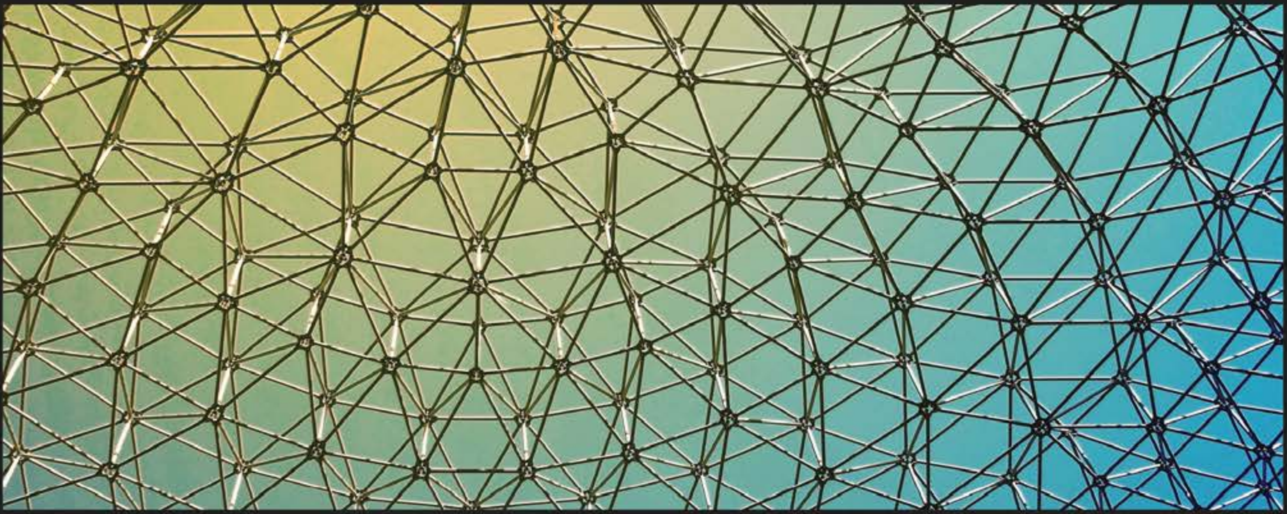
<packt>



1ST EDITION

Effective Threat Investigation for SOC Analysts

The ultimate guide to examining various threats and attacker techniques using security logs

MOSTAFA YAHIA

Table of Contents

Preface xiii

Part 1: Email Investigation Techniques

1

Investigating Email Threats 3

Top infection vectors 3

Why do attackers prefer phishing emails to gain initial access? 4

Email threat types 5

Spearphishing attachments 6

Spearphishing Link 7

Blackmail email 8

Business Email Compromise (BEC) 10

Attacker techniques to evade email security detection 10

Social engineering techniques to trick the victim 12

The anatomy of secure email gateway logs 15

Investigating suspicious emails 17

Investigating the email sender domain and SMTP server reputation 17

Spoofing validation 18

Email sender behavior 21

Email subject and attached filename 21

Investigating suspicious email content 22

Summary 26

2

Email Flow and Header Analysis 27

Email flow 27

Email header analysis 29

Email message content and metadata 34

Email X-headers 36

The header that was added by the hop servers 37

Email authentication 38

Investigating the email header of a spoofed message 45

Summary 46

Part 2: Investigating Windows Threats by Using Event Logs

3

Introduction to Windows Event Logs 49

Windows event types 49
Security event log types 50
System event log types 51
Application event log types 51
Other event log types 51
Windows event log analysis tools 52
The investigative approach for this part of the book 56
HELK installation 56
Summary 57

4

Tracking Accounts Login and Management 59

Account login tracking 59
Windows accounts 60
Tracking successful logins 62
Tracking successful administrator logins 64
Tracking logon sessions 66
Tracking failed logins 67
Login validation events 71
Login validation Event IDs (NTLM protocol) 71
Login validation Event IDs (Kerberos protocol) 72
Account and group management tracking 73
Tracking account creation, deletion, and change activities 74
Tracking creation and account adding to security groups 75
Summary 78

5

Investigating Suspicious Process Execution Using Windows Event Logs 79

Introduction to Windows processes 80
Windows process types 81
Common standard Windows processes 82
Windows Process Tracking events 86
Creator Subject 87
Target Subject 87
Process Information 88

Investigating suspicious process executions 92
Hiding in plain sight 92
Living Off The Land (LOTL) 94
Suspicious parent-child process relationships 96
Suspicious process paths 99
Summary 100

6

Investigating PowerShell Event Logs 101

Introducing PowerShell 101
Why do attackers prefer PowerShell? 102
PowerShell usage in different attack phases 103
PowerShell execution tracking events 106
Investigating PowerShell attacks 112
Fileless PowerShell malware 112
Suspicious PowerShell commands and cmdlets 112
Summary 114

7

Investigating Persistence and Lateral Movement Using Windows Event Logs 115

Understanding and investigating persistence techniques 116
Registry run keys 116
Windows scheduled tasks 119
Windows services 122
WMI event subscription 124
Understanding and investigating lateral movement techniques 126
Remote Desktop connection 126
Windows admin shares 130
PsExec – a Sysinternals tool 135
PowerShell remoting 140
Summary 143

Part 3: Investigating Network Threats by Using Firewall and Proxy Logs

8

Network Firewall Logs Analysis 147

Firewall logs value 147
Firewall logs anatomy 149
Log Timestamp 149
Source IP 149
Source Port 149

Destination IP 150
Destination Port 150
Source Interface Zone 151
Destination Interface Zone 151
Device Action 152
Sent Bytes 152
Received Bytes 152
Sent Packets 152
Received Packets 153
Source Geolocation country 153
Destination Geolocation country 153
Summary 153

9

Investigating Cyber Threats by Using the Firewall Logs 155

Investigating reconnaissance attacks 155
Public-facing IPs and port scanning 156
Internal network service discovery 157
Investigating lateral movement attacks 158
Remote desktop application (RDP) 158
Windows admin shares 159
PowerShell Remoting 160
Investigating C&C and exfiltration attacks 161
Investigating suspicious traffic to external IPs 162
Investigating DNS tunneling 163
Investigating data exfiltration 167
Investigating DoS attacks 168
Summary 171

10

Web Proxy Logs Analysis 173

Understanding the value of proxy logs 173
The significance of proxy log investigation 174
The anatomy of proxy logs 175
The source IP (src) 176
The source port (srcport) 176
The destination IP (dst) 176
The destination port (dstport) 177
The username (username) 177
The log timestamp (devicetime) 177
The device action (s-action) 178
The response status code (sc-status) 178
The HTTP method (cs-method) 179
The received bytes from the server by the client (sc-bytes) 179
The sent bytes from the client to the server (cs-bytes) 180
The web domain (cs-host) 180
The MIME type (Content-Type) 180
The user agent (cs(User-Agent)) 181
The referrer URL (cs(Referer)) 182
The website category (filter-category) 183
The accessed URL (cs-uri) 184
Summary 184

11

Investigating Suspicious Outbound Communications (C&C Communications) by Using Proxy Logs 185

Suspicious outbound communications alerts 186

Investigating suspicious outbound communications (C&C communications) 186

Investigating the web domain reputation 187

Investigating suspicious target web domain names 188

Investigating the requested web resources 192

Investigating the referrer URL 193

Investigating the communications user agent 196

Investigating the communications' destination port 199

Investigating the received and sent bytes, the HTTP method, and the Content-Type 200

Investigating command and control techniques 202

Summary 204

Part 4: Investigating Other Threats and Leveraging External Sources to Investigate Cyber Threats

12

Investigating External Threats 207

Investigating web attacks 207

The command injection vulnerability 207

The SQL injection vulnerability 208

Path traversal vulnerability 209

XSS vulnerability 211

Investigating WAF logs 212

Investigating suspicious external access to the remote services 216

Investigating unauthorized VPN and RDP access 216

Investigating compromised mailboxes 217

Investigating suspicious authentications to web services 218

Summary 218

13

Investigating Network Flows and Security Solutions Alerts 219

Investigating network flows 220

Investigating IPS/IDS alerts 220

Investigating endpoint security solutions alerts 224

Investigating AV alerts 224
Investigating EDR alerts 225
Investigating network sandbox and AV alerts 228
Summary 229

14

Threat Intelligence in a SOC Analyst's Day 231
Introduction to threat intelligence 231
Strategic level 232
Operational level 232
Tactical level 232
The role of threat intelligence in SOCs 232
Investigating threats using VirusTotal 233
Investigating suspicious files 234
Investigating suspicious domains and URLs 242
Investigating suspicious outbound IPs 244
Investigating threats using IBM X-Force Exchange 245
Investigating suspicious domains 246
Investigating suspicious IPs 248
Investigating the file hash 250
Investigating suspicious inbound IPs using AbuseIPDB 250
Investigating threats using Google 252
Summary 254

15

Malware Sandboxing – Building a Malware Sandbox 255
Introducing the sandbox technology 255
Sandbox types 256
Sandbox installation requirements 256
Required tools for analysis 257
Static analysis tools 257
Dynamic analysis tools 257
Preparing the guest VM 258
Guest preparation steps 259
Tips to evade the sandbox's detection 259
Analysis tools in action 260
Static analysis phase 260
Dynamic analysis phase 263
Hands-on demo lab 267
Scanning the file using YARA 268
Conducting static analysis 269
Conducting dynamic analysis 273
Analyzing the outputs 273
Summary 278
Index 279
Other Books You May Enjoy 290

1

Investigating Email Threats

Email threats are among the most common types of attacks encountered by **Security Operations Center** (**SOC**) analysts, and they often occur multiple times during a working shift. Moreover, malicious emails are often the first step in an attacker's attempt to gain access to a target environment. Given the increase in these types of threats, SOC analysts and cyber investigators must understand attackers' techniques to initiate attacks via email and how to investigate and respond to email threats.

The objective of this chapter is to learn why attackers prefer phishing emails to gain initial access, the most common email threats, the most common techniques by attackers to evade detection and trick the victim, how to analyze email secure gateway logs, and how to investigate suspicious emails.

In this chapter, we will cover the following main topics:

- Top infection vectors
- Why attackers prefer phishing emails to gain initial access
- Email threat types
- Attackers' techniques to evade email security detection
- Social engineering techniques to trick the victim
- The anatomy of secure email gateway logs
- Investigating suspicious emails

Let's get started!

