Phishing Email Analysis

By Tariqul Islam
Cipher Shadow

Intro

Phishing Emails are a common attack that attackers send randomly large numbers of email to download malware or steal credentials.

In this document we will talk about Phishing email along phases of Cyber Kill Chain, what type of phishing email, Attacker technique and how to analyze it.

Phishing Email attack along phases of Cyber Kill Chain

1. Reconnaissance: Gather information about the target.
2. Weaponization: attacker crafts a phishing email designed to deceive recipients. This email typically contains malicious elements such as a link to a fake website, a malicious attachment, or a payload that exploits vulnerabilities.
3. Delivery: send mail to the target. Attackers often use various tactics to make the email appear legitimate, such as spoofing the sender's address or using social engineering techniques.
4. Exploitation: exploitation occurs when the recipient interacts with the malicious elements within the email.
5. Installation: the payload is installed on the victim's system. This could be malware, ransomware, or another type of malicious software.
6. Command And control: Once the attacker has control over the compromised system, they establish a command and control channel. This allows them to communicate with the infected device, exfiltrate data, or issue additional commands to further their objectives.
7. Action An Objective: With control over the compromised system, the attacker can now carry out their ultimate goals.

Phishing types

Phishing email attacks separate into to types:

1.Phishing: mass email attacks that are sent to a randomly large number of people.

2.Spear Phishing: Targeted form of phishing, Spear phishing have a multi type:

2.1.Spear Phishing Attachment: attacker sends office document, PDF, compressed file or image that have a malicious intent.

2.1.Spear Phishing URL: URL can install malware or steal credentials in such a way.

2.1.Black Email: where an attacker claims to have compromised the victim's machine and exfiltrated sensitive data and prove it by screenshot or spoofing victim's email address.

2.1.Business Email Compromise(BEC): Attacker targets a specific individual within a company who has access to financial information and uses it to send requests for wire transfers, access to sensitive data, or other financial transactions.

Attacker Techniques

Attackers are continuing to improve their techniques to evade email security detection, making it difficult for security systems to detect. Here are some common techniques attackers may use to avoid email security detection:

- Using newly created domains
- Used non-blacklist SMTP server
- Dynamic content generation
- Email spoofing
- Social engineering tactics
- Fileless malware
- Evasion through Encryption

Phishing Email Investigation

To investigate in Phishing Email we can use email security logs or we can use email header
We will discuss both:

1.Investigating Suspicious Emails using Email security logs

First we need to know what is the anatomy of Secure Email Gateway logs:

- TimeStamp
- SMTP server IP
- Sender Email
- Recipient Email
- Email subject
- Massage ID
- Action Taken
- Action reason
- Attachment information
- URL information
- Category

Now, what is investigation steps in details:

1.Investigating the Email sender domain and SMTP server reputation:

- Use (https://mxtoolbox.com/) to check Domain validation and look for the created date of the domain.
- Check if SMTP IP is blacklisted or not.

2.Spoofing Validation:

We need to validate that the sender domain is not spoofed by attacker

- Use(https://mxtoolbox.com/MXLookup.aspx) to check if the SMTP server is authorized or not.

3.Email subject and attached file or url:

- Check email subject if normal or have suspicious value like Action required, you have a massage.
- Use (https://urlscan.io/) to scan the attached URL.
- Use (https://any.run/) to scan the attached file.

These are the simplest steps to investigate using Secure Email Gateway.

But you should search in logs for how many people are targeted in your environment to create a full screen of this incident using src IP or domain or file hash in hosts.

2.Investigating Suspicious Emails using Email header:

First we need to know what is Email flow:

- Mail User Agent (MUA): that sends email like outlook, gmail or browser.
- Mail Submission Agent (MSA): the server that receive the email after client has submitted it from MUA
- Mail Transfer Agent (MTA): known as the SMTP relay server, this is an email server that maps email from sender to recipient.
- Mail Exchange (MX): the Email Server that is responsible for receiving messages intended for a particular domain that are sent and transferred from MTA to be delivered to recipients, MX is DNS record.
- Mail Delivery Agent (MDA): the server responsible for providing the user (recipient) with sent email after successful authentication.

We can divide Email header into four sections:
1.Email message content and metadata
2.Email X-header
3.Header that was added by hops
4.Email authentication

Below you can see the describe:

1. Email header and metadata:
    - Date: date and time when email is sent.
    - From: email address of the sender.
    - Return-path: contain sender address to return errors and reply messages.
    - To: recipient email address.
    - Message-ID: A unique identifier assigned to the email message, It helps in tracking and referencing specific emails.
    - Subject: subject line of message.
    - MIME-Version: (Multipurpose Internet Mail Extensions) used for encoding multimedia content within email.
    - Content-Type: specifies type of email content such as text, html, attachment,.....
    - Content-Transfer-Encoding: Defines the encoding method used to convert binary data into ASCII text for email transmission. Common values include "7bit," "8bit," and "base64".
    - Reference: Contains a list of message identifiers that this email is in reference to, creating a threaded view for email clients that support conversation tracking.

- **Content-Length:** size of the email's body in bytes.

2. Email X-headers:
   Email X-headers are custom headers that are added to the email header by the mailbox providers
   - **X-Mailer:** refers to the email client that used to send the email as MUA
   - **X-Originating-IP:** contains the IP address of the device that is the origin the IP

3. Header that are added by hops:
   We must have 3 headers added by MSA, MTA and MDA. These headers contain critical information such as the server's hostname, IP address, and timestamp for email processing.

4. Email authentication Protocols:
   These section contain critical 3 Records SPF, DKIM and DMARC
   - **SPF:** (Sender Policy Framework) is an email authentication protocol that helps prevent email spoofing by verifying that the sending mail server is authorized to send emails on behalf of a specific domain. SPF works by allowing domain owners to publish a policy in their DNS records, listing the authorized mail servers for sending emails. Receiving mail servers then check this SPF record during the email delivery process to ensure that the sending server is legitimate.

- DKIM: (DomainKeys Identified Mail) is a cryptographic email authentication method that uses public-key cryptography to sign outgoing emails. The sender's mail server generates a digital signature and attaches it to the email header. The recipient's mail server can then verify the signature by retrieving the sender's public key from the DNS records of the sender's domain. DKIM helps ensure the integrity of the email content and confirms that it has not been tampered with during transit.

- DMARC: (Domain-based Message, Authentication, Reporting and Conformance) is a policy framework that builds on SPF and DKIM to provide domain owners with greater control over email authentication. DMARC allows domain owners to publish a policy in their DNS records specifying how receivers should handle emails that fail SPF or DKIM checks. DMARC also enables domain owners to receive reports on email authentication failures, helping them monitor and improve their email security.