Solution interface for a rule definition. It is divided into two main sections: 'About' and 'Definition'.

About: This section provides metadata for the rule. It includes fields for Author, Severity, Risk score, License, and MITRE ATT&CK. The rule is identified as 'Initial Access (T14001)' and is associated with the 'WMI' tactic. It also lists related MITRE ATT&CK techniques such as 'Spearphishing Attachment (T1566.001)', 'EvilWinEXE (T1021)', 'Command and Scripting Interpreter (T1059)', and 'Visual Basic (T1026.001)'. The rule is categorized under 'Domain: Endpoint', 'OS: Windows', and 'Use Case: Threat Detection'.

Definition: This section contains the EQL query used for detection. The query is as follows:

```
index_patterns: ["logs-endpoint.events.*", "logs-windows.*", "logs-gmsa.*"]
sequence by host.id with maxspan = 5
only where host.os.type == "windows" and
(event.category == "Library", "Driver") or (event.category == "Process" and
event.action == "Image Loaded") and
(ctl.name == "wmiutils.dll" or file.name == "wmiutils.dll") and process.name in
["wscript.exe", "cscript.exe"]
process where host.os.type == "windows" and event.type == "start" and
process.parent.name == "wmiprvse.exe" and
user.domain != "NT AUTHORITY" and
(process.exe.original_file_name
in
["cscript.exe",
"msocrt.exe",
"PowerShell.exe",
"cmd.exe",
"MShta.exe",
"RUNESHELL32.EXE",
"REGSVR32.EXE",
"cmd64.exe",
"mshta64.exe",
"Regedit.exe",
"Regsvcs.exe",
"CONTROL.EXE",
"WINLSASS.EXE",
"Microsoft.Windows.Common-Infrastructure",
"msocrt.exe"]
) or
process.executable == ("C:\Users\%user%\AppData\Local\Microsoft\Windows\Scripts\wscript.exe")
```

Figure 100 - Windows Script Interpreter Executing Process via WMI query

This EQL query is crafted to identify potential malicious activities associated with the **"wmiutils.dll"** library on Windows systems, with a maximum time span of 5 seconds. The sequence is organized by host ID and consists of two primary components. The first part focuses on events related to the loading of libraries or drivers, or process events where an image is loaded. It specifically looks for occurrences involving the **"wmiutils.dll"** library and associated processes such as **"wscript.exe"** and **"cscript.exe"**. The second part of the sequence delves into process start events where **"wmiprvse.exe"** is the parent process, excluding events from the **"NT AUTHORITY"** domain. It further filters processes based on their original file names and executable paths, targeting potentially malicious executables commonly associated with various cyber threats. This comprehensive approach enables the detection of suspicious activities related to the **"wmiutils.dll"** library within a short time span⁶⁷.

⁶⁶ Suspicious execution via Microsoft Office Add-Ins | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/suspicious-execution-via-microsoft-office-add-ins.html>

⁶⁷ Windows Script Interpreter Executing Process via WMI | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/windows-script-interpreter-executing-process-via-wmi.html>

AWS Execution via System Manager

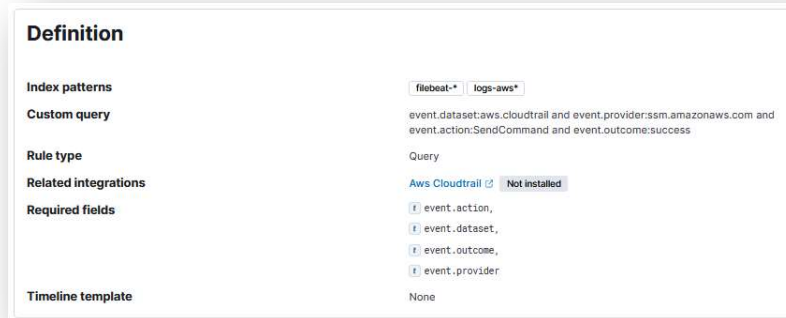


Figure 101 - AWS Execution via System Manager query

This query identifies the execution of commands and scripts via System Manager. Execution methods such as **RunShellScript**, **RunPowerShellScript**, and alike can be abused by an authenticated attacker to install a backdoor or to interact with a compromised instance via reverse-shell using system only commands. This EQL (Event Query Language) statement is designed to filter events within the AWS CloudTrail dataset, specifically focusing on actions related to the AWS Systems Manager (SSM) service⁶⁸. The query narrows down to events where the action is "**SendCommand**," indicating the initiation of a command within SSM, and the outcome of the action is deemed successful ("**event.outcome:success**").