Top infection vectors

In the cyberattack chain, once an attacker has conducted reconnaissance against the target victim's environment and infrastructure, and prepared the necessary weapons and equipment, the next step is to determine their preferred method and technique to gain initial access to the victim's environment. Attackers have several techniques at their disposal to gain initial access, including sending phishing emails, exploiting public-facing applications, luring users to visit a compromised website through drive-by compromise, and stealing valid remote credentials such as a VPN or RDP. Understanding the various techniques attackers use to gain initial access is crucial for security professionals to identify and prevent attacks before they can cause damage.

As per the IBM Security X-Force report, 41% of the attackers prefer phishing techniques to gain initial access to the victim's environment, either by sending a weaponized document or a malicious link to the target victims (see *Figure 1.1*).

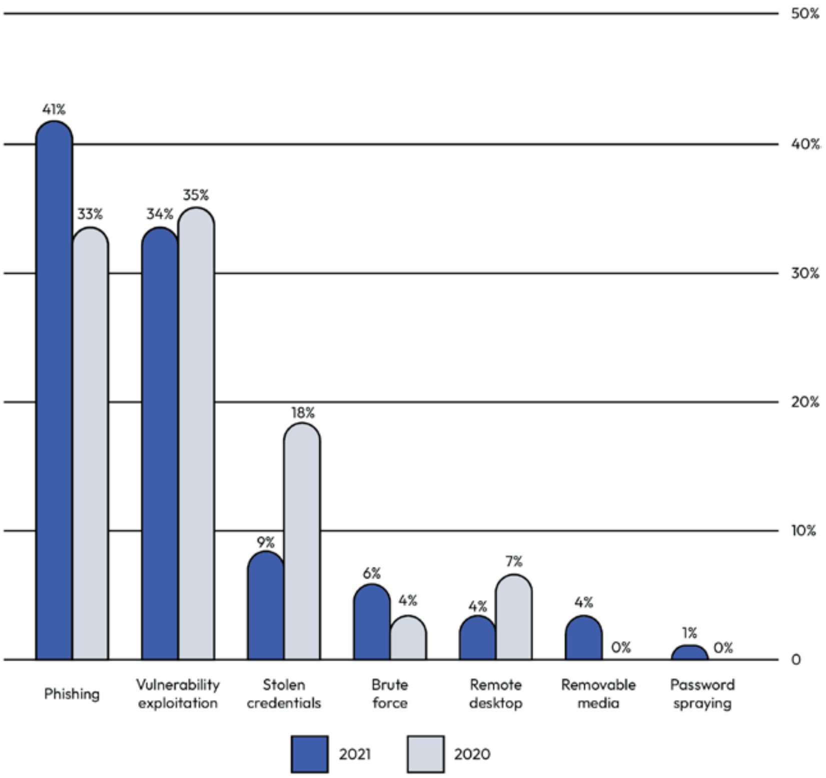


Figure 1.1 – The top infection vectors from the IBM Security X-Force Threat Intelligence Index 2022

Let us explain why most attackers prefer to gain initial access by using phishing mechanisms.

Why do attackers prefer phishing emails to gain initial access?

A **phishing email** is a type of social engineering attack where an attacker tricks target victims into opening a malicious file or link or providing personal or confidential information, such as passwords and credit card numbers, through fraudulent emails. The reason why phishing is a preferred and successful way for attackers to gain initial access to the victim's environment is due to several factors, including the following:

- It is easy during the reconnaissance phase to acquire a list of target victim users' email addresses.

  The reconnaissance phase is the first step taken by intruders to breach a target environment. This phase can last for hours, days, weeks, or even months. During this phase, attackers collect information about the target victim, including their email addresses, which can be used to deliver a weaponized document or link. Attackers can collect email addresses in several ways, such as through job postings, social media platforms such as LinkedIn, third-party subscriptions, data leaks on the dark web, Wayback Machine archives such as `Archive.org`, or data collection from marketing platforms such as `ZoomInfo.com`.

- It is not hard to prepare a weaponized attachment or link.

  It is relatively easy for an attacker to upload malware to legitimate cloud platforms and then share the download link with the victim through email. They can also weaponize a document through **Visual Basic for Applications** (**VBA**) macros or send the malware executable itself in a compressed format, all of which can be sent to the victim via email.

- Many users lack security awareness.

  Attackers exploit the fact that many users may be vulnerable to social engineering attacks, and a majority of them may not have received proper security awareness training to recognize and respond to these threats.

Now that you understand why most attackers choose phishing emails as a way to achieve their goals, such as gaining initial access to the victim's environment, let us discuss the various email threat types.

Email threat types

Email threats are every threat your environment faces when deciding to use an email service. They are not limited to phishing emails only; some attackers also use email for blackmailing, information leakage, data exfiltration, and lateral movement. In this section, we will focus on email threats that originate from external sources and discuss in detail four common types of email threats that organizations face:

- Spearphishing attachments
- Spearphishing links
- Blackmail emails
- Business Email Compromise

Spearphishing attachments

A **spearphishing attachment** involves adversaries sending phishing emails to target victims with malicious attachments, either to gain initial access to their systems or harvest their credentials. After defining a list of the victims' email addresses and preparing the weaponized attachment, the attacker become ready to send the email to the victim with one click. However, the question remains, which weaponized attachment will an attacker choose? Let us discuss the most common weaponized attachment types used by threat actors.

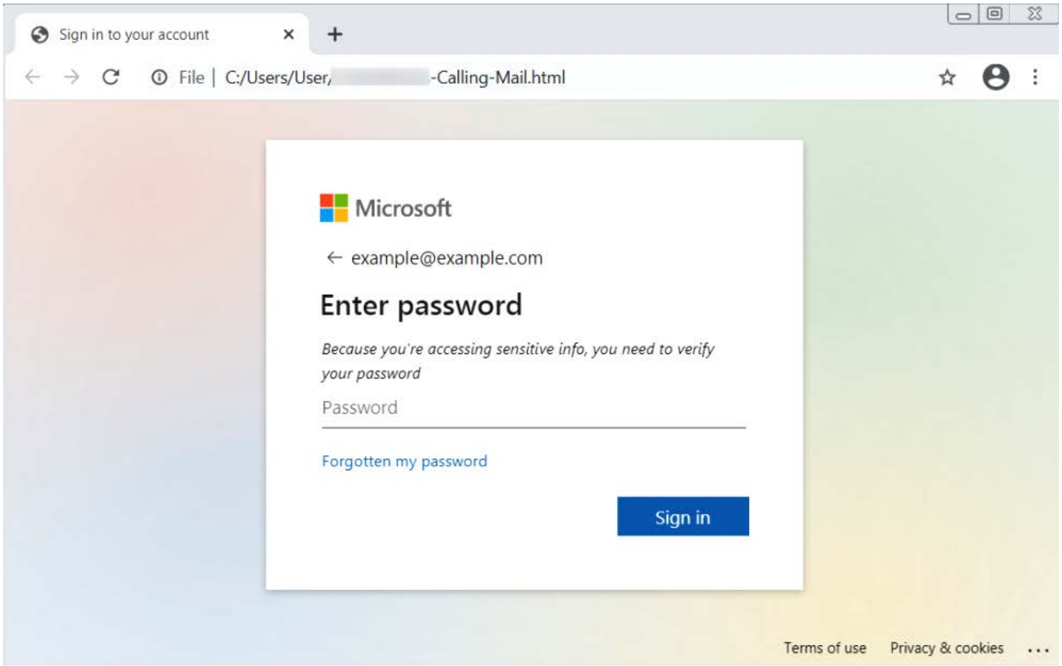
> **Note**
>
> Phishing and spearphishing are both types of email attacks that aim to steal sensitive information or compromise a target's computer system. While both methods have the same ultimate goal, the primary difference between the two is the level of targeting involved. Phishing emails are mass email attacks that are sent to a randomly large number of people. In contrast, spearphishing emails are much more targeted and personalized. They are specifically crafted to target a particular individual or group of individuals, such as employees of a particular company or members of a specific organization.

Phishing attachment types

When you hear the term *phishing attachment*, you may think about just one or two types of attachments, but due to the different preferred attacker methods, target victims' infrastructure and business, and attacker goals, there are variants of the malicious attachment types that attackers email to their target victims. The following are the five most common examples of phishing attachment types:

- **Malicious Microsoft Office documents**: Attackers often use a weaponized Microsoft document with VBA macros, such as Excel, Word, or PowerPoint documents, and send it to the target victim to trick them into opening it, thereby gaining initial access to their machine. This type of attachment is the most commonly used in spearphishing attacks because almost all enterprises use Microsoft documents in their day-to-day work. Additionally, it is easy for attackers to develop a weaponized Microsoft document. Weaponized Microsoft documents provide unlimited features to attackers, and also, they can exploit known vulnerabilities that affect Office apps.
- **Malicious PDF files**: Attackers can also use a decoy PDF file that contains malicious code to exploit PDF reader vulnerabilities and gain initial access to the victim's system, or harvest their credentials. PDF files are a popular choice for attackers because it allows them to easily embed malicious JavaScript code, and the inclusion of links, images, and fonts can make a file appear legitimate and increase the likelihood that the victim will interact with it. This type of attack is often used in spearphishing campaigns, where the attacker targets a specific individual within an organization with a highly personalized email that contains a malicious PDF attachment.
- **Compressed files (.rar, .7z, zip, etc.)**: An attacker may send a compressed file containing executable malware to the victim, tricking them into extracting it and executing the executable file.

- **ISO images**: Recently, we observed a notable increase in the use of `.iso` files to deliver malware to target recipients. Attackers depend on ISO image files because they are like disc images; hence, they can be used to bypass file filters and evade antivirus detection.
- **HTML files**: An attacker may send an HTML phishing attachment that impersonates familiar login pages, such as the Microsoft login page, the DHL login page, or a bank login page, to harvest the victim's credentials (see *Figure 1.2*).



Sign in to your account

File | C:/Users/User/[redacted]-Calling-Mail.html

Microsoft

example@example.com

Enter password

Because you're accessing sensitive info, you need to verify your password

Figure 1.2 – An HTML phishing attachment impersonating a Microsoft login page

As you can see, an attacker developed an HTML phishing file impersonating the Microsoft login page to trick the victim into entering their credentials.

Spearphishing Link

A **spearphishing link** involves adversaries sending spearphishing emails to target victims with a malicious link, to either harvest their credentials or trick them into downloading malware and executing it on their machine, thus gaining initial access to their systems. As with all email threats, after defining a list of the victim's email addresses and preparing the phishing link, the attacker is ready to send an email to the victim. But what is the attacker's purpose in sending the spearphishing link to the victims? Let us discuss the two most common types of phishing links used by attackers.

