Official Incident Report

Event ID: 257

Rule Name: SOC282 - Phishing Alert - Deceptive Mail Detected

Table of contents

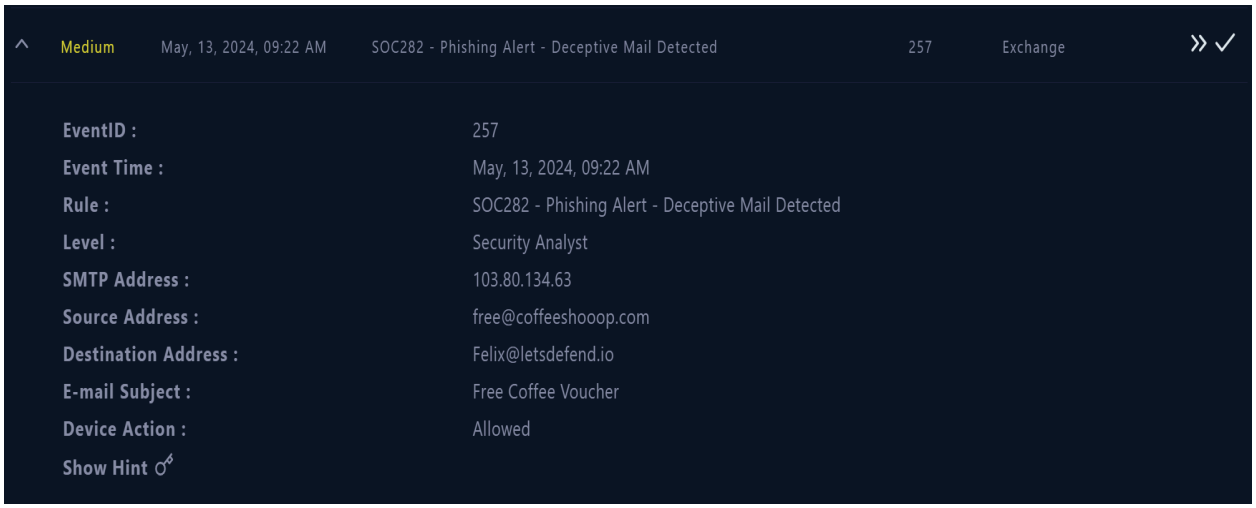
Official Incident Report **1**
Event ID: 257 1
Rule Name: SOC282 - Phishing Alert - Deceptive Mail Detected 1
Table of contents **2**
Alert **3**
Detection **4**
Analysis **7**
Containment **15**
Lesson Learned **16**
Remediation Actions **16**
Appendix **17**
MITRE ATT&CK 17
Artifacts 18

Alert

Based on the information that the alert provided, it seems that a suspicious link has been detected in an email sent to "**Felix**" from the email address "**free@coffeeshoop.com**" with the SMTP IP address **103.80.134[.]63**. The Alert is triggered by the **SOC282** rule **Phishing Alert - Deceptive Mail Detected**.

Adversaries may send phishing emails containing malicious attachments or links.

The device action is marked as "allowed", indicating that no action was taken by the Email security product to prevent or block the related mail.

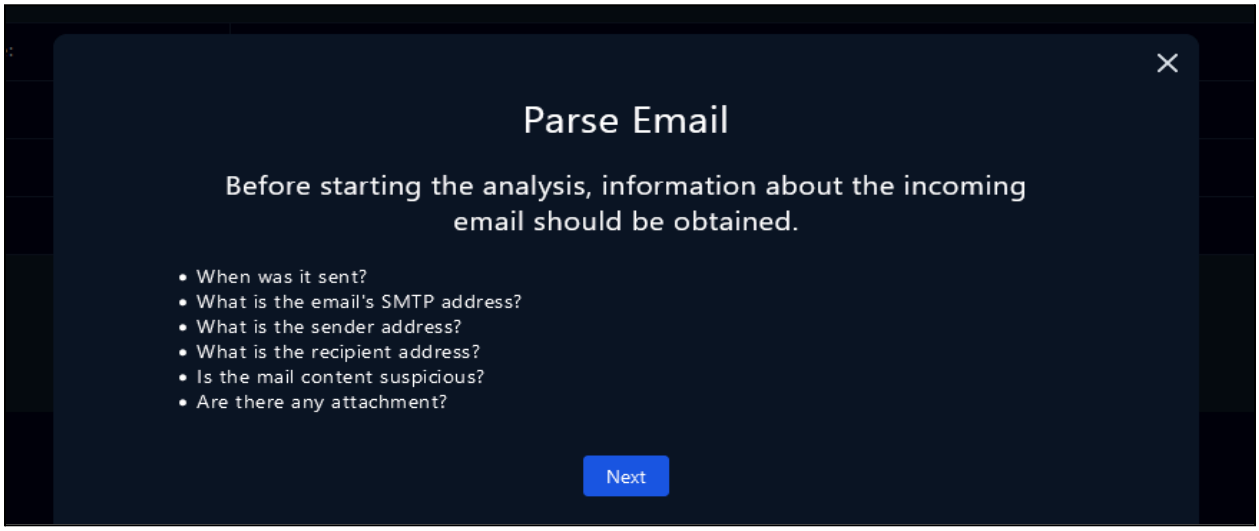


the email was sent to "**Felix**" on **May, 13, 2024, 09:22 AM**. The subject line of the email is "**Free Coffee Voucher**".

Overall, it appears that there may be **phishing** activity occurring on the network, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

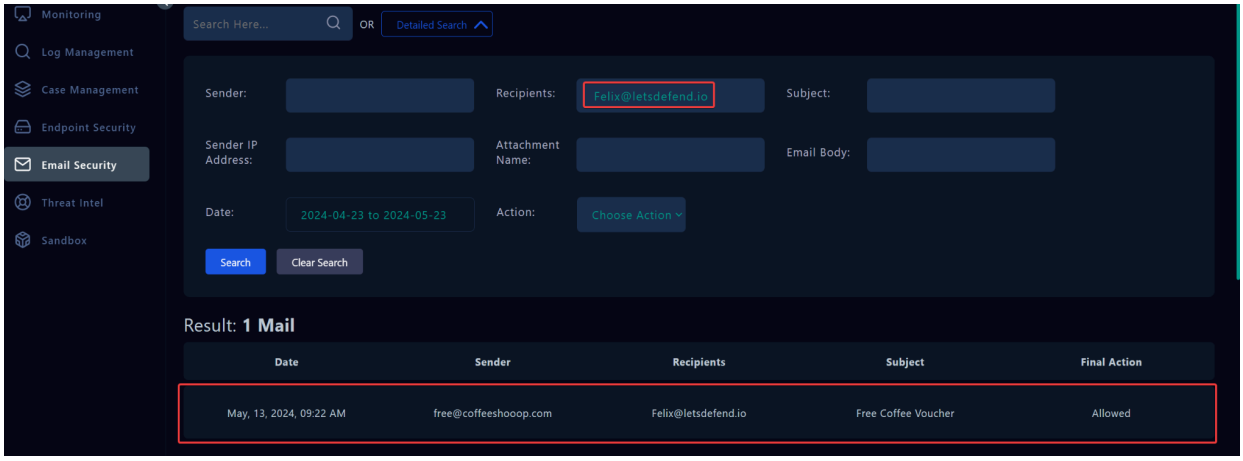
As the playbook suggests we can start investigating the alert by parsing email information.