Host Isolation with Elastic

Host isolation allows to isolate hosts from the network, blocking communication with other hosts on the network until manually release the host after threat investigation has been completed. Isolating a host is useful for responding to malicious activity or preventing potential attacks, as it prevents lateral movement across other hosts. Isolated hosts can still transmit data to Elasticsearch and Kibana. To facilitate this, host isolation exceptions can be established for specific IP addresses. These exceptions permit isolated hosts to communicate with designated IP addresses, even when restricted from accessing the rest of the network. Unfortunately, that feature is available on Platinum and Enterprise versions of Elastic, which do not give the opportunity to be tested on the lab environment. For host isolation feature to be used, the hosts must have Elastic Agents installed and run on Windows, macOS and Linux environments such as Ubuntu Servers, Debian, and CentOS. A host can be isolated from an agent having the privilege of Host Isolation within Elastic PAM system⁶⁹.

⁶⁸ AWS Execution via System Manager | Elastic Security Solution [8.12] | Elastic. (n.d.). Elastic. <https://www.elastic.co/guide/en/security/current/aws-execution-via-system-manager.html>

Endpoints

Hosts running Elastic Defend

Filter your data using KQL syntax Refresh Auto ref... 10 seconds

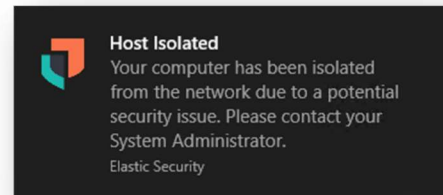
Showing 4 endpoints

Endpoint	Agent status	Policy	Policy status	OS	IP address	Version	Last active	Actions
ubuntu-2004	Healthy Isolated	Elastic Defend integr...	Success	Linux	192.168.1.10	8.5.0	Sep 27, 2022...	...
windows-10	Healthy	Elastic Defend integr...	Success	Windows	192.168.1.11	8.5.0	Sep 27, 2022...	...
windows-329	Healthy	Elastic Defend integr...	Success	Windows	192.168.1.12	8.5.0	Sep 27, 2022...	...
elastic-523	Healthy	Elastic Defend integr...	Success	macOS	192.168.1.13	8.5.0	Sep 27, 2022...	...

Rows per page: 10 < 1 >

Figure 102 - Elastic host isolation on Elastic Defender panel

Isolation of a host from a detection alert’s details flyout, from the Endpoints page, or (with an Enterprise subscription) from the endpoint response console. Once a host is successfully isolated, an Isolated status displays next to the Agent status field, which you can view on the alert details flyout or Endpoints list table as the screenshot shows above.



All actions executed on a host are tracked in the host’s response actions history, which can be accessed from the Endpoints page. The hosts isolation from the network can be executed through a detection alert (rule successfully finds a threat), an endpoint, the response and from automatic isolation rule. After the host is successfully isolated, an Isolated status is added to the endpoint. Active end users receive a notification that the computer has been isolated from the network.

For releasing an isolated host some actions must be executed by the user that has Host Isolation privilege. There are three ways from which the release of the hosts can be done such as releasing a host from detection alert, endpoint, and the response console. After the host is successfully released, the Isolated status is removed from the endpoint. Active end users receive a notification that the computer has been reconnected to the network. To confirm if a host has been successfully isolated or released, check the response actions history, which logs the response actions performed on a host⁷⁰.

⁷⁰ Jakobsson, M., & Myers, S. (2007). Phishing and countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience.