Phishing link types

As we mentioned before, every adversary has different intentions. Some of them just want to harvest a victim's credentials, while others want to gain an initial foothold in the victim's system. As with spearphishing attachments, there are variants of malicious link types that attackers use to mail to target victims. The following are two common examples of phishing link types:

- **A phishing link to harvest credentials**: One of the forms of a credential harvesting attack is when the attackers send a phishing email armed with links to bogus websites to trick a user into entering their credentials. To host their phishing page, an attacker may use their own domains or abuse legitimate web applications hosting domains, such as `appspot.com` and `web.app` domains, as we will see later in the *Attacker techniques to evade email security detection* section. In 2014, an American multinational financial services company fell victim to a cyberattack. The attack started when attackers sent phishing emails to employees that contained a link to a fake website resembling the company's VPN login page. The employees were tricked into entering their login credentials, which were then harvested by the attackers. With access to the company's network, the attackers were able to steal data on more than 76 million households and 7 million small businesses.
- **A phishing link to download malware**: An attacker may host the malware on their web server or well-known legitimate cloud file hosting services, such as MEGA, OneDrive, or Dropbox, and then share the file sharing link with their victim over email and try to trick them into downloading and executing the malicious executable. In 2017, a global law firm fell victim to a massive cyberattack that used a phishing email to deliver malware. The attack started when an employee received an email that appeared to be from a client, with a subject line referencing a real estate matter. The email contained a link that the employee clicked on, which then downloaded malware onto the firm's network. The malware quickly spread throughout the firm's global network, infecting systems and encrypting files. The attackers demanded a ransom payment in exchange for the decryption key. The attack caused significant disruption to the firm's operations, and it took several weeks to fully recover.

Blackmail email

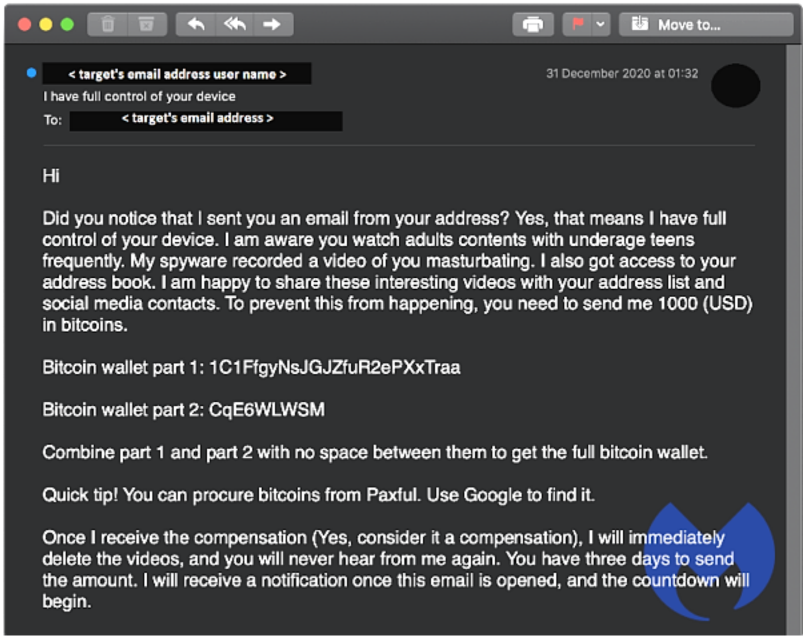
A **blackmail email**, also known as a **"sextortion" email**, is a term used to describe an email scam where an attacker claims to have compromised the victim's machine and exfiltrated sensitive data, including sexual content and pictures to the attacker's server. The attacker then demands payment in bitcoin and threatens to publish the data on the internet if the victim does not comply. In order to convince the victim that they have indeed been compromised, attackers typically employ one of two methods, which we will discuss in the next section. This type of email scam is particularly effective as it preys on people's fear of having their private information exposed, and the use of cryptocurrency makes it difficult to trace the attacker.

Methods to prove infections

Proving a data breach to the victim may seem simple if the attacker has acquired actual sensitive data, such as sexual content, pictures, or confidential files. However, in many cases, attackers may not have accessed valuable data or compromised the victim's machine at all and simply attempt to scam the victim. There are two common methods that attackers use to convince victims that a data breach has occurred:

- **Screenshots of the breached data or from the victim's machine**: The blackmailer may compromise the victim's data by either deploying malware on their machine, such as Infostealer malware, or by purchasing the victim's data from data leakage stores on the dark web. In both cases, the attacker usually obtains screenshots of the breached data or the victim's machine desktop and folders to prove the breach to the victim.
- **Spoofing the target victim's email address**: In many cases, the blackmailer is simply a scammer and never had access to either the victim's machine or data. In such situations, the blackmailer uses the email spoofing technique to trick the victim into thinking that his machine has been compromised by the blackmailer. The **email spoofing** technique is a technique used in email attacks to trick recipients into thinking that a message came from a mail sender other than the actual sender. In the case of blackmail, the attacker usually spoofs the victim's email address itself to send the blackmail email to the victim to trick them into thinking that they are compromised, and the attacker used their email address to send him this blackmail email to prove the breach (see *Figure 1.3*).

The email spoofing technique will be covered in detail in the next chapter, *Email Flow and Header Analysis*.



< target's email address user name >

31 December 2020 at 01:32

I have full control of your device

To: < target's email address >

Hi

Did you notice that I sent you an email from your address? Yes, that means I have full control of your device. I am aware you watch adults contents with underage teens frequently. My spyware recorded a video of you masturbating. I also got access to your address book. I am happy to share these interesting videos with your address list and social media contacts. To prevent this from happening, you need to send me 1000 (USD) in bitcoins.

Bitcoin wallet part 1: 1C1FfgyNsJGJZfuR2ePXxTraa

Bitcoin wallet part 2: CqE6WLWSM

Combine part 1 and part 2 with no space between them to get the full bitcoin wallet.

Quick tip! You can procure bitcoins from Paxful. Use Google to find it.

Once I receive the compensation (Yes, consider it a compensation), I will immediately delete the videos, and you will never hear from me again. You have three days to send the amount. I will receive a notification once this email is opened, and the countdown will begin.

Figure 1.3 – A spoofed blackmail email (Malwarebytes)

As you see in the preceding screenshot from the Malwarebytes website, the attacker in this scenario used the email spoofing technique to spoof the victim's email address to send a blackmail message to the victim, claiming that the victim's data has been compromised and that the attacker possesses sexual content, which they will release to the victim's contacts if the victim does not transfer 1,000 USD to the attacker's bitcoin wallet.

Business Email Compromise (BEC)

Business Email Compromise (**BEC**) is a type of email scam where the attacker targets a specific individual within a company who has access to financial information, such as an executive or a finance employee, and tricks them into making a fraudulent financial transaction or wire transfer. BEC attacks often involve the email thread hijacking technique, which we will discuss in the *Social engineering techniques to trick the victim* section, or spoofing the email address of a trusted partner or company executive to convince the victim to transfer money or sensitive information to the attacker's account.

BEC attacks are one of the most trending and result in significant financial losses for organizations, making them a growing concern in the cybersecurity community.

In 2018, the US Department of Justice reported that a Nigerian cybercriminal group called Gold Galleon had used the email thread hijacking technique in BEC attacks against maritime shipping companies. The group would first gain access to an employee's email account through spearphishing or other means. Once they had access, they would search the employee's emails for ongoing conversations related to cargo shipments and then use the email thread hijacking technique to intercept and take over the thread. Using this technique, the attackers could impersonate the legitimate email sender and request that payment for the cargo shipment be redirected to a new bank account. Since the email appeared to be part of an ongoing conversation, the victim would often not suspect anything was wrong and would comply with the request, resulting in significant financial losses for the targeted companies.

In one case, the Gold Galleon group was able to steal over $1 million from a shipping company using this technique. The group is believed to have targeted over 100 maritime shipping companies in the United States, Europe, and Asia, with losses totaling tens of millions of dollars.

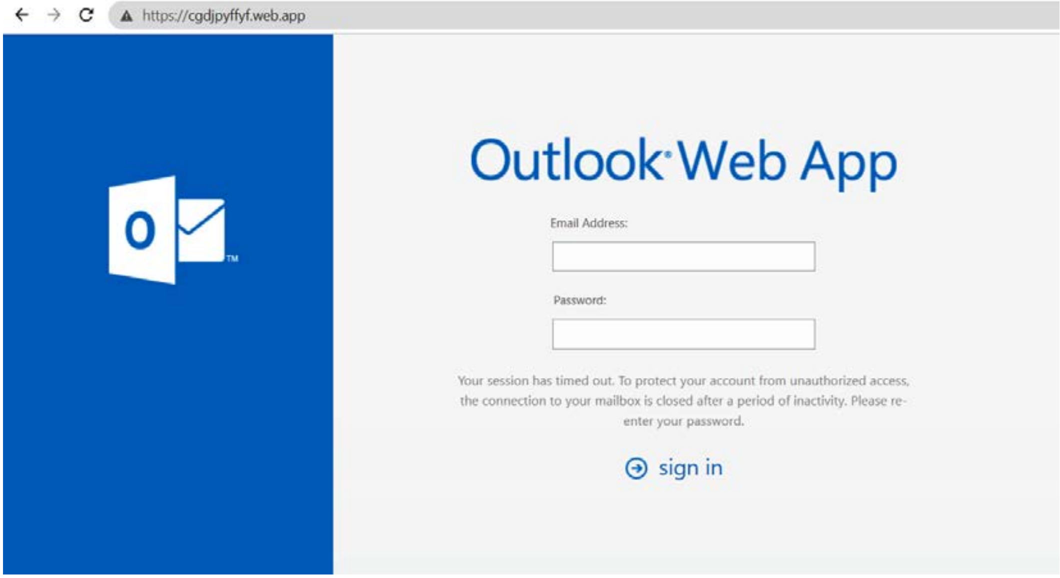
Now that you are familiar with the most four common email threat types, let us see the attacker techniques to bypass email security solutions deployed in the victim's environment, as well as the attacker techniques to evade email security detection.