The first step in the playbook is to gather information about the email. This includes:

- When was the email sent?
- What is the SMTP address of the email?
- What is the sender's email address?
- What is the recipient's email address?
- Is the content of the email suspicious?
- Are there any attachments in the email?

By answering these questions, we can gather more information about the email and determine whether it is a legitimate message or a phishing attempt. On the email security tab, we can simply filter the username to see what emails Felix received or sent.



As seen in the email, **Felix** received a message from an email address that claims to be **free@coffeeshoop.com**. However, it's important to note that this email could potentially be a phishing attempt.

The email also contains phrases like 'Hurry' and 'This offer expires soon', which are meant to pressure the user, a common tactic in phishing attempts. After analyzing the email from the email security tab, we now have the information that the playbook requires.

QUESTIONS	ANSWERS
When was it sent?	May, 13, 2024, 09:22 AM
What is the email's SMTP address?	103[.]80[.]134.63
What is the sender's address?	free@coffeeshoop.com
What is the recipient's address?	felix@letsdefend.io
Is the mail content suspicious?	Yes
Are there any attachments or Links?	https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee[.]zip

Enjoy a Free Cup of Coffee on Us!

Dear Felix,

Start your day off right with a complimentary cup of coffee at our café! Just click the link below to redeem your voucher.

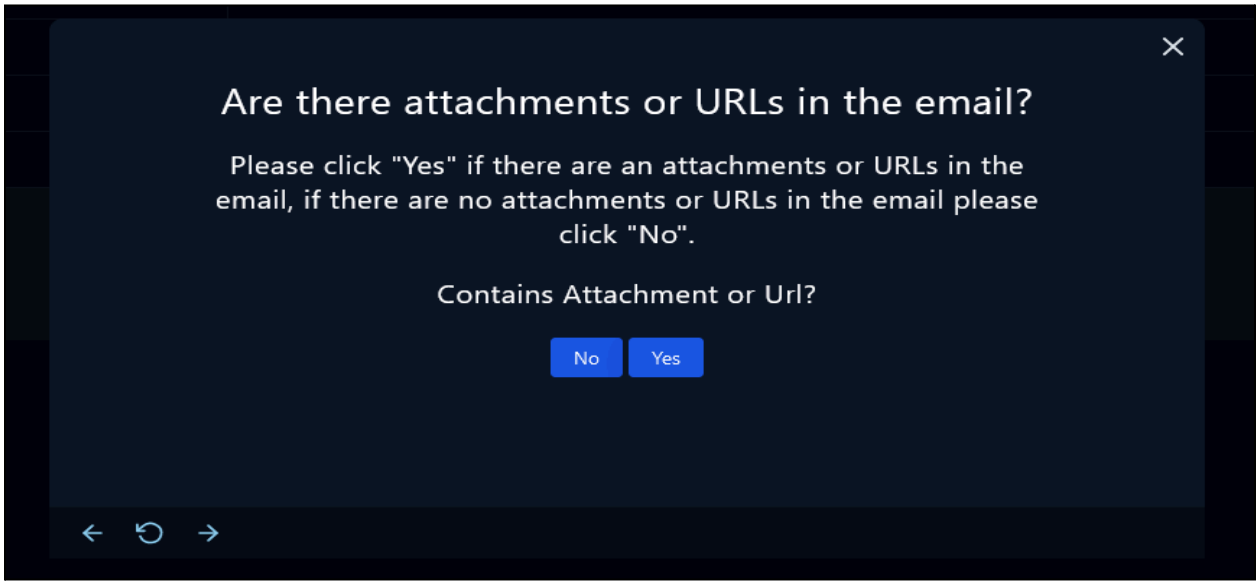
Redeem Now

Hurry, this offer expires soon!

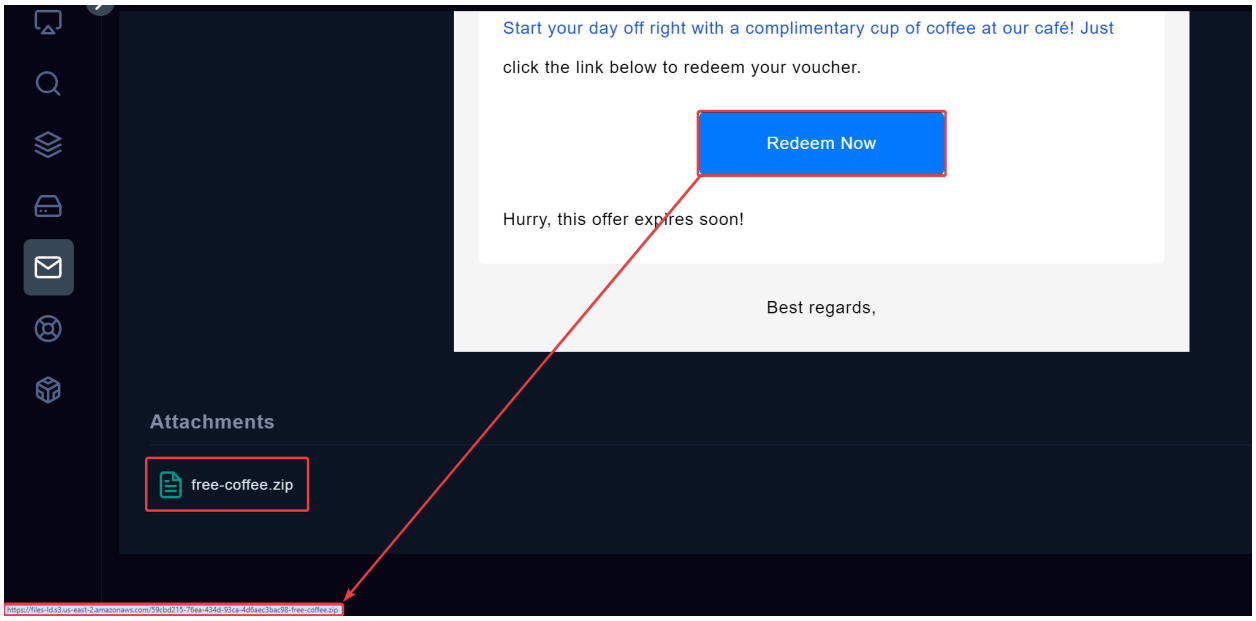
Best regards,

Analysis

As part of the investigation process, the second step of the playbook requires us to check if the email contains any attachments or URLs.