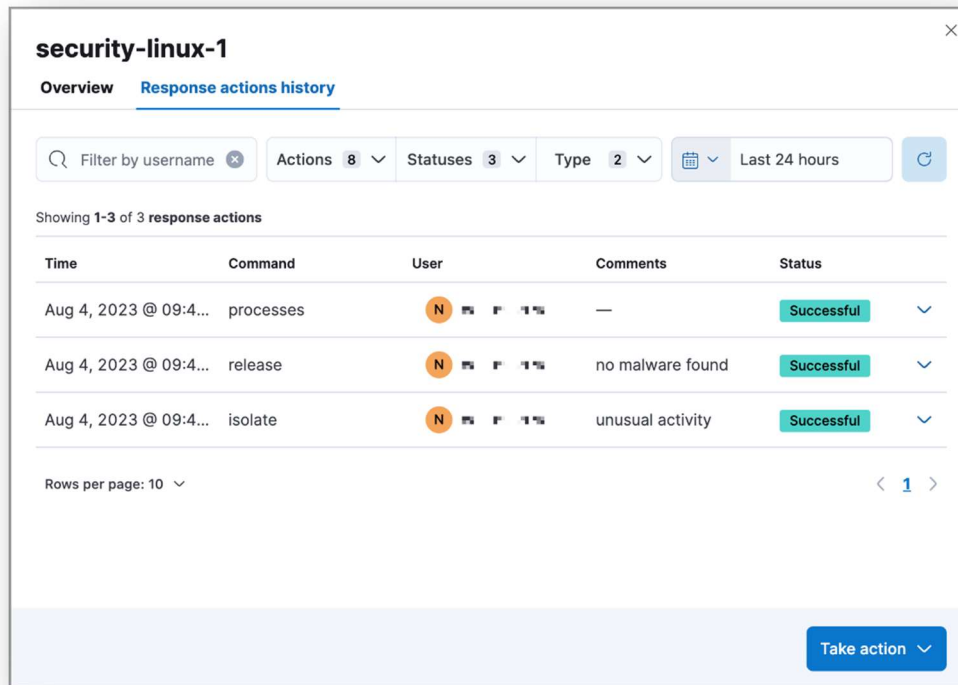


Figure 103 - Releasing isolated hosts

Proxmox Mail Gateway Controls

On the previous chapters an email architecture was designed. A fully functional approach to receive and deliver email messages across the components. The first component when receiving emails and the last component when sending emails is a Mail Gateway. In this architecture, Proxmox's solution named as Proxmox Mail Gateway (PMG) was implemented. PMG works as a firewall when managing emails both incoming and outgoing. Proxmox Mail Gateway has multiple white- and blacklists. It differentiates between the SMTP Whitelist, the rule-based whitelist, and the user whitelist. In addition to the whitelists, there are two separate blacklists: the rule-based blacklist and the user blacklist.

- SMTP Whitelist: the SMTP Whitelist is responsible for disabling greylisting, as well as SPF and DNSBL checks. These are done during the SMTP dialogue.
- Rule-based White-/Blacklist: the rule-based white- and blacklists are predefined rules. They function by inspecting the attached Who objects, which contain information such as a domain or email address, to identify a match. If it matches, the assigned action is used, which by default is Accept for the whitelist rule and Block for the blacklist rule. In the default setup, the blacklist rule has priority over the whitelist rule and spam checks.
- User White-/Blacklist: the user white- and blacklist are user specific. Every user can add mail addresses to their white- and blacklist. When a user adds a mail address to the whitelist, the result of the spam analysis will be discarded for that recipient. This capability can aid in the acceptance of the email, yet subsequent actions rely on other rules. In the default configuration, this leads to the email being accepted for the intended recipient.

For mail addresses on a user's blacklist, the spam score will be increased by 100. When a high spam score is encountered, the subsequent actions taken depend on the rule system in place. In the default setup, it will be recognized as spam and quarantined (spam score of 3 or higher).⁷¹

Mail Gateway Objects

Mail filter is the main tab which has the default implemented rules such as Blacklist etc. There a custom query can also be implemented. Every rule has 5 categories (**FROM, TO, WHEN, WHAT,** and **ACTION**), and each category may contain several objects to match certain criteria. Who is the sender or recipient of the email? Those objects can be used for the TO and/or FROM category. **Who** is the sender or recipient of the email? **What** is in the email? Does the email contain spam? **When** is the email received by Proxmox Mail Gateway? **Actions** - Mail is received between 8:00 and 16:00. Defines the final actions. Mark email with "SPAM:" in the subject. Rules are ordered by priority, so rules with higher priority are executed first. It is also possible to set a processing direction. **In** for incoming emails, **out** for outgoing emails A rule can be also disabled completely, which is mostly useful for testing and debugging. The Factory Defaults button allows you to reset the filter rules.