Attacker techniques to evade email security detection

As cyber defense and security controls have become increasingly advanced, attackers have become more creative in their techniques to evade detection by email security solutions. Many critical organizations have now deployed such solutions to check every email sent from external senders to internal recipients, and they have skilled SOCs and threat-hunting teams to detect and respond to threats. In this section, we will explore some of the techniques that attackers use to bypass email security solutions and carry out successful attacks:

- **Using newly created domains to send a malicious email**: Modern email security solutions are fortified with threat intelligence feeds, which include an updated list of sender domains with a bad reputation resulting from their malicious use in previous phishing campaigns. To evade detection by email security solutions that block malicious emails due to sender domain reputation, attackers often create new domains that have not been used previously in any malicious activities.
- **Using non-blacklisted SMTP servers**: Like malicious sender domain feeds, a secure email gateway can be enriched with threat intelligence feeds of the known malicious **Simple Mail Transfer Protocol** (**SMTP**) server IPs that are usually used during phishing campaigns, which are blocked. To avoid their malicious emails being blocked by email security solutions due to the bad reputation of the SMTP server IPs, attackers tend to use non-blacklisted IP addresses.
- **Sandbox analysis evasion**: Email gateway security appliances have significantly improved over time and now include sandbox technology that can analyze every attachment sent from external email senders to internal employees. We will deep dive into sandboxing later in the book, but for now, it is worth knowing that **sandbox** technology is a vital tool, used by cybersecurity analysts and solutions to analyze the behavior of files and executables before running them in a real environment, ensuring that they are not harmful. However, attackers are well aware of this technology and use various techniques to evade sandbox detection efforts, such as the following:
    - **Malware sleep**: To evade detection from sandbox analysis, an attacker can take precautions by, for example, incorporating a sleep time of up to three minutes in their malware code after execution, thereby delaying the start of any malicious activity until after the sandbox analysis has been completed and avoiding detection by the sandbox's real-time monitoring.
    - **Encrypted file**: An attacker can employ a technique of sending a malware file to the victim in the form of a compressed folder or document file, encrypted with a password, which is then shared with the victim via the email body for decryption. Since submitting an attachment file to a sandbox by an email gateway is not an interactive submission process, the password cannot be provided to the sandbox during file analysis to decrypt and analyze the file. Therefore, the sandbox fails to analyze the attachment, allowing it to pass through to the victim's mailbox undetected.
    - **Sandbox discovery**: After the malware is executed, it may check for the presence of a virtual machine environment, search for any malware analysis tools, and detect abnormal user activity to determine whether it is running in a sandbox environment. If the malware detects any signs of sandbox technology, it may alter its intended actions, stop running, go into sleep mode, or take other evasive actions to avoid detection by the sandbox.
    - **Responding to specific requests**: Another technique used by sophisticated attackers in targeted attacks to evade analysis is to respond only to requests sent from the victim environment's IP addresses, collected during the reconnaissance phase.

- **Trusted domains hosting phishing pages**: In 2019, cybersecurity researchers detected phishing subdomains and pages hosted on trusted cloud application hosting domains, including `appspot.com` and `web.app` domains. Attackers were able to abuse these domains by hosting malicious subdomains that contained phishing login pages targeting well-known brands, such as Microsoft Outlook and Dropbox. Due to being hosted on legitimate web servers, these phishing URLs were not categorized as malicious domains in threat intelligence platforms, which made them difficult to block with email gateway security solutions. However, email gateway security solutions that received threat intelligence feeds that included specific phishing subdomains/hostnames could block the phishing attempts (see *Figure 1.4*).



https://cgdjpyffyf.web.app

Your session has timed out. To protect your account from unauthorized access, the connection to your mailbox is closed after a period of inactivity. Please re-enter your password.

Figure 1.4 – A phishing subdomain targeting Outlook hosted in a web.app domain

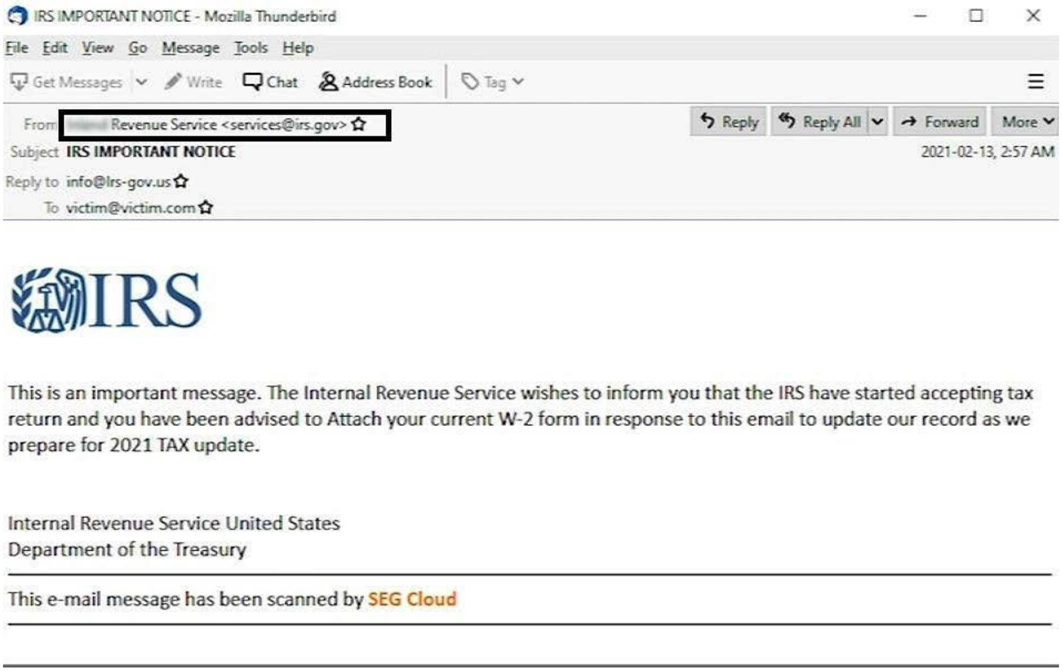
As you can see, an attacker developed an HTML phishing file impersonating the Microsoft Outlook login page and hosted it on a subdomain of the `web.app` domain.

Now that you are familiar with most attackers' techniques to bypass the email security solutions deployed on a victim environment, let us see some attacker techniques to trick the victim into listing their email as a trusted email and interacting with its contents.

Social engineering techniques to trick the victim

Now, after bypassing the email security controls, an attacker will trick the victim into listing their email as a trusted email and interacting with its content, such as executing attachments or browsing URLs. To trick the victim into interacting with the attacker's email as a trusted mail, the attacker conducts some social engineering techniques. **Social engineering** is when an attacker accomplishes malicious activities by tricking the victim into performing human interactions – for example, executing malware, entering credentials into phishing URLs, spreading malware by sending it to their colleagues, and providing sensitive information. There are several techniques used by attackers to conduct successful social engineering attacks, as listed here in detail:

- **Email spoofing**: As discussed previously, email spoofing is a technique used in email attacks to trick recipients into thinking a message came from an email sender other than the attacker. For example, think about an attacker targeting a victim who is an employee at ABC Bank; during the reconnaissance phase, the attacker knew that there was business between ABC Bank and another local bank called XYZ Bank. When sending a phishing email to the victim, the attacker spoofs the XYZ Bank email domain address to trick the victim into thinking that the email is trustworthy and related to the business. Hence, they will comfortably interact with the email contents (see *Figure 1.5*).


IRS IMPORTANT NOTICE - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
IRS

From [redacted] Revenue Service <services@irs.gov>
Subject IRS IMPORTANT NOTICE
2021-02-13, 2:57 AM
Reply to info@lrs-gov.us
To victim@victim.com

This is an important message. The Internal Revenue Service wishes to inform you that the IRS have started accepting tax return and you have been advised to Attach your current W-2 form in response to this email to update our record as we prepare for 2021 TAX update.

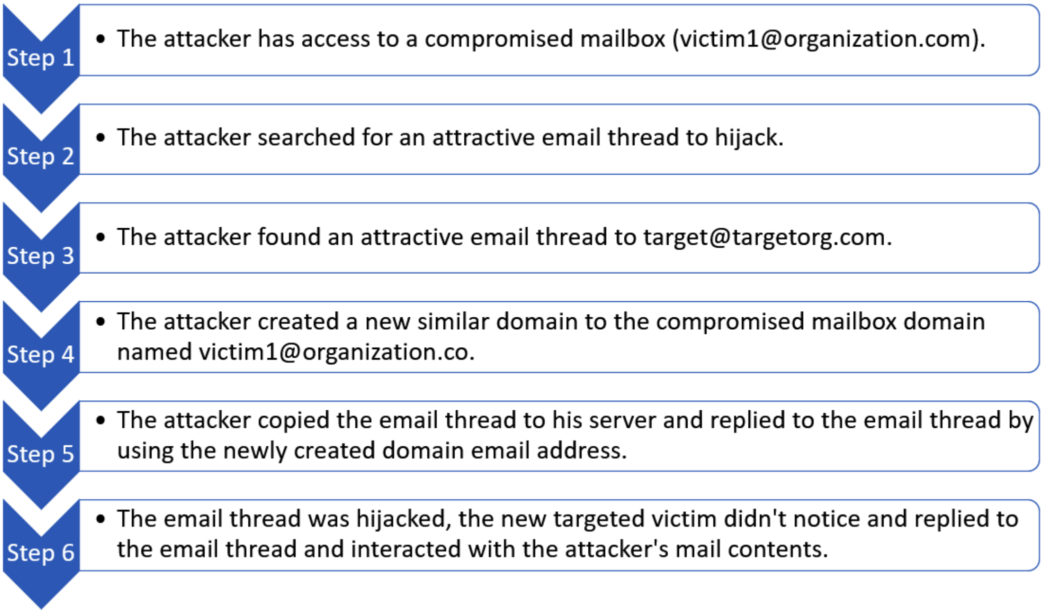
Internal Revenue Service United States
Department of the Treasury

This e-mail message has been scanned by SEG Cloud

Figure 1.5 – Spoofing an IRS domain to send a phishing email (ABC7 Chicago)

As you see in the preceding screenshot, the attacker spoofed the US government **Internal Revenue Service** (**IRS**) domain to send a phishing email to their victims.

- **Email thread hijacking**: Email thread hijacking occurs when an attacker takes control of an existing email conversation between a compromised user and another target victim by replying to the email thread using a newly created email domain that looks similar to the compromised company's domain. This makes it difficult for the new target victim to spot the difference between the two domains, and they continue the thread without suspicion. For example, an attacker may gain access to `organization.com` by compromising the `victim1@organization.com` mailbox. The attacker then spots an email thread between the compromised email address and the target company's email address, `target@targetorg.com`. Using their access to the compromised victim mailbox, the attacker copies the email thread to his external server and replies to the thread, using a newly created domain email address similar to the compromised organization, such as `victim1@organization.co`. The attacker then asks the targeted user to perform some actions, such as changing bank account information, transferring money, providing sensitive information, or executing attachments. This way, the attacker hijacks the email thread between `victim1@organization.com` and `target@targetorg.com` for their newly created domain email address, `victim1@organization.co` (see *Figure 1.6*).