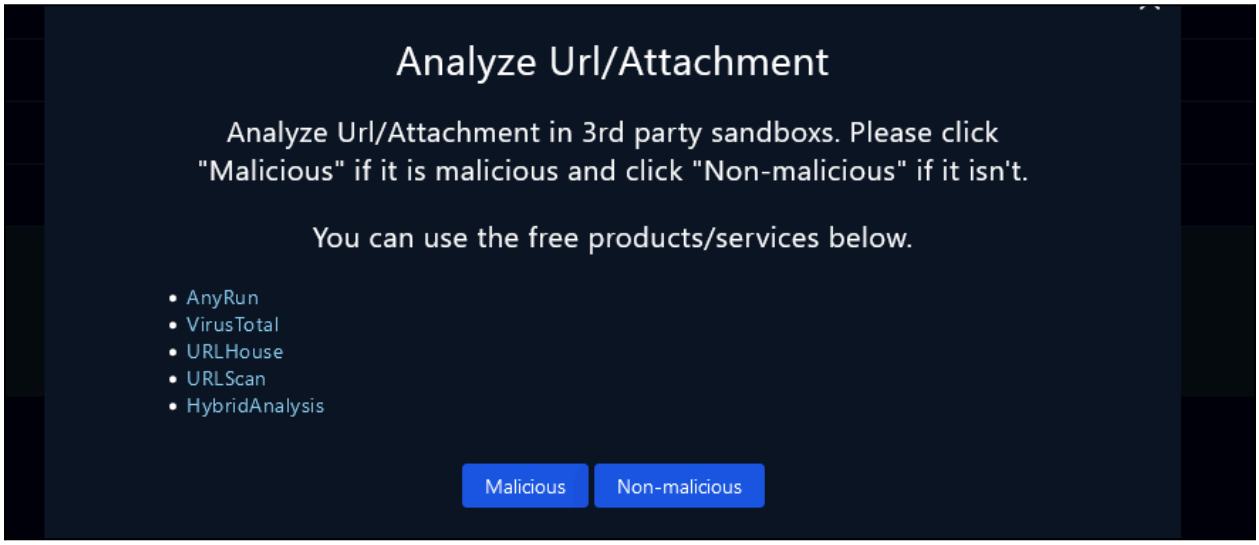


During the investigation, it was discovered that the email contained a suspicious URL - "https://files-ld.s3.us-east-2.amazonaws[.]com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip".

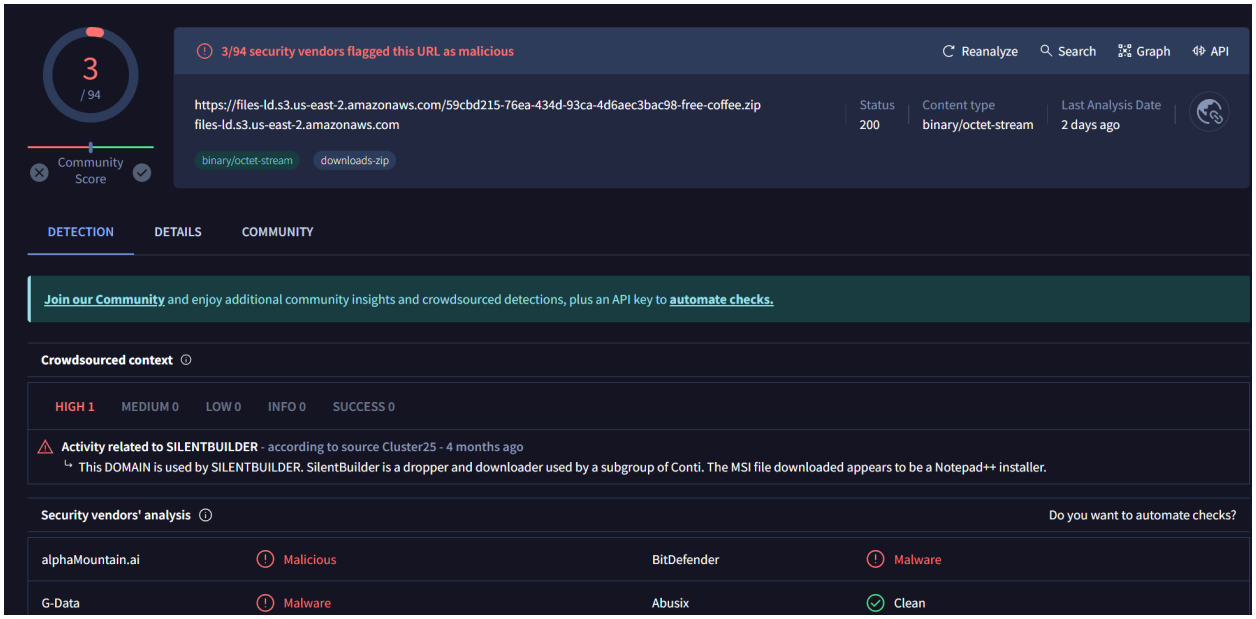


The playbook's answer is **YES**, the mail contains URL and attachment.

In the second step of the analysis, it is important to further analyze the suspicious URL or attachment using third-party sandboxing tools. This will provide additional insight into the nature of the threat and help determine the appropriate course of action.