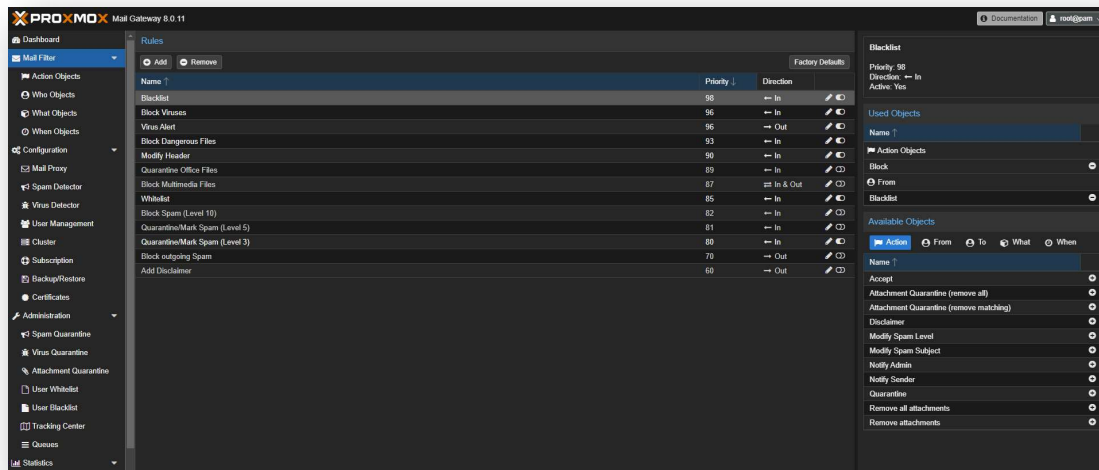


Figure 104 - Default rules of Proxmox

ACTION Objects

Accepting mail for delivery is acknowledged as a conclusive action in the email processing system. Similarly, **blocking** mail is recognized as a final step, preventing the delivery of specified emails. The **quarantine** procedure involves moving emails to designated quarantine areas based on their content, with virus-infected mails directed to the "virus quarantine" and others to the "spam quarantine." This quarantine process is also considered a final action.

The **notification** function encompasses sending notifications, leveraging macros in object configuration to easily incorporate additional information. An example is the default notify Admin object, which provides comprehensive details in the notification action body, including sender, receivers, targets, subject, and relevant rule information. Notifications can also include a copy of the original mail.

⁷¹ Proxmox Mail Gateway Documentation Index. (n.d.-b). <https://pmg.proxmox.com/pmg-docs/>

The **BCC** object duplicates emails to another target, allowing for the transmission of the original unmodified mail or the processed result. This distinction becomes significant, especially when prior rules have removed attachments.

The **Header Attributes** object facilitates the addition or modification of mail header attributes, utilizing macros for enhanced customization. For instance, the Modify Spam Level actions can add detailed information about detected spam characteristics to the X-SPAM-LEVEL header. Another example is the Modify Spam Subject action, which appends the "SPAM:" prefix to the original mail subject.

The **Remove Attachments** object offers the capability to strip all attachments or selectively remove those matching the rule's criteria. Additionally, users can specify replacement text if desired. Optionally, these modified mails can be relocated to the attachment quarantine, preserving the original mail with all attachments.

The **Disclaimer** function involves adding a disclaimer to emails, with support for HTML markup. This disclaimer is incorporated into the first text/html and text/plain parts of an email, contingent upon the text's compatibility with the mail's character encoding.

Name	Description	Comment	Editable
Attachment Quarantine (rem...)	remove matching attachments	Remove matching attachments and move the whole mail to the attachment quarantine.	Yes
Remove attachments	remove matching attachments	Remove matching attachments	Yes
Attachment Quarantine (rem...)	remove all attachments	Remove all attachments and move the whole mail to the attachment quarantine.	Yes
Remove all attachments	remove all attachments	Remove all attachments	Yes
Notify Sender	notify __SENDER__	Send notification	Yes
Notify Admin	notify __ADMIN__	Send notification	Yes
Modify Spam Subject	modify field: subject:SPAM: __SUBJECT__	Mark mail as spam by modifying the subject.	Yes
Modify Spam Level	modify field: X-SPAM-LEVEL: __SPAM_INFO__	Mark mail as spam by adding a header tag.	Yes
Disclaimer	disclaimer	Add Disclaimer	Yes
Block	block message	Block mail	No
Accept	accept message	Accept mail for Delivery	No
Quarantine	Move to quarantine.	Move mail to quarantine	No

Figure 105 - Action objects of rules

WHO Objects

These types of objects can be used for the TO and/or FROM category and match the sender or recipient of the email. A single object can combine multiple items, and the following item types are available:

- **Email:** Allows you to match a single mail address.
- **Domain:** Only match the domain part of the mail address.
- **Regular Expression:** This one uses a regular expression to match the whole mail address.