Step 1
- The attacker has access to a compromised mailbox (victim1@organization.com).

Step 2
- The attacker searched for an attractive email thread to hijack.

Step 3
- The attacker found an attractive email thread to target@targetorg.com.

Step 4
- The attacker created a new similar domain to the compromised mailbox domain named victim1@organization.co.

Step 5
- The attacker copied the email thread to his server and replied to the email thread by using the newly created domain email address.

Step 6
- The email thread was hijacked, the new targeted victim didn't notice and replied to the email thread and interacted with the attacker's mail contents.

Figure 1.6 – The steps of email thread hijacking

Attackers usually utilize the email thread hijacking technique in a BEC attack, a type of social engineering attack where the attacker targets a specific individual within another company with whom the victim has an established business relationship, often someone who has access to financial information. The attacker then poses as the legitimate business entity, using similar email domains, and sends a convincing email requesting a change in payment instructions, such as instructing the victim to transfer funds to a new bank account number.

- **Hosting phishing pages on trusted websites that issue an SSL certificate**: When a normal user is asked to enter their credentials on a website, the first thing they do is to check for the green padlock symbol. If the padlock exists, the user assumes that it's safe to interact with the website and enters their credentials. Knowing this, attackers can host a phishing URL on trusted websites that issue SSL certificates for web communications with the end user, such as dynamic DNS domains or cloud applications that host domains (e.g., `appspot.com` and `web.app` domains), to trick the victim.

Now that you are familiar with some attacker techniques to trick victims into listing their email as a trusted email and interacting with its content, let's move on to analyze secure email gateway logs.

The anatomy of secure email gateway logs

Email gateway security is a security solution that checks and analyzes every email, including its content, sent from external email addresses to internal email addresses and vice versa. Such an inline position allows email security controls to have visibility of all emails sent and received, which makes its logs very valuable during threat detection and investigations.

Email security solutions typically provide several types of logs to help organizations monitor and analyze email activity. Here are some common types of logs:

- **SMTP logs**: These logs contain information about the delivery of emails via the **SMTP**, including information such as the sender's IP address, recipient's email address, and timestamps
- **Message tracking logs**: These logs provide detailed information about the email messages that pass through the email security solution, including metadata such as message ID, sender, recipient, subject, and date/time
- **Content filtering logs**: These logs record information about any content filtering rules that were applied to an email message, including the nature of the content and whether it was blocked or allowed
- **Spam and malware logs**: These logs contain information about any emails that were flagged as spam or detected as containing malware by the email security solution
- **Quarantine logs**: These logs contain information about any emails that were quarantined by the email security solution, including metadata about the message and the reason it was quarantined

During this section, we will discuss and analyze the most common log fields that are generated and exist in all security email gateways, regardless of product name or vendor:

- **SMTP server IP**: An SMTP server IP is the IP used by a sender to send an email to a recipient. We can use it to observe any backlisted SMTP server IPs sending us an email or to check for a spoofing presence, as we will see later.

- **Sender email address**: The sender email address is the address used to send an email to the recipient. We can use it to observe whether we received an email from a blacklisted domain. It's also important to consider that this email address could be spoofed by an attacker to trick the victim.
- **Recipient email address**: The recipient's email address is the address that will receive the email in their mailbox from the sender. If there is a cyber incident where a phishing email is distributed to recipients, we can use it to scope the potentially infected users and machines.
- **Email subject**: The email subject is a field in an email message that typically describes the content of the message or its purpose. It is entered by the email sender when composing the email and is usually displayed prominently in the recipient's email client. Attackers usually use motivational phrases in the email subject to encourage their victims into interacting with the email content. For instance, they may use phrases such as **Urgent Action Required**, **Confirm your Account Details**, or **Unauthorized Access Attempt**. Also, it's crucial to check any suspicious emails that have an irrelevant subject that does not align with the recipient's interests or job role. For instance, it is unusual for an accountant to receive an email with a subject related to IT courses, so such emails should be treated with caution.
- **Attached filename**: If the email sender attached files to the email sent to the recipient, the attachment filename appears in this log field. We mentioned previously the most common phishing attachment types used by attackers to gain initial access to the victim's machine. The correlation between the list of file types used in phishing attacks and attractive filenames that attackers usually use to encourage a user into opening a malicious file (for example, `Purchase order`, `Important note`, and `Invoice`) will help you detect the spearphishing attachment emails.
- **Attached file hash**: Some email gateway security solutions provide a hash value of every file attached in the email passed through it. Some of them provide a hash value when the attached file is detected as malicious, and some of them do not provide a file hash under any conditions. Regardless of the file hash type provided by the secure email gateway solution, you should find one provided. You can hunt for a malicious email passed to recipients by extracting a list of the file hashes provided by email security, executing the list against a threat intelligence feed database, such as the VirusTotal platform, where a script can be utilized.
- **Malware category**: This log field will only appear when the email gateway security's malware signature database matches any file passed through it. The malware category field will provide the malware family (ZLoader, a Trojan Word document, RedLine Infostealer, etc.).
- **Attached URL**: If an email contains any URL in the email body, it will be provided in this log field. Some appliances log every URL contained in the email body, and some appliances just log the URL when a match occurs between the attached URL and one in the malicious URL database of the email gateway.
- **Device action**: The device action is the action that the email security appliance takes regarding the sent email. The value of this log field helps a security analyst to determine whether a malicious mail was successfully passed to the end user or not.

- **Block reason**: When an email is blocked by the email gateway, the blocking reason will be provided to you in this log field.

Now that we are familiar with the most common possible log fields in all email security gateway logs, let us learn how to investigate suspicious emails.

Investigating suspicious emails

Investigating suspicious emails is the process of investigating every digital evidence related to an email, such as the email appliances log attributes, email body content, email sender behavior, analyzing the email header (as we will see in the next chapter), and investigating the attachments (either a file or URL). We will divide our investigation of the suspicious email process into subsections. In each one, we will try to confirm whether an email is either malicious or benign. To do such confirmation, you will need to follow all the investigation subsections, even if you felt during any subsection that you were sure about the email classification as either malicious or benign.

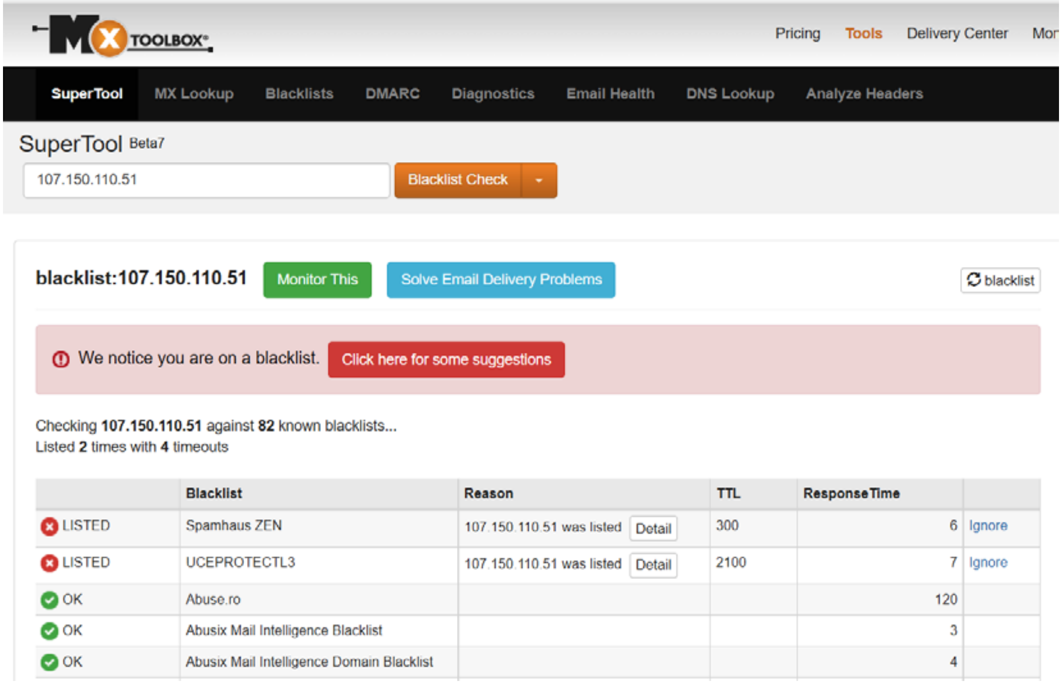
We will be discussing the following topics in the sub sections:

- Investigating the email sender domain and SMTP server reputation
- Spoofing validation
- Email sender behavior
- Email subjects and attached filenames
- Investigating suspicious email content

Investigating the email sender domain and SMTP server reputation

While investigating suspicious and unusual emails, a useful initial step is to examine the reputation of the email sender domain by conducting a search engine query, such as on Google. By researching the domain's reputation, you may find several threat reports, articles, and threat tweets, indicating that the email sender domain is a well-known malicious email sender domain that is currently used by an active threat actor to deliver spearphishing emails. Alternatively, you may find the email sender domain is related to an organization that your organization may do business with and the email seems legit. Also, you may not find any results of the email sender domain and find it was recently created, which makes the email even more suspicious, as most attackers now find it easy and cheap to create a new domain with a non-malicious history to send phishing emails. However, it's important to note that conducting a search engine query on the email domain is only an initial step and does not provide a confirmation of whether the email is malicious or not. It's also worth considering that attackers may use public mail domains such as Gmail or Yahoo for spearphishing emails, due to their easy account creation and non-malicious history reputations.