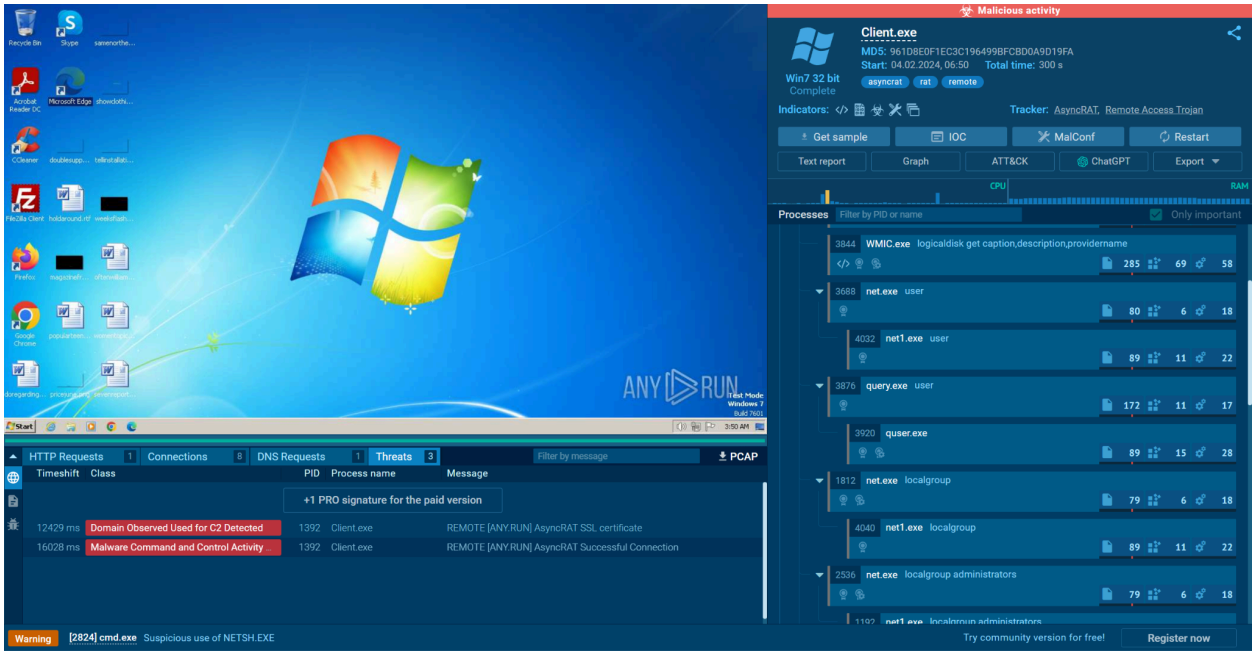


As part of the analysis in the second step, we checked the suspicious URL on VirusTotal.



The results showed that 3 antivirus engines flagged the URL as **malicious**. And in the crowdsourced context tab, it is categorized as silent builder. This indicates a high probability that the URL is malicious and poses a significant threat to the recipient's system and personal information.

As part of the analysis in the second step, we used Any.run to simulate the malware and gather more information about the threat.



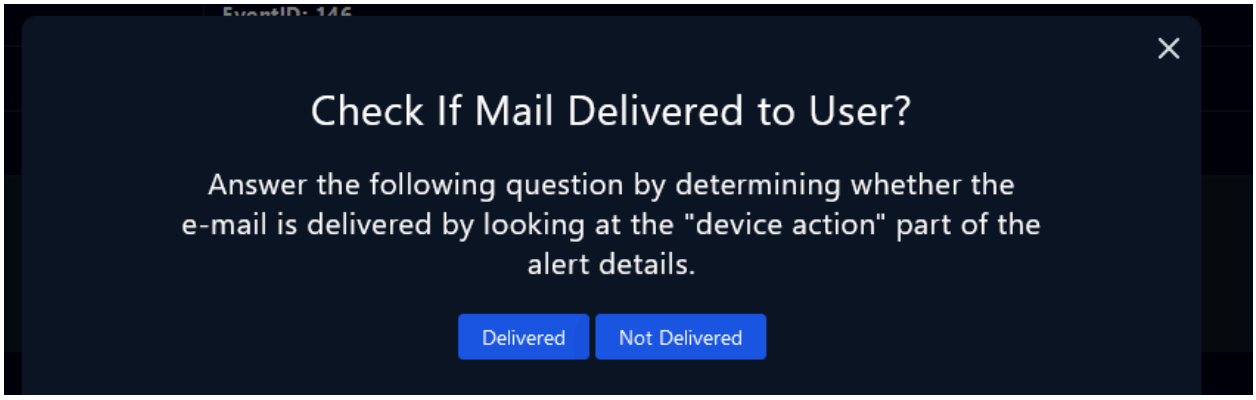
Public Submission Report

Our findings revealed that the URL provided in the email **imitates the Adobe login page**, making it difficult for the user to differentiate between the real and fake login page.

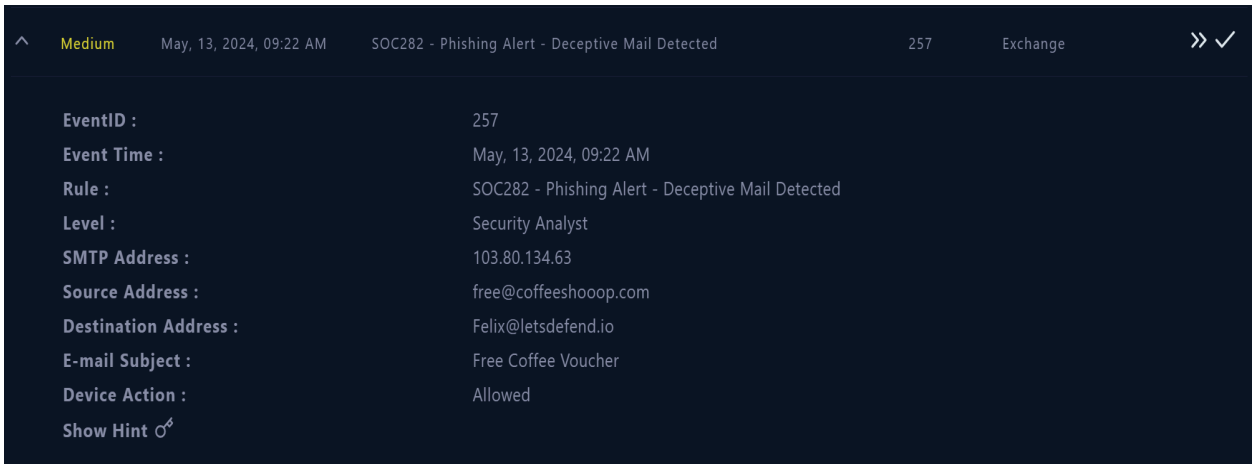
Based on the analysis, it has been determined that the **URL contained in the email is malicious**. Several engines on **VirusTotal** flagged the URL as **malicious**, and our simulation on **Any.run** revealed that the attachment is a malicious AsyncRAT variant, making it difficult for users to identify it the first sight.

We can choose the **Malicious** button and continue the playbook.

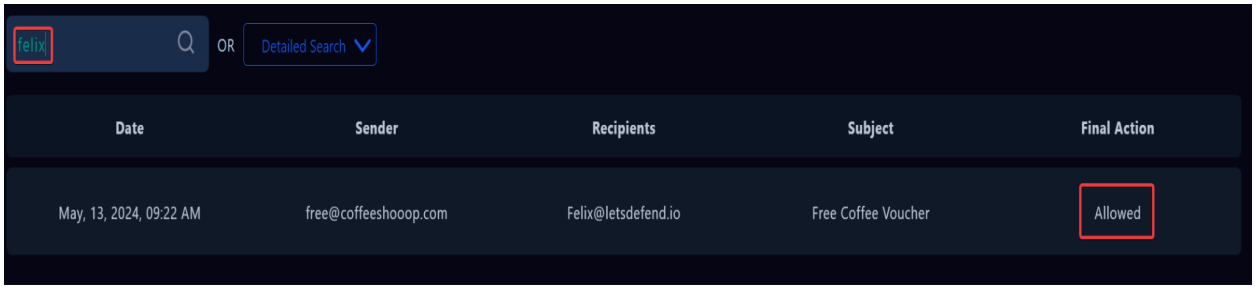
In the 3rd step of the playbook, we need to check if the mail was **delivered** to the user.