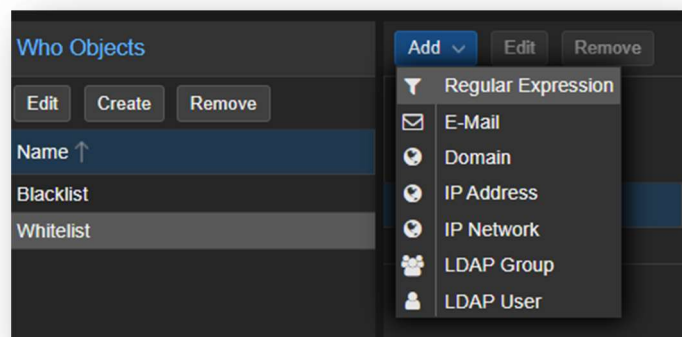


Figure 106 - Who objects of rules

- **IP Address or Network:** This can be used to match the senders IP address.
- **LDAP User or Group Test:** if the mail address belongs to a specific LDAP user or group.

Two important Who objects called Blacklist and Whitelist. These are used in the default ruleset to globally block or allow specific senders.

WHAT & WHEN Objects

Various objects are employed to classify the content of emails, and a single object can encompass multiple items. The available item types for content classification are as follows:

- **Spam Filter:** This object matches if the detected spam level is greater than or equal to the configured value, aiding in the identification and filtering of spam emails.
- **Virus Filter:** Designed to match on infected mails, the Virus Filter is instrumental in detecting and handling emails containing malicious content.
- **Match Field:** This object allows the matching of specified mail header fields, such as Subject: From: and others. It provides a versatile means to filter emails based on specific header information.
- **Content Type Filter:** Utilized to match specific content types within emails, the Content Type Filter is effective in categorizing and handling emails based on their content.
- **Match Filename:** Using regular expressions, the Match Filename object enables the matching of attachment filenames. It is particularly useful for identifying and managing emails with specific attachment names.
- **Archive Filter:** The Archive Filter is employed to match specific content types inside archives. This includes content types of both archived and regular (non-archived) attachments, offering comprehensive content classification capabilities.
- **Match Archive Filename:** This object uses regular expressions to match attachment filenames inside archives. Like the Archive Filter, it extends its matching criteria to cover filenames for both archived and regular (non-archived) attachments.

These content classification objects and item types contribute to a flexible and robust system for effectively managing and filtering emails based on their diverse attributes and characteristics.

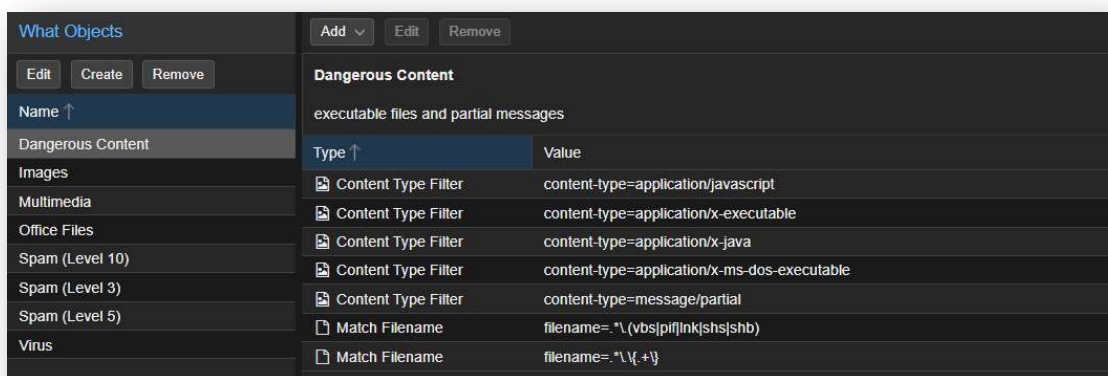


Figure 107 - What objects of rules

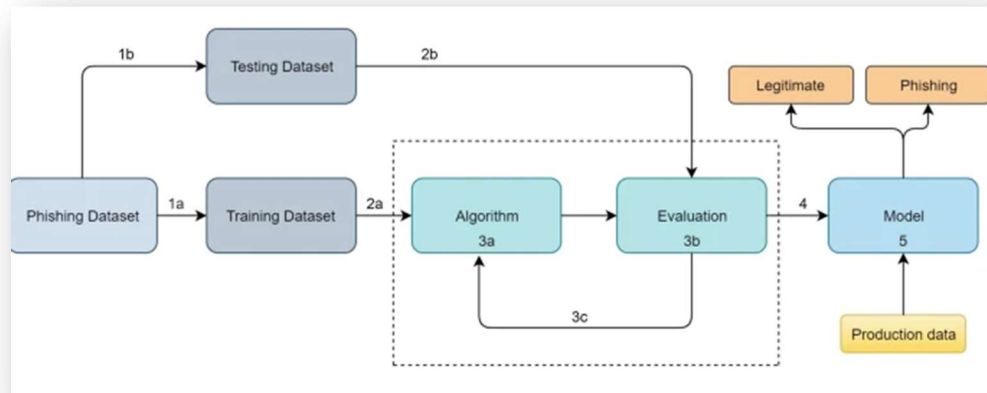
When objects are used to activate rules at specific times of the day. You can compose them from one or more time limit items.