One of the most popular online tools that you can use to check whether a specific domain sender or sender SMTP IP is blacklisted due to its reputation is MxToolbox (`https://mxtoolbox.com/`). The tool allows you to check the suspicious email sender domain or the sender SMTP server IP against **82** known blacklists (see *Figure 1.7*).



blacklist:107.150.110.51

We notice you are on a blacklist. Click here for some suggestions

Checking **107.150.110.51** against **82** known blacklists...
Listed **2** times with **4** timeouts

	Blacklist	Reason	TTL	ResponseTime	
☒ LISTED	Spamhaus ZEN	107.150.110.51 was listed Detail	300	6	Ignore
☒ LISTED	UCEPROTECTL3	107.150.110.51 was listed Detail	2100	7	Ignore
✓ OK	Abuse.ro			120	
✓ OK	Abusix Mail Intelligence Blacklist			3	
✓ OK	Abusix Mail Intelligence Domain Blacklist			4	

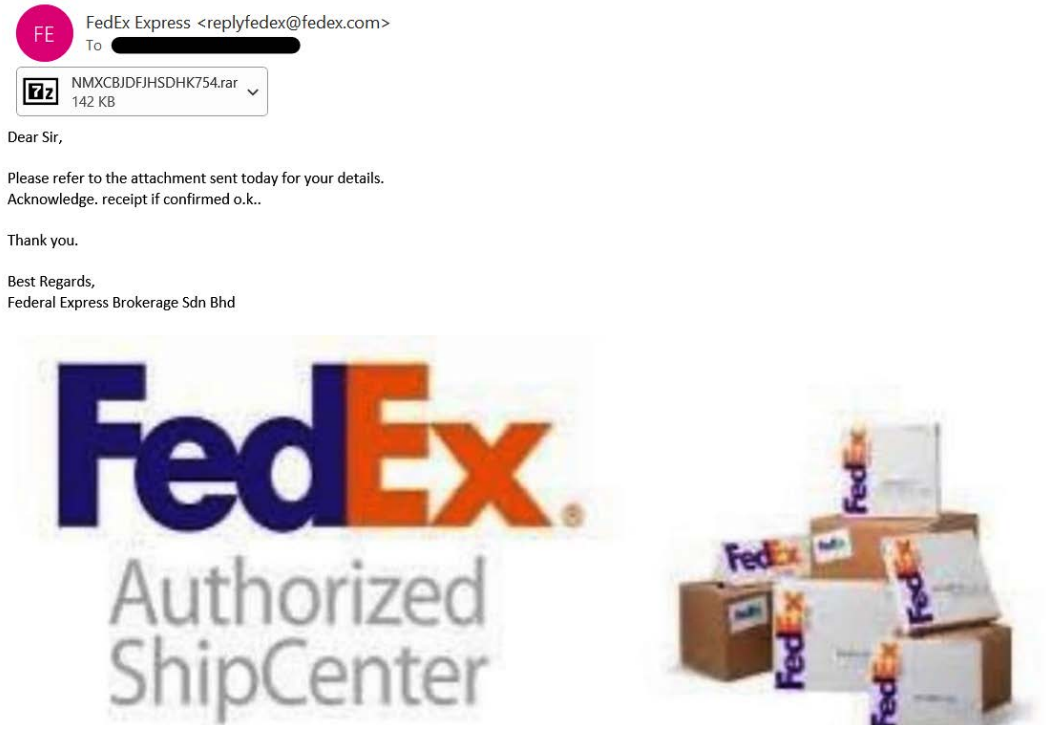
Figure 1.7 – Checking a suspicious sender IP on MxToolbox blacklists

As you can see in the preceding screenshot, I checked a suspicious sender SMTP server IP, as we can check suspicious email sender domains also as well. After checking the IP against the 82 blacklists, we found it blacklisted on two lists, which indicates that it has a history of sending malicious emails.

Spoofing validation

During the previous subsection, we discussed that you may find an email sent from a legit organization domain address that your organization has business with. However, as we mentioned before, the attacker can spoof a legit domain email address to trick a user into interacting with their email content. Hence, if we identified during the previous subsection that the Email sender domain is related to a legit organization, we have to validate that the sender domain is not spoofed by the attacker. We will learn how to check and investigate the presence of spoofing during our analysis of email headers in the next chapter, but you will not always have an email header to analyze; hence, we will try to check the presence of spoofing instead by using the email security appliance logs.

To check for spoofing attempts, we will try to validate whether an email sender domain sent an email from its authorized SMTP server IP or not. For example, in the screenshot in *Figure 1.8*, the email sender claims to have sent the email from an email address associated with the legitimate domain `fedex.com`. To validate this, we extracted the sender's SMTP server IP by analyzing the email security appliance logs and identified that the email was sent from the `95.211.214.81` SMTP server IP address.



FE FedEx Express <replyfedex@fedex.com>
To [redacted]

NMXCBJDFJHSDHK754.rar
142 KB

Dear Sir,

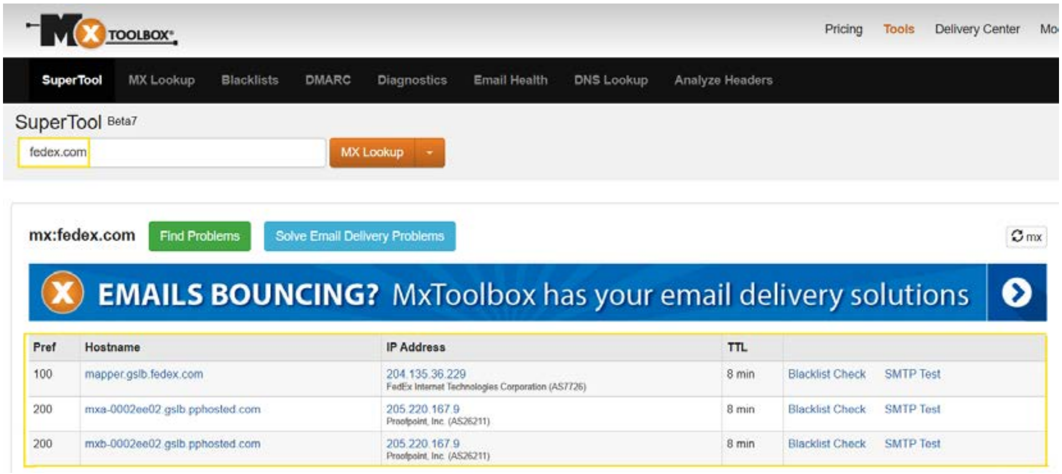
Please refer to the attachment sent today for your details.
Acknowledge. receipt if confirmed o.k..

Thank you.

Best Regards,
Federal Express Brokerage Sdn Bhd

Figure 1.8 – A suspicious email, sent from an email sender who claims to be a member of the FedEx domain

To investigate whether the email sender spoofed the `fedex.com` domain to send this email, we will use MxToolbox to check the MX record of the `fedex.com` domain to verify the authorized and acceptable SMTP servers that send emails on behalf of the `fedex.com` domain. While the primary objective of MX servers is to receive emails sent to specific domain recipients, as we will see in the next chapter, I have observed that many domains also utilize their MX servers to send emails to external recipients. To check the domain MX record, open the MxToolbox MX lookup URL (`https://mxtoolbox.com/MXLookup.aspx`), then enter the domain that you need to verify, and press *Enter* (see *Figure 1.9*).

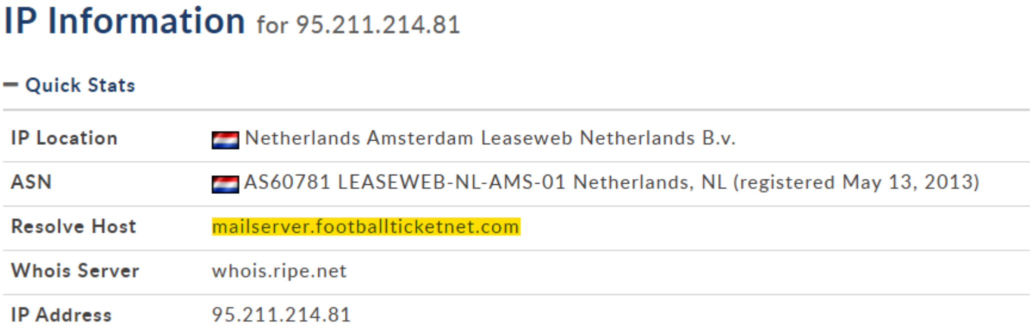


Pref	Hostname	IP Address	TTL	
100	mapper.gslb.fedex.com	204.135.36.229 FedEx Internet Technologies Corporation (AS7726)	8 min	Blacklist Check SMTP Test
200	mxa-0002ee02.gslb.pphosted.com	205.220.167.9 Proofpoint, Inc. (AS26211)	8 min	Blacklist Check SMTP Test
200	mxb-0002ee02.gslb.pphosted.com	205.220.167.9 Proofpoint, Inc. (AS26211)	8 min	Blacklist Check SMTP Test

Figure 1.9 – Checking an MX record FedEx domain

As you see in the preceding screenshot, we checked the MX record to verify the authorized SMTP servers to send emails on behalf of the `fedex.com` domain and found that the authorized servers are `mapper.gslb.fedex.com`, `mxa-0002ee02.gslb.pphosted.com`, and `mxa-0002ee02.gslb.pphosted.com`, and their corresponding IPs. You can also see in the preceding screenshot that there are multiple MX records with different preference values. The preference value is the way of setting the priority of each MX record. The lowest preference is the MX server with the highest priority – that is, the first one that a sending mail server should attempt to use.

On the other hand, in the email gateway security appliance logs, the SMTP server that sent the email is the `95.211.214.81` IP. To verify whether this IP is related to one of the three aforementioned authorized SMTP servers or not, we checked the WHOIS record of the IP and found it was not related to any of them, which means the attacker used an unauthorized SMTP server to spoof the `fedex.com` domain to scam the recipients (see *Figure 1.10*). To check the IP Whois record, we used the Domain Tools platform (`https://whois.domaintools.com/`).



IP Location	Netherlands Amsterdam Leaseweb Netherlands B.v.
ASN	AS60781 LEASEWEB-NL-AMS-01 Netherlands, NL (registered May 13, 2013)
Resolve Host	mailserver.footballticketnet.com
Whois Server	whois.ripe.net
IP Address	95.211.214.81

Figure 1.10 – The 95.211.214.81 Whois record

Now, you should have the basic information to determine whether the email was spoofed or sent from a known malicious source. In the next subsection, we will explain how to observe suspicious email sender behavior.

Email sender behavior

Let's suppose that the previous two investigation steps show that the email sender domain and its SMTP server are not blacklisted, and the email sender domain of the suspicious email has not been spoofed and is related to a company that your organization may have business with. Now, you may be confused because the email seemed suspicious but your investigations show that everything is normal. To make a decision on this, we need to check the email sender behavior by checking the following:

- Have the recipient/s received emails from the email sender or its domain before? If there is a history of receiving emails from the same sender or domain, then it could be considered normal email communication between the parties.
- Check whether the email sender sent emails using the same email subject formula to several recipients from different departments. If so, it's highly likely to be a phishing campaign or spam emails sent to random users in your organization.
- Check whether the sent mail subject seems related to the employee's job duties or not – for example, if an accountant employee received an email with a subject indicating IT stuff, that's maybe an indicator of spam or a phishing email sent by an attacker who has not conducted prober reconnaissance activities.