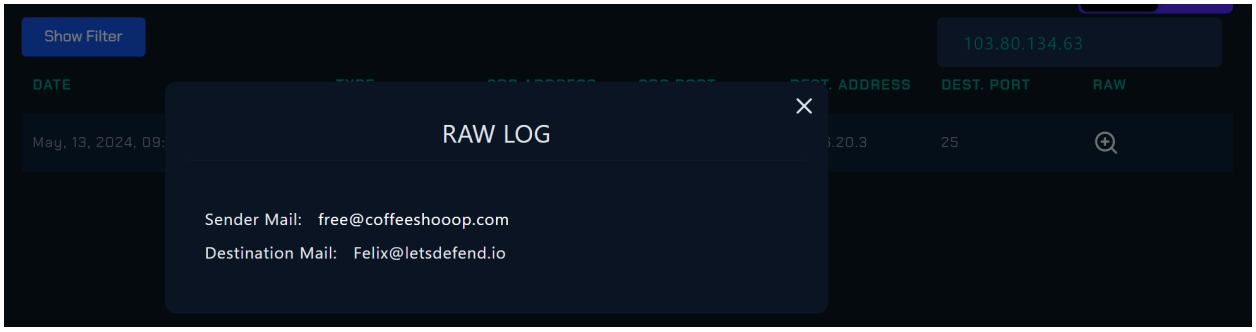
We can determine this by looking at the "**device action**" part of the alert details, which will tell us if the email was delivered to the user's inbox, marked as spam, or blocked by the email security system.



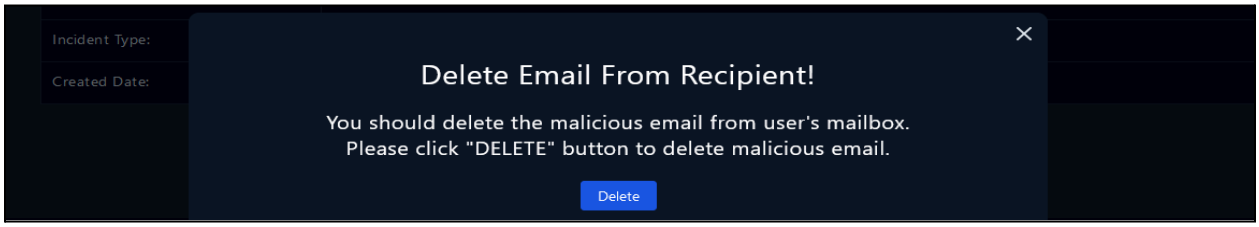
We can also see that the device action allowed on email security:



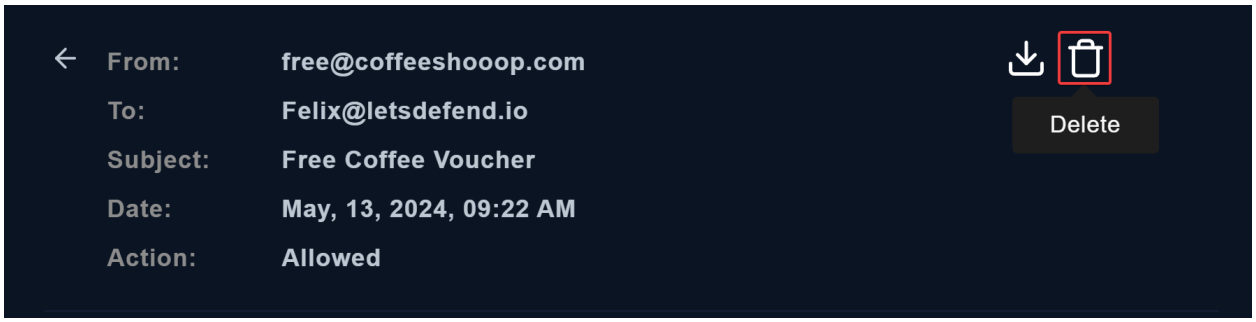
Based on the device action part of the alert details, the email was allowed and delivered to the user. We can also see that the email was delivered to the user by filtering the SMTP address on Log Management.



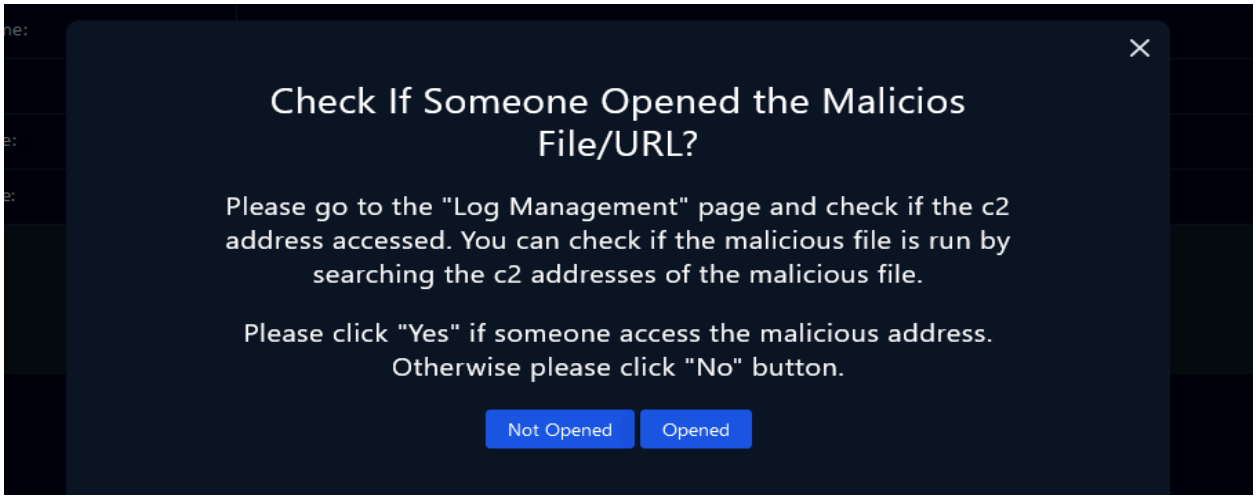
The answer to the 3rd part of the playbook is: **Delivered.**



After that, we should delete the malicious email from the user's mailbox.