Phishing and Artificial Intelligence

As phishing attacks continue to proliferate, so too do the technologies and techniques are employed by cybercriminals. Many cybersecurity tools designed to detect and prevent phishing emails from reaching users inboxes may be bypassed using newer adversary techniques. For instance, some emails containing HTML content may evade detection by mail gateways. With the advent of Artificial Intelligence (AI), some cybersecurity tools have integrated this technology to enhance their capabilities. The widespread adoption of Artificial Intelligence (AI) has a significant impact across various industries, including the realm of cybersecurity. In the domain of email security, AI has introduced heightened levels of speed, accuracy, and the ability to conduct thorough analyses. By leveraging prior knowledge stored in datasets, AI systems can effectively identify and mitigate various forms of email-based threats such as spam, phishing, and spear phishing attacks. These types of attacks can significantly erode trust among users of social services, such as web-based platforms. As described on previous chapters, a standard phishing attack typically unfolds in four stages. Initially, the perpetrator crafts and establishes a counterfeit website resembling a legitimate one. Subsequently, they distribute a URL link to this website to a targeted victim, assuming the guise of a credible entity, individual, or organization. Then, the unsuspecting victim is enticed to access the fraudulent website. Finally, the unfortunate victim unwittingly clicks on the deceptive link and divulges valuable personal data.

Recent advancements in deep learning (DL) methodologies have suggested that employing deep neural networks (NN) for the classification of phishing websites could surpass the performance of traditional machine learning (ML) algorithms. However, the effectiveness of deep NNs hinges heavily on the configuration of various learning parameters. Various DL approaches have been utilized for cybersecurity intrusion detection, including deep neural networks, feed-forward deep neural networks, recurrent neural networks, convolutional neural networks, restricted Boltzmann machines, deep belief networks, and deep auto-encoders. Figure 5 illustrates the functioning of deep learning models, where a set of input data is inputted to neurons and assigned specific weights to predict either phishing attacks or legitimate traffic.

Machine learning (ML) approaches are widely employed for detecting phishing websites, transforming the task into a straightforward classification challenge. To construct a learning-based detection system, the available data must encompass features relevant to both phishing and legitimate website classes. Various classifiers are utilized for phishing attack detection, with previous research indicating high detection accuracy owing to the adoption of robust ML techniques. Several feature selection methods are implemented to streamline the feature set. Figure 6 depicts the operation of the machine learning model, where a batch of input data is provided to the model for training, enabling it to discern between phishing attacks and legitimate traffic.



Streamlining features enhances dataset visualization, rendering it more efficient and comprehensible. Among the classifiers frequently utilized in numerous studies, C4.5, k-NN, and SVM have demonstrated notable accuracy in detecting phishing attacks. These classifiers, particularly those based on decision trees like C4.5, exhibit optimal accuracy and efficiency in phishing attack detection. However, researchers have identified limitations in their exploration of phishing attack detection. Many studies have noted a common constraint: the omission of ensemble learning techniques, while in some instances, feature reduction was neglected.

The Random Forest (RF) method consistently demonstrates superior performance, boasting the highest accuracy among various classification methods across diverse datasets. Multiple studies have substantiated that employing the RF classification method can achieve attack detection accuracies exceeding 95%. The UCI machine learning dataset emerges as a prevalent choice among researchers for detecting phishing attacks. While some studies have developed scenario-based environments to detect phishing attacks, these solutions are often tailored to specific contexts and may not generalize well across different organizational settings. Individual users within each organization exhibit unique behaviors, and awareness of predefined scenarios can vary. In addition to traditional methods, the hybrid learning approach has garnered attention for its potential to outperform RF in certain scenarios. Researchers advocate for the exploration of ensemble models, suggesting that they may further enhance performance in phishing attack detection⁷².