All previous checks and email characteristics may indicate legitimate emails sent from a legitimate sender without any malicious content, or they may also be a legitimate organization compromised by an attacker who is trying to gather new victims by utilizing the trusted relationship between the current victim and the new targets. To determine which of the two situations is the case, you will need to analyze the email content, as we will see later.

Email subject and attached filename

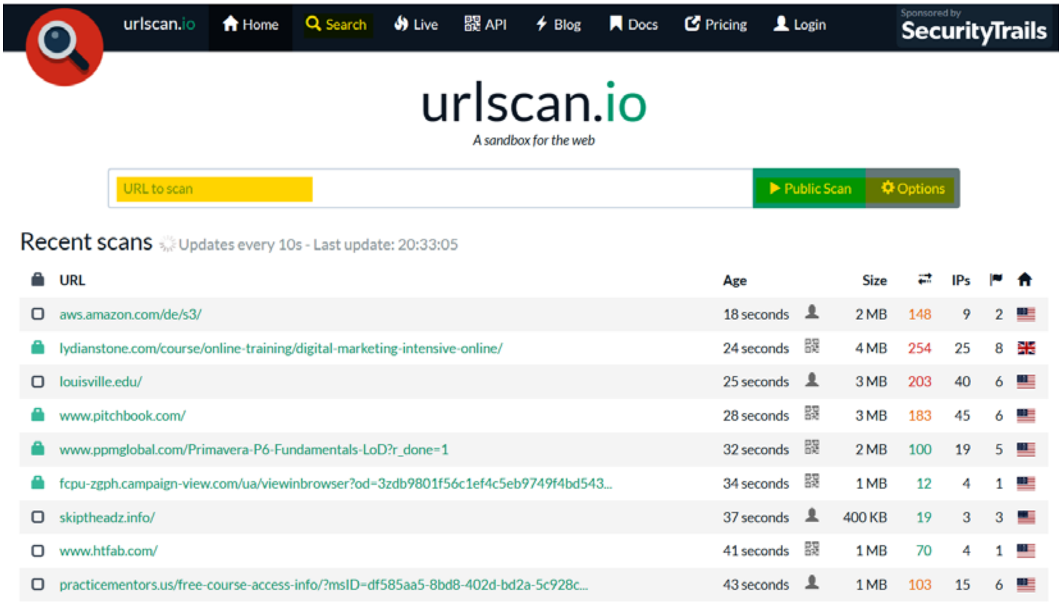
The email subject and attached filename usually refer to the email content. When investigating suspicious emails from email security log properties, try to observe the most common attacker keywords used in the subject lines of phishing emails, such as **RE:**, **FW:**, **Invoice**, **Missing Inv**, **New Message from**, **New scanned**, **You have a New Message**, **New message from**, **Verification Required**, and **Action Required**. Also, attackers use common keywords in filenames, such as **invoice**, **order**, **contract**, **payment**, **offer**, **planning**, and **SWIFT**. All these keywords are used by an attacker to encourage and trick the victim into interacting with the email content.

Investigating suspicious email content

As you may know, the main objective of phishing emails is to convince the victim into interacting with malicious email contents, such as malicious attachment files, phishing URLs, or forms to harvest the victim's information. Hence, to accurately classify an email as malicious or benign, the best option is to carefully examine its contents, including any attached files or URLs; to do so, we will depend on two online tools – the **URL scan** tool to analyze the suspicious URLs and the **ANY.RUN** sandbox to analyze the suspicious files.

URL analysis by using the URL Scan platform

As previously mentioned, attackers can send phishing URLs to victims in an attempt to harvest their credentials or download malware onto their machines. In this section, our investigation will focus on identifying and analyzing URLs used for credential harvesting, utilizing the URL Scan platform (`https://urlscan.io/`). URL Scan is a powerful platform that allows users to investigate suspicious URLs, in both public and private modes. Public submissions can be viewed by other visitors, while private submissions are only visible to the user who submitted them. Additionally, the platform provides a searchable database of historical URL submissions for those that were scanned using the public scan mode (see *Figure 1.11*).



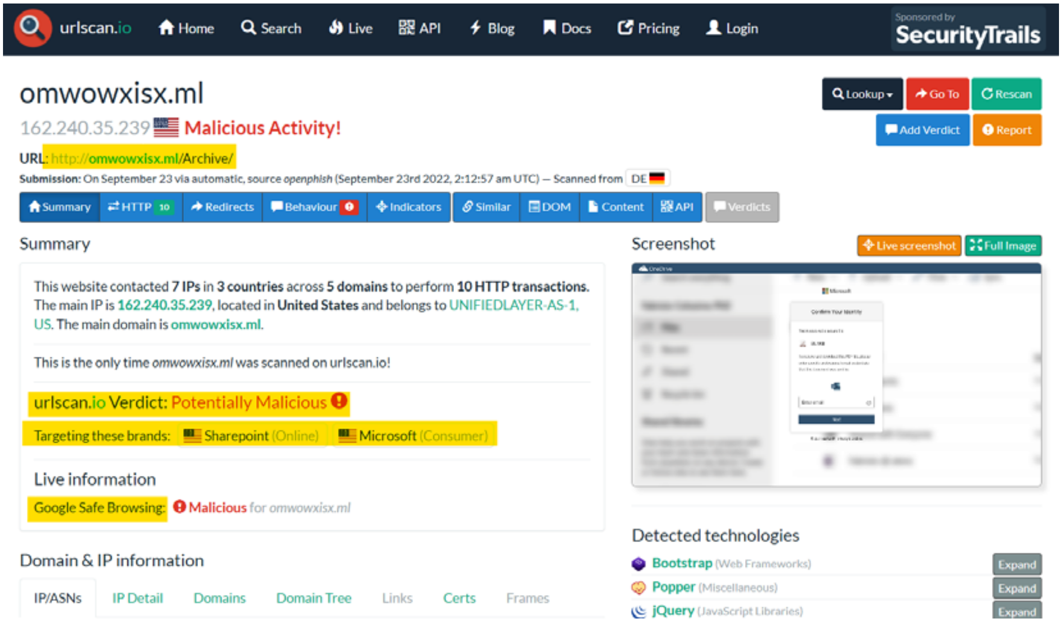
Recent scans Updates every 10s - Last update: 20:33:05

🔒	URL	Age		Size	⇄	IPs	🚩	🏠
□	aws.amazon.com/de/s3/	18 seconds	👤	2 MB	148	9	2	🇺🇸
🔒	lydianstone.com/course/online-training/digital-marketing-intensive-online/	24 seconds	▦	4 MB	254	25	8	🇬🇧
□	louisville.edu/	25 seconds	👤	3 MB	203	40	6	🇺🇸
🔒	www.pitchbook.com/	28 seconds	▦	3 MB	183	45	6	🇺🇸
🔒	www.ppmglobal.com/Primavera-P6-Fundamentals-LoD?r_done=1	32 seconds	▦	2 MB	100	19	5	🇺🇸
🔒	fcpu-zgph.campaign-view.com/ua/viewinbrowser?od=3zdb9801f56c1ef4c5eb9749f4bd543...	34 seconds	▦	1 MB	12	4	1	🇺🇸
□	skiptheadz.info/	37 seconds	👤	400 KB	19	3	3	🇺🇸
□	www.htfab.com/	41 seconds	▦	1 MB	70	4	1	🇺🇸
□	practicementors.us/free-course-access-info/?msID=df585aa5-8bd8-402d-bd2a-5c928c...	43 seconds	👤	1 MB	103	15	6	🇺🇸

Figure 1.11 – The URL Scan platform main view

As you see in the preceding screenshot, upon opening the URL Scan platform, this is the primary view that appears. Also, note that I have highlighted the most interesting features, such as the **Search** button that allows you to search in the submissions history of URLs scanned in the public mode, the URL submissions bar that allow you to submit the URL to scan, and the current scan mode. As you can see, you are in public scan mode by default; to explore the possible custom configurations and to switch to private scan mode, you can click on the **Options** button.

Now, let us assume that you are investigating a suspicious URL sent over email to a recipient who is an employee at your organization. The suspicious URL is `hxxp[:]//omwowxisx[.]ml/Archive/`. To analyze this URL, we just need to copy and paste it into the submission bar (**URL to scan**) and press the *Enter* button (see *Figure 1.12*).



omwowxisx.ml

162.240.35.239 Malicious Activity!

URL: http://omwowxisx.ml/Archive/

Submission: On September 23 via automatic, source *openphish* (September 23rd 2022, 2:12:57 am UTC) — Scanned from DE

Summary

This website contacted **7 IPs** in **3 countries** across **5 domains** to perform **10 HTTP transactions.** The main IP is **162.240.35.239**, located in **United States** and belongs to **UNIFIEDLAYER-AS-1, US**. The main domain is **omwowxisx.ml**.

This is the only time *omwowxisx.ml* was scanned on urlscan.io!

urlscan.io Verdict: Potentially Malicious

Targeting these brands: Sharepoint (Online) Microsoft (Consumer)

Live information

Google Safe Browsing: Malicious for *omwowxisx.ml*

Domain & IP information

Screenshot

Detected technologies

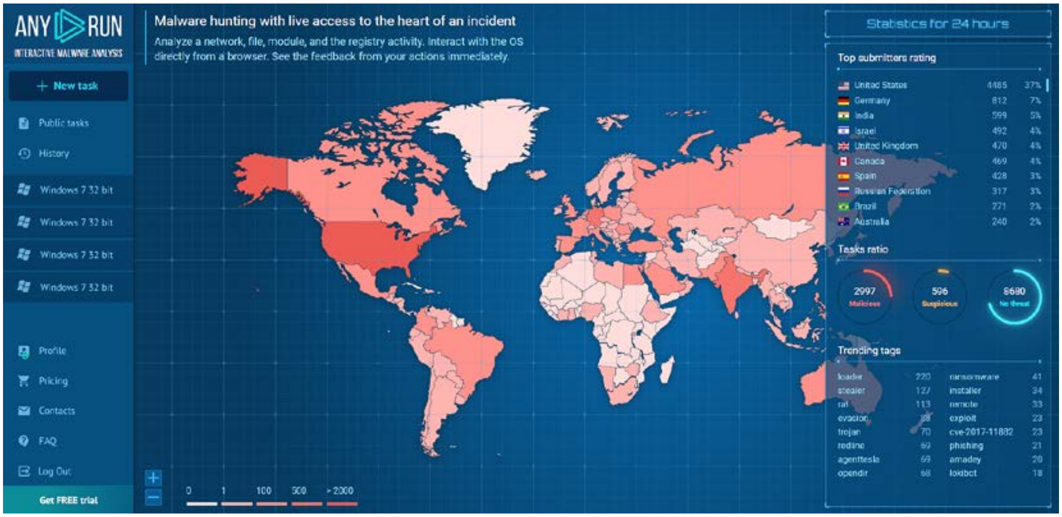
Bootstrap (Web Frameworks)
Popper (Miscellaneous)
jQuery (JavaScript Libraries)

Figure 1.12 – An analysis of suspicious URLs using URL Scan

As you can see in the preceding screenshot, the investigation of the suspicious URL resulted in the URL being a malicious and phishing one. And as you see in the targeted brands section, this phishing URL targets the SharePoint and Microsoft brands to harvest their users' credwentials. If you were investigating a phishing URL and found the target brand is your organization brand, the attacker may use your organization logo and its login page to harvest the organization's employee credentials. If so, you need to know that your organization and employees are under attack by a threat actor.