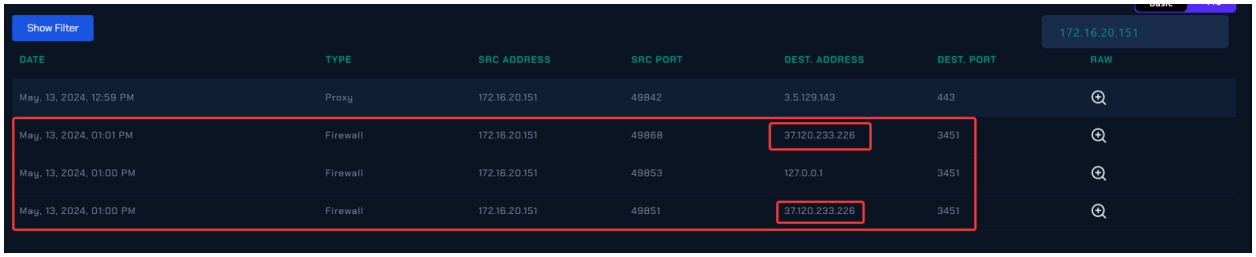


Step 4 of the playbook is to check if someone opened the malicious file/URL.

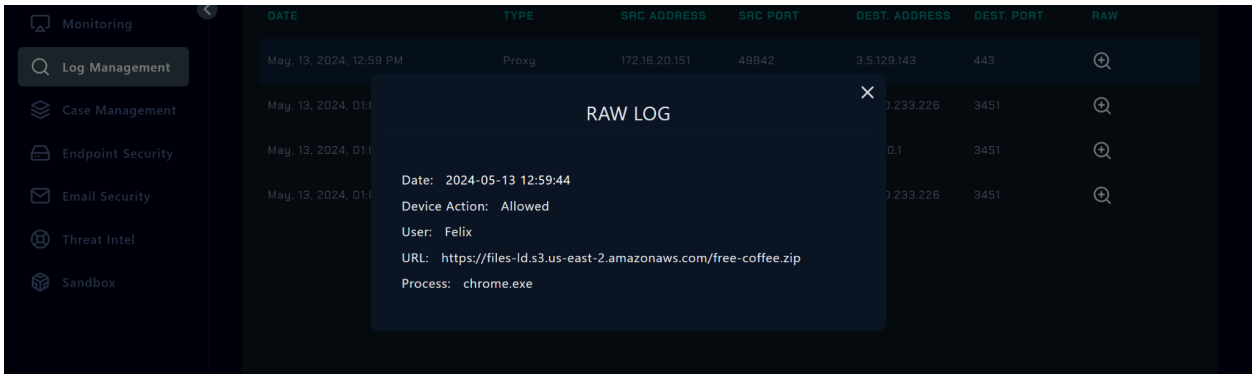


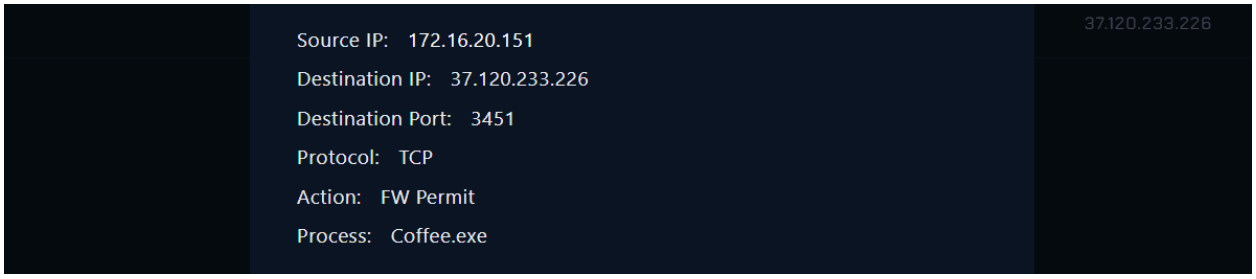
To do this, we need to go to the "Log Management" page and check if the C2 (command-and-control) address was accessed.

When we filter for the given Felix's client IP address we can see the traffic.



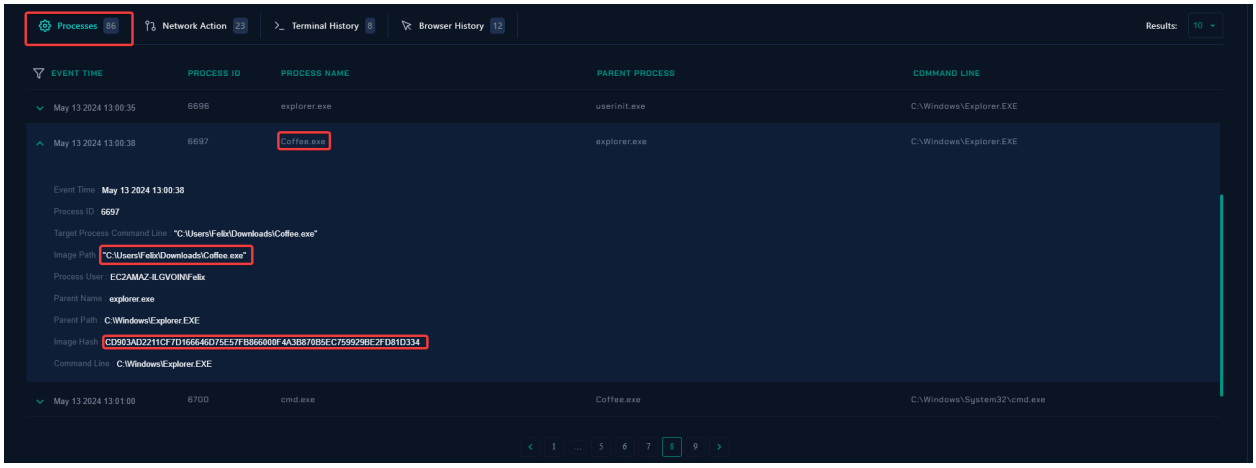
On the raw log of Proxy traffic. We can see the malicious URL: https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee[.]zip