Defending against phishing attacks is increasingly challenging for system security experts. Developing a feasible detection system with low false positives is crucial for effectively identifying phishing attacks. While machine learning and deep learning algorithms are commonly used for this purpose, they come with high computational costs and may exhibit elevated false-positive rates, albeit being adept at distinguishing phishing attacks. Despite technological defenses, the most effective protection against phishing attacks remains educated and vigilant employees. However, human nature, characterized by curiosity and a desire for exploration, can still pose risks. To mitigate these risks, organizations should endeavor to cultivate a mindset among employees that discourages clicking on

⁷² Abdelhamid, N., Thabtah, F., Abdel-jaber, H. (2017). Phishing detection: A recent intelligent machine learning comparison based on models content and features. In 2017 IEEE international conference on intelligence and security informatics (ISI) (pp. 72–77). IEEE.

suspicious links and webpages. This involves distancing employees from their inherent inclination to explore and encouraging them to prioritize caution when interacting with online content⁷³.

Current practices and future challenges

Phishing attacks continue to intrigue attackers as they aim to deceive inexperienced internet users into divulging their private and confidential data. Despite various measures proposed to combat these attacks, attackers continuously exploit vulnerabilities in proposed solutions to persist with their malicious activities. The surge in phishing attacks linked to COVID-19 and online collaboration tools like ZOOM and Microsoft Teams during the pandemic has heightened research focus in this domain. With the shift towards online activities across government, corporate, educational, and non-commercial sectors, there is a growing demand for comprehensive phishing attack detection solutions offering improved accuracy and response times. Conventional detection approaches often fall short, recognizing only a fraction of phishing attacks. While machine learning (ML) approaches show promise, they come with scalability trade-offs and can be time-consuming, particularly on small datasets. Heuristic techniques, while effective, often result in high false-positive rates.

User awareness plays a crucial role in preventing phishing attacks, alongside interface modifications such as dynamic warnings to identify malicious emails. As IoT devices become more integrated into daily life, their security vulnerabilities make them prime targets for attackers. Phishing serves as a gateway for various malware and ransomware attacks, with recent trends indicating a rise in ransomware demands following data breaches. Phishing scams exploiting COVID-19 and healthcare-related themes have targeted unsuspecting users in 2020. Proactive defense measures, including anti-phishing frameworks or browser plug-ins, are essential for identifying and blocking suspicious websites. Automated reporting features can facilitate swift responses from organizations to mitigate potential damages to productivity and profitability. Looking ahead, an integrated phishing attack detection solution that autonomously identifies, reports, and blocks malicious websites without user intervention is envisioned. Such a solution would verify the legitimacy of websites requesting sensitive information and promptly alert relevant organizations. The development of scalable and robust web page health-checking mechanisms is imperative in this evolving landscape of online threats.

Finally, Machine learning (ML) techniques consistently yield superior results compared to other methods, with some ML approaches capable of identifying true positives (TP) up to 99%. Given the ever-evolving nature of malicious URLs and attackers' tactics to deceive users by modifying URLs, deep learning and machine learning methods have become indispensable for phishing attack detection. Commonly employed classification methods such as Random Forest (RF), Support Vector Machines (SVM), C4.5, Decision Trees (DT), Principal Component Analysis (PCA), and k-Nearest Neighbors (k-NN) have proven to be highly effective in this regard. Future research efforts should focus on developing more scalable and robust methods, including the integration of smart plugin solutions capable of tagging or labeling websites as either legitimate or potential phishing threats. By leveraging advanced ML techniques and innovative approaches, such as smart plugins, it is possible to enhance the efficiency and

⁷³ Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. *IEEE Access*, 8, 142532–142542.

accuracy of phishing attack detection, thus better equipping users and organizations to combat evolving cyber threats⁷⁴.

OCR Solution for Phishing

The advent of Optical Character Recognition (OCR) during the 1980s and 1990s held the promise of substantial time and cost savings by transforming printed or handwritten text into a machine-readable format. However, traditional OCR technologies fell short of expectations. While faster than manual data entry, they still required substantial manual effort and oversight. Setting up templates, establishing rules, and manually reviewing data were all necessary steps. Fortunately, advancements in AI OCR software have addressed these limitations. Modern AI-powered OCR systems are more accurate and automated than earlier versions, fulfilling the long-awaited promise of time and cost savings. These systems can swiftly and accurately extract data from documents, recognizing contextual clues to identify various elements such as addresses, names, and totals. Moreover, they can utilize this information to make data-driven decisions. Unlike their predecessors, modern AI OCR solutions require minimal manual intervention. There is no need for extensive manual exceptions, pre-sorting, or template-based document preparation. The automated process seamlessly captures and processes data, streamlining workflows and enhancing efficiency⁷⁵.