File analysis by using the ANY.RUN sandbox

As we mentioned before, an attacker may send a spearphishing email containing a malicious file to the victim to gain an initial foothold in their machine and environment. In this section, we will learn how to analyze and investigate suspicious files by using an online sandbox platform called ANY.RUN (`https://app.any.run/`). ANY.RUN is an online interactive malware sandbox that presents a virtual machine interface, which can be controlled in real time and perform file analysis. ANY.RUN allows you to submit both files and URLs to interactively analyze them (see *Figure 1.13*).



Malware hunting with live access to the heart of an incident

Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.

Top submitters rating

United States	4485	37%
Germany	812	7%
India	599	5%
Israel	492	4%
United Kingdom	470	4%
Canada	469	4%
Spain	428	3%
Russian Federation	317	3%
Brazil	271	2%
Australia	240	2%

Tasks ratio

2997 Malicious
596 Suspicious
8680 No threat

Trending tags

loader	220	ransomware	41
stealer	127	installer	34
rat	113	remote	33
evasion	88	exploit	23
trojan	70	cve-2017-11882	23
rodinc	69	phishing	21
agenttesla	69	amadey	20
opendir	68	lokibot	18

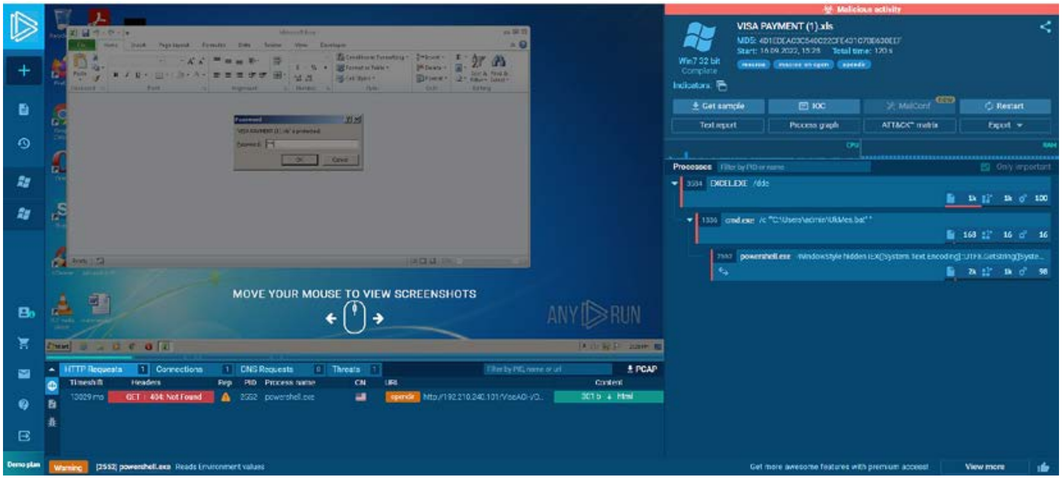
Figure 1.13 – The main view of the ANY.RUN online sandbox

As you can see in the preceding screenshot, in the upper left of the main view of the ANY.RUN sandbox platform, there is a **New task** button, which allows you to submit either a file or URL for analysis. Under the **New task** button, we find **Public tasks**, which allows you to view the history of all users' submitted tasks, analyzed in public mode. Also, you are able to search this history data by using some filters, such as file extension, submission country, and tags. The **History** button allows you to view your account submission history. On the right, you will find statistics of the submissions, such as the top submitting country and trending tags.

Important note

To prevent unintentionally becoming involved in a data leakage incident, it is recommended to refrain from submitting any potentially suspicious attachment files that may contain sensitive information about your organization or its business to any cloud sandbox or analysis tools.

To analyze a suspicious file on ANY.RUN, click the **New task** button, choose to upload a file, and then upload the suspicious file for analysis. In this case, we will analyze a Microsoft Office document file type, which is the most used file type in spearphishing attacks to gain initial access to the victim's machine. The file that we will analyze is named `VISA PAYMENT (1).xls` (see *Figure 1.14*).



3584 EXCEL.EXE /dde

1336 cmd.exe /c "C:\Users\admin\UkMes.bat"

2552 powershell.exe -windowstyle hidden IEX([system.text.encoding]::UTF8.GetString([syste...

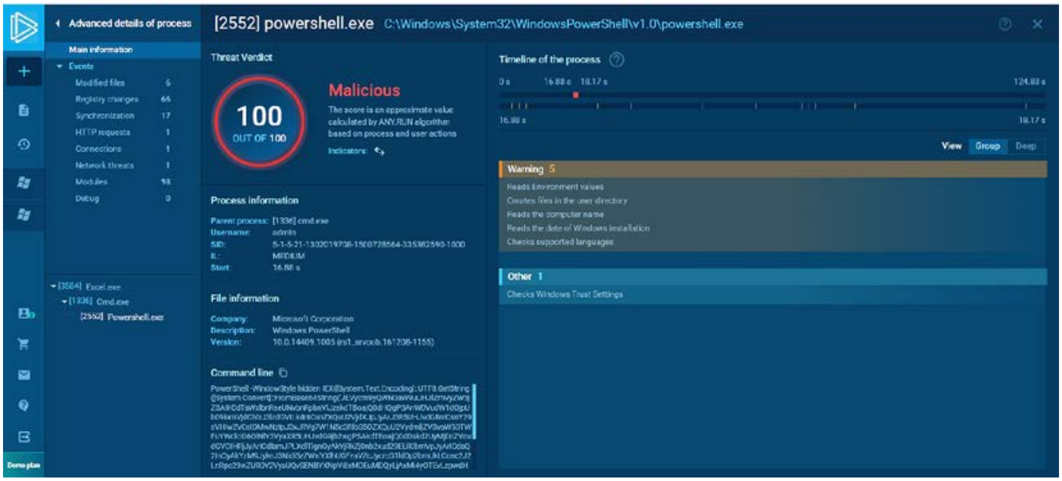
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
13029 ms	GET 404: Not Found	⚠	2552	powershell.exe		opendir http://192.210.240.101/VisaAD-VO...	301 b ↓ Html

Warning [2552] powershell.exe Reads Environment values

Figure 1.14 – Analyzing a suspicious file using the ANY.RUN sandbox

As you see in the preceding screenshot, we submitted the `VISA PAYMENT (1).xls` file for analysis on ANY.RUN. As you can see, the file is encrypted by a password that is shared with the victim through the email body. After submitting the file, ANY.RUN will allow you to interact with the file and the virtual machine desktop as if it were opened on a regular machine. Upon the opening of the `excel.exe` process that is responsible for opening the Excel sheets, a `.bat` file named `UkMes.bat` is dropped on the disk under the user profile path, then the Excel process spawned the `cmd.exe` process to execute the dropped `UkMes.bat` file. After the execution of the `.bat` file, the `cmd.exe` process spawned the `powershell.exe` process with a long command argument that is not visible in the main view. Hence, we need to explore the `powershell.exe` details to be able to see and analyze its command-line argument. Before that, I just want you to pay attention to the details bar in the preceding screenshot of the VM machine where you will see several tabs. **HTTP Requests** shows you whether any process during submission initiated HTTP requests to external servers with great details, such as the reputation of the remote server, the process name, and the URL. As you can see in the **HTTP Requests** tab, `powershell.exe` performed suspicious communications to external malicious servers to download binaries. The **Connections** tab shows you that all connections initiated from the machine to external servers including the same details that exist in the **HTTP Requests** field. The **DNS Request** tab contains all the DNS queries initiated from the machine during file submission to external servers. Finally, the **Threats** field shows you that the IDS signatures match with the process network communication packets.

Now, let us explore the PowerShell process details by clicking on the **PowerShell.exe** bar and then **More Info** to see and analyze the full `powershell.exe` command-line argument and its behavior (see *Figure 1.15*).



[2552] powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Threat Verdict

100 OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Parent process: [1336] cmd.exe
Username: admin
SID: S-1-5-21-1302019708-1500728564-335382590-1000
IL: MEDIUM
Start: 16.88 s

File information

Company: Microsoft Corporation
Description: Windows PowerShell
Version: 10.0.14409.1005 (rs1_srvoob.161208-1155)

Command line

```
PowerShell -WindowStyle hidden IEX([System.Text.Encoding]::UTF8.GetString
([System.Convert]::FromBase64String( [illegible]
```

Timeline of the process

0 s 16.88 s 18.17 s 124.83 s

16.88 s 18.17 s

Warning 5
Reads Environment values
Creates files in the user directory
Reads the computer name
Reads the date of Windows installation
Checks supported languages

Other 1
Checks Windows Trust Settings

Figure 1.15 – Exploring the powershell.exe details

As you can see in the preceding screenshot, after exploring the `powershell.exe` process details, we find that the calculated threat score of the process is 100 out of 100, which means that the process behavior is malicious. While the Windows interpreter executable itself is legitimate, the command-line argument used in this case is malicious. As you can see in the screenshot, the argument consists of `base64`-encoded characters that cannot be easily analyzed, which is a strong indicator of malicious activity. To decode the encoded command, we can depend on an online platform called **CyberChef** (`https://gchq.github.io/CyberChef/`). Also, note the process behaviors on the right of the screenshot; as you can see, there are categories of the behaviors, such as the **Warning** level, that show the process tried to discover the machine computer name, language, and installation date, which is usually considered an initial discovery activity by a threat actor.

Summary

In this chapter, we explored the most common attack vectors used by hackers to gain an initial foothold in victim environments, with a particular focus on email-based attacks. We reviewed the different types of email threats and discussed the techniques used by attackers to evade detection and trick their victims into interacting with malicious email content. Additionally, we delved into the anatomy of email secure gateway logs and provided insights on how to investigate email threats effectively.

In the next chapter, we will learn about email flow and header analysis.