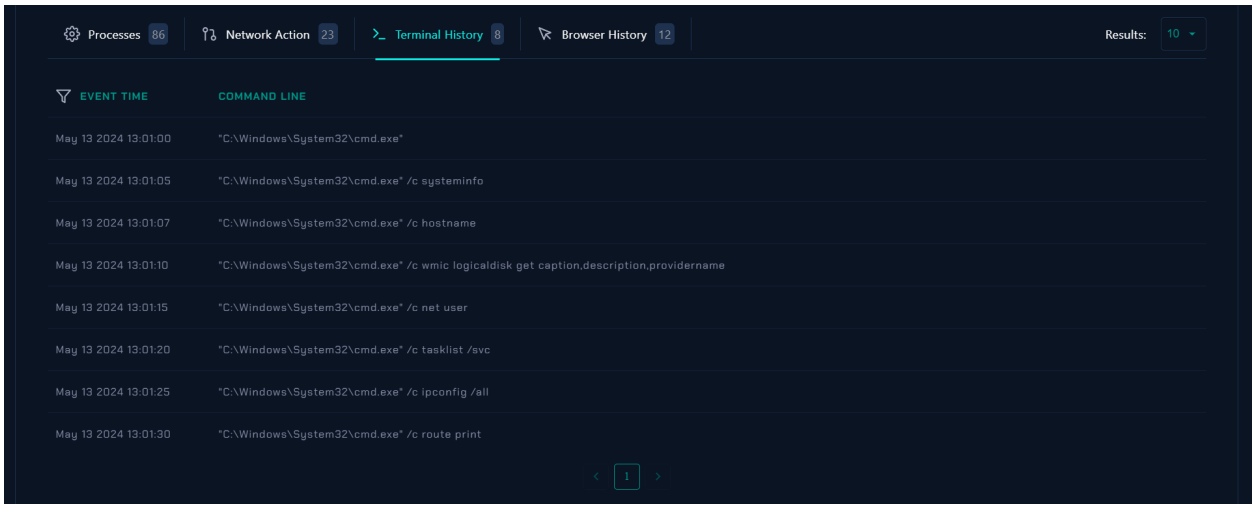


Coffee.exe connects to the C2 address **37.120.233[.]226**

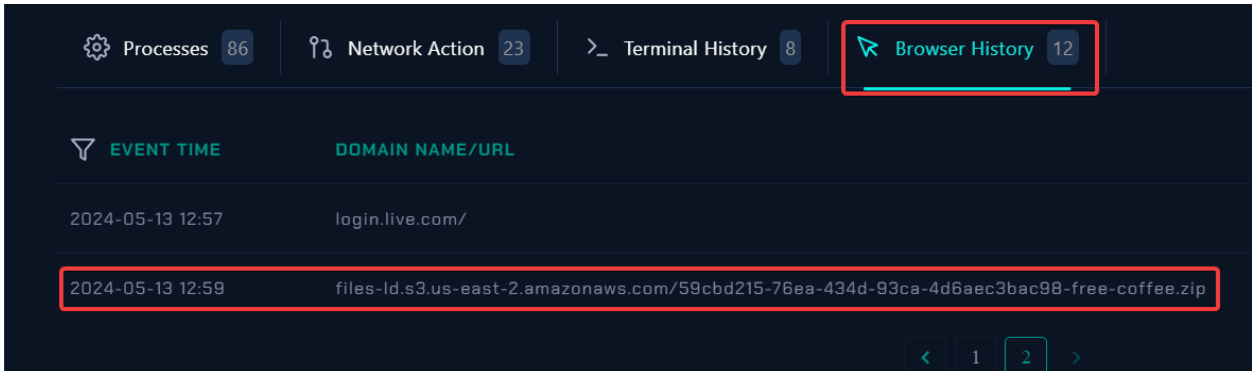
A malicious address was accessed by the host machine. And the answer is **Opened**. Additionally, we can see that the coffee.exe has run on the Felix's host.



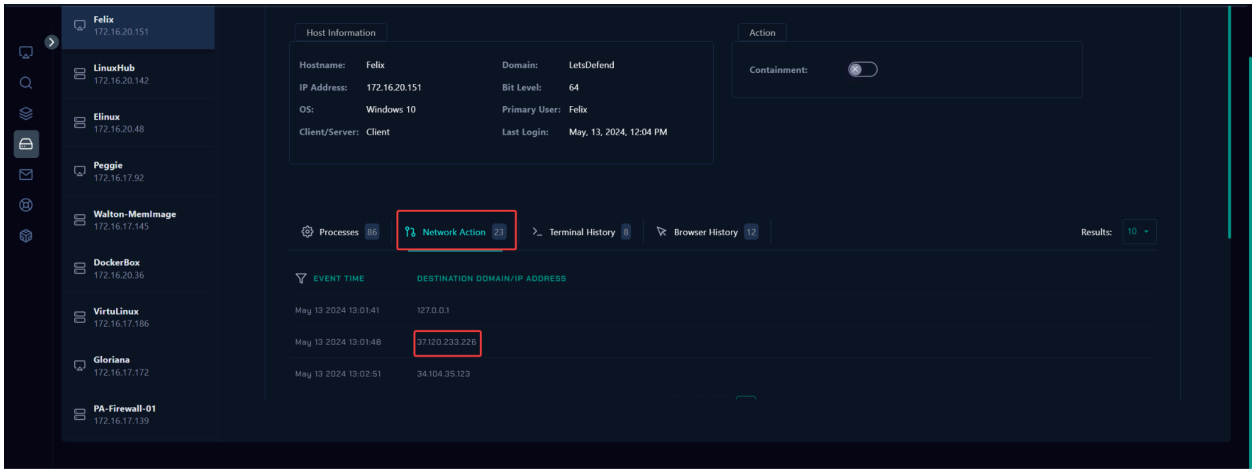
The malicious commands that had run on the system can be seen through the Terminal History.



Initial access for the host is 2024-05-13 12:59:

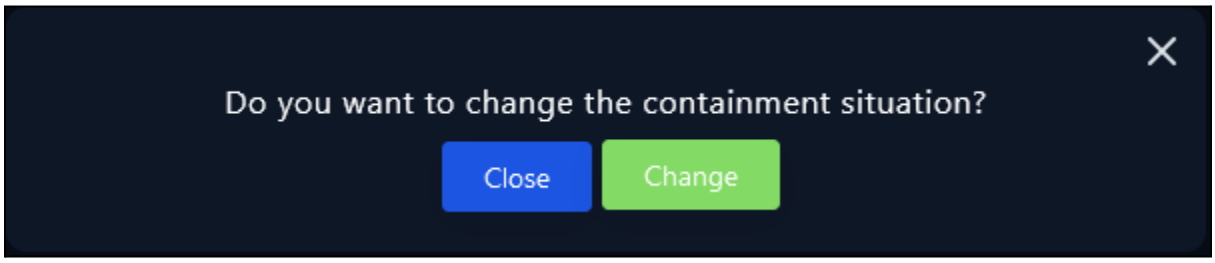


We can also see the connection to the C2 right after Coffee.exe is executed.