Analyzing the logo content from a target website and comparing it against the official website can be an effective method for confirming the authenticity of a website. Similarly, comparing SSL certificates between the target website and the official website can help identify phishing websites. This approach offers a high detection accuracy rate, and initial evaluation results are promising.

The OCR methodology described aims to detect potential phishing activity by analyzing images extracted from a website and comparing them to images from official websites. The process involves four steps:

- **Image Extraction:** Images, such as logos or background images, are extracted from the website using a web crawler. This includes considering both HTML code and .css files, as logos may be linked in various ways.
- **Image Content Description:** The content of the extracted images is described using the Google Optical Character Recognition (OCR) API. This helps identify relevant text within the images, such as logos or symbols, while ignoring redundant or irrelevant images.
- **Confirmation of Official URL:** Based on the content described in the images, keywords are used to search for related official URLs using the Google Search API. The top three results from the search are considered in the initial experiment.
- **Verify the feasibility of this methodology, programs may develop, requiring registration for access to open-source APIs including the Google OCR API and Google Search API.**

⁷⁴ Basit, A., Zafar, M., Liu, X. et al. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommun Syst* 76, 139–154 (2021). <https://doi.org/10.1007/s11235-020-00733-2>

⁷⁵ Rossum. (2023, December 19). OCR and AI: How Modern Automated Processing Works - Cognitive Data Capture | Rossum. Cognitive Data Capture | Rossum. <https://rosum.ai/blog/ocr-and-ai-how-modern-automated-processing-works-2/>

The effectiveness of this method heavily relies on OCR technology, as the accuracy of the result depends on the details recognized within the images. Initially, e.g., on Microsoft (Azure) OCR API utilization, the testing of OCR revealed limitations, particularly with logos featuring dark backgrounds or using SVG image formats. However, challenges persist, including:

- **Accuracy of Logo Extraction:** Phishing schemes may employ various methods to insert logos, making it challenging to locate them, especially if the entire page is an image.
- **Cost of OCR API:** While OCR APIs offer a free quota per day, additional checks incur charges. Thus, processing on a larger scale requires careful consideration of the associated costs.
- **Efficiency of System:** Phishing websites can be complex, storing numerous images or .css files. This complexity can significantly prolong the computing process for both web crawling and image recognition.
- **Single Detectability:** While this method aids in identifying phishing URLs based on image comparison, it does not address the broader threat landscape. Phishing attacks can also involve malware deployment, making it crucial to incorporate additional security measures to mitigate such risks effectively.

It is worth noting that while the published OCR APIs may be effecting on recognizing specific text in images, while other OCR APIs, such as Microsoft Azure, did not yield satisfactory results. This underscores the importance of choosing appropriate tools and techniques for image analysis in phishing detection.⁷⁶

Conclusion

This dissertation has delved into the pervasive and detrimental impact of phishing attacks on organizations and individuals, highlighting the pressing need for robust security measures. The study has underscored the pivotal role of implementing effective security controls and solutions at the mail gateway and Security Information and Event Management (SIEM) levels. These measures are crucial for fortifying defenses against evolving phishing techniques and mitigating the potential risks associated with unauthorized access, data breaches, and financial losses.

Looking ahead, the integration of artificial intelligence (AI) in the realm of phishing detection emerges as a promising frontier. The advent of sophisticated AI algorithms promises to enhance the accuracy and efficiency of phishing detection systems. As technology advances, AI-driven solutions are poised to evolve, becoming more adept at recognizing subtle patterns and anomalies indicative of phishing attempts. The proactive adoption of such innovative technologies is essential for staying ahead of increasingly sophisticated cyber threats. However, it is imperative to recognize that technological solutions alone are not sufficient. The human element remains a critical factor in the defense against phishing attacks. It is crucial to promote awareness among individuals, fostering a culture of cyber vigilance. Education initiatives must be widespread, equipping users with the knowledge and skills needed to identify phishing attempts, understand the consequences of falling victim to such attacks, and adopt best practices for safeguarding personal and organizational information.

⁷⁶ Y. Wang and I. Duncan, "A Novel Method to Prevent Phishing by using OCR Technology," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 2019

In conclusion, a multi-faceted approach that combines advanced technological solutions, continuous education, and heightened user awareness is essential for building resilient defenses against phishing attacks. As the digital landscape evolves, a collaborative effort between technology developers, security professionals, and end-users is paramount to create a secure online environment for individuals and organizations alike.