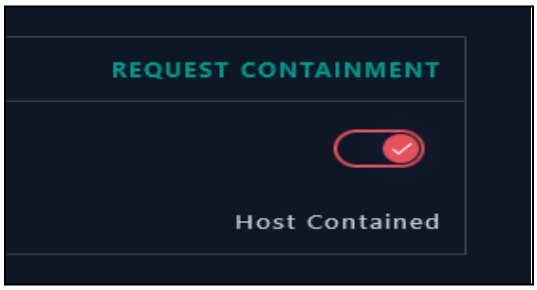
Containment

Based on the information gathered during the investigation, it is highly likely that the user credentials have been compromised and sensitive information may have been exfiltrated. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



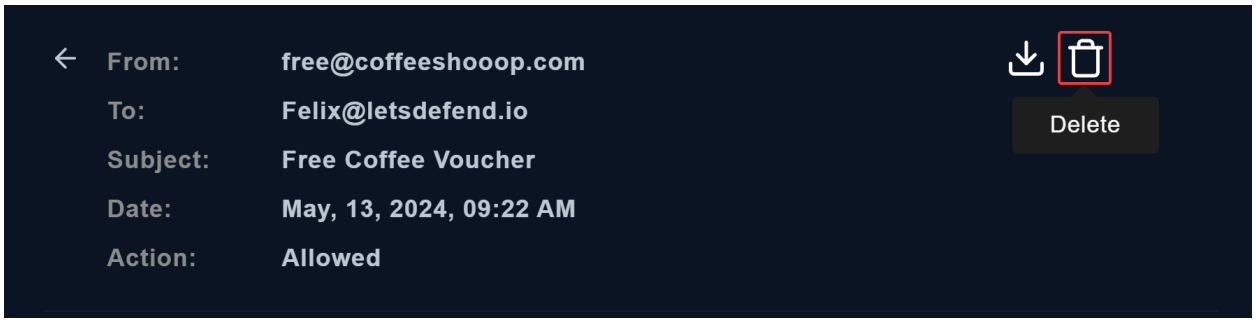
Isolation of the host can be made from the endpoint security tab.

Hostname	Felix
IP Address	172.16.20.151



Additionally, we should delete the phishing email from the user's mailbox to prevent any accidental or intentional re-execution of the malware. The user should also be educated on how to identify and avoid phishing emails in the future to minimize the risk of similar incidents occurring.

Deletion of mail can be made from the Email Security tab.



Lesson Learned

- It is important to carefully inspect suspicious emails, especially those that contain links or attachments.

- Phishing emails can be disguised to look like legitimate messages from reputable companies, but there are ways to identify and avoid them.

Remediation Actions

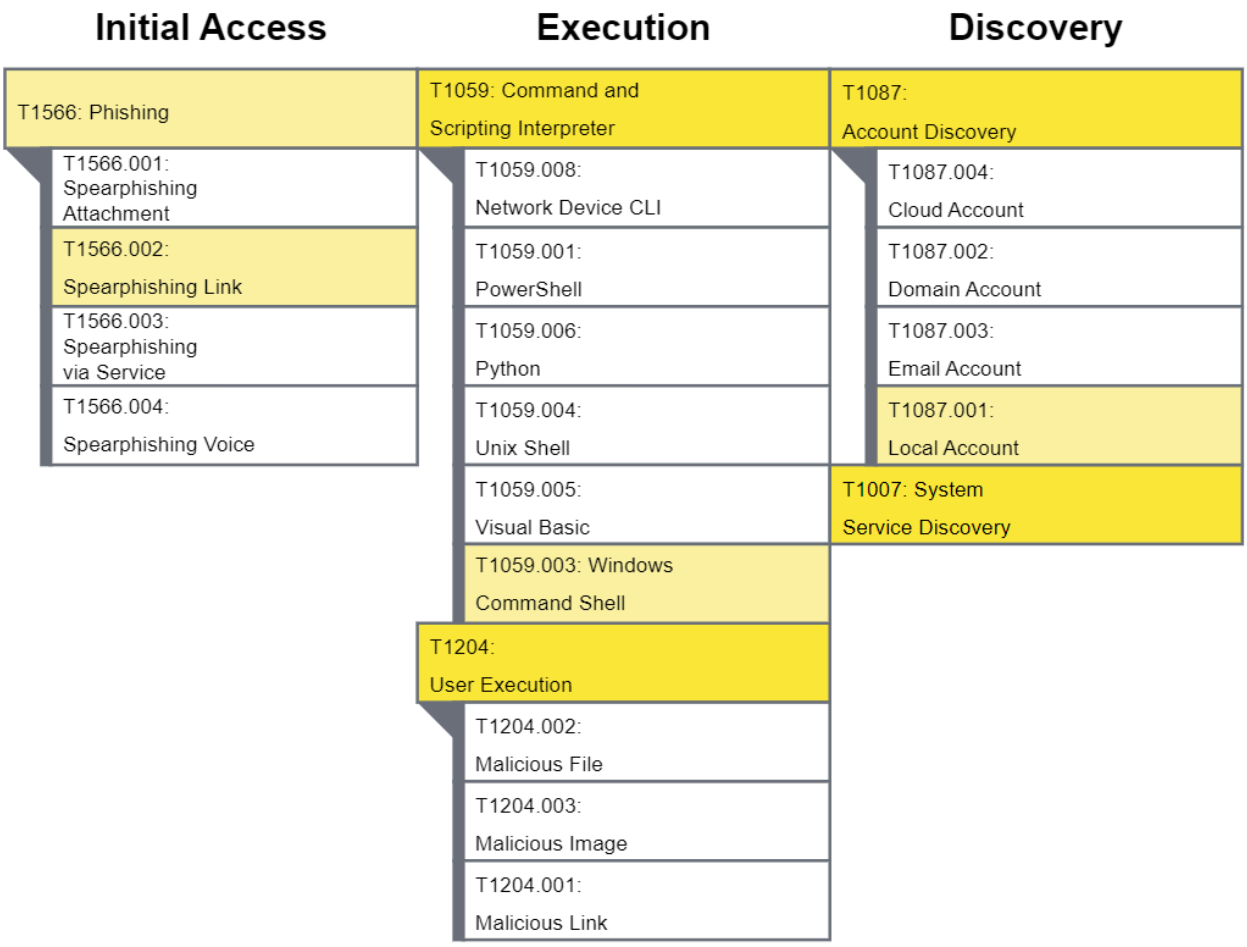
- Educate employees about how to identify and report suspicious emails, and provide training on how to avoid falling for phishing scams.

- Reset any compromised user credentials and implement a strong password policy.

- Implement email filtering and security measures, such as DKIM and SPF, to help detect and block spoofed emails.

Appendix

MITRE ATT&CK



MITRE Tactics	MITRE Techniques
Initial Access	T1566 Phishing
Execution	T1059: Command andScripting Interpreter
Execution	T1204:User Execution
Discovery	T1087:Account Discovery
Discovery	T1007: SystemService Discovery

Artifacts

IOC TYPE	VALUE
URL	https://files-ld.s3.us-east-2.amazonaws[.]com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip
SMTP Address	103[.]80[.]134.63
IPv4 - C2	37[.]120[.]233.226
Coffee.exe	CD903AD2211CF7D166646D75E57FB866000F4A3B870B5EC759929BE2FD81D334