Author: Jack Fitzgerald

Official Incident Report

Date: May, 13, 2024, 09:22 AM

Event ID: 257

Rule Name: SOC282 - Phishing Alert - Deceptive Mail Detected

Table of Contents

Alert Details

Severity: Medium

Type: Exchange

SMTP Address: 103.80.134.63

Source Address: free@coffeeshooop.com

Destination Address: Felix@letsdefend.io

E-mail Subject: Free Coffee Voucher

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious **phishing email** sent to **Felix@letsdefend.io** has been detected. The alert is triggered by rule SOC282 - Phishing Alert - Deceptive Mail Detected).

Upon reviewing the alert, it is observed that an email with the subject **Free Coffee Voucher** was sent from **free@coffeeshooop.com** with an SMTP of **103.80.134.63**.

The device action is marked **allowed**, indicating that the email was delivered to the **Felix@letsdefend.io** inbox.

Overall, it appears that the email may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

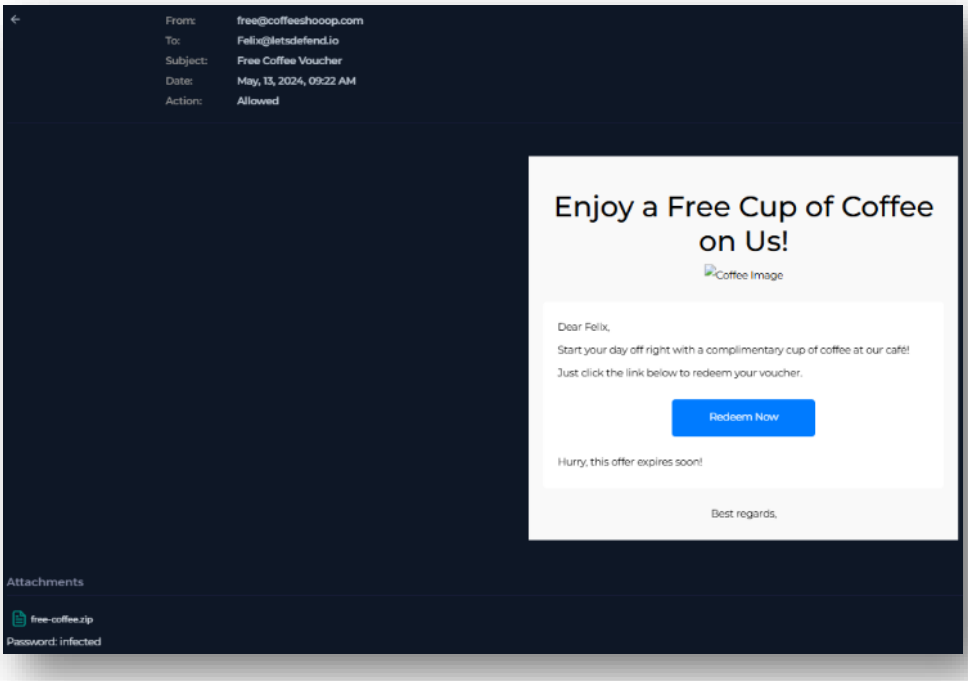
Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

We need to investigate the IP address on threat intelligence platforms and check host processes to validate whether the user clicked the link or executed any files.

It is important to check the Email Security product and analyze for any signs of phishing, links, or attachments.

By searching for the email sender of **free@coffeeshooop.com** in Email Security, we can find the email and some further details.



On the first look, the email looks suspicious. The email address shows signs of phishing, such as **free** and **coffeeshooop.com**. It also encourages the user to click the link with urgency **offer expires soon!** and includes a zip file named **free-coffee.zip**.

The first step we take when investigating a potential phishing email is to parse the email information.

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@coffeeshooop.com

What is the recipient's address?

Felix@letsdefend.io

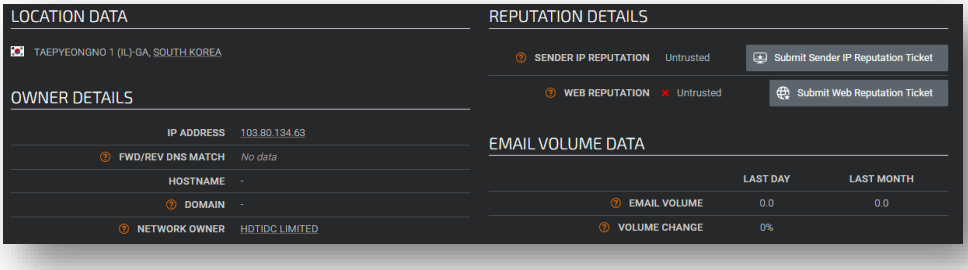
Analysis

Now, we can analyse the email data further, starting with the SMTP address via **VirusTotal** and **Talos Intelligence**.

https://www.virustotal.com/gui/ip-address/103.80.134.63

9/95 security vendors flagged this IP address as malicious

https://talosintelligence.com/reputation_center/lookup?search=103.80.134.63



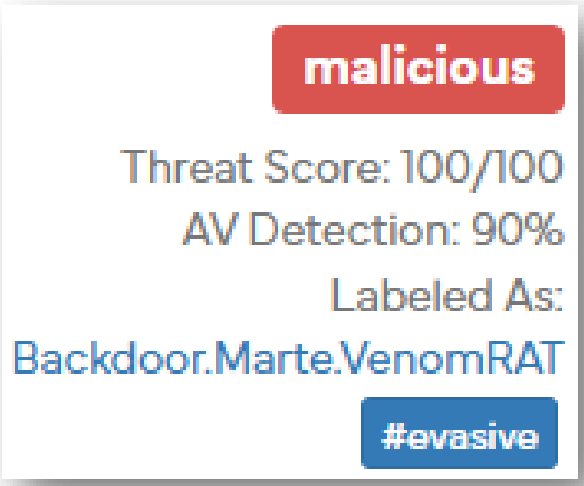
It is identified that the address the email was sent from is **untrusted**, **suspicious**, and **potentially malicious**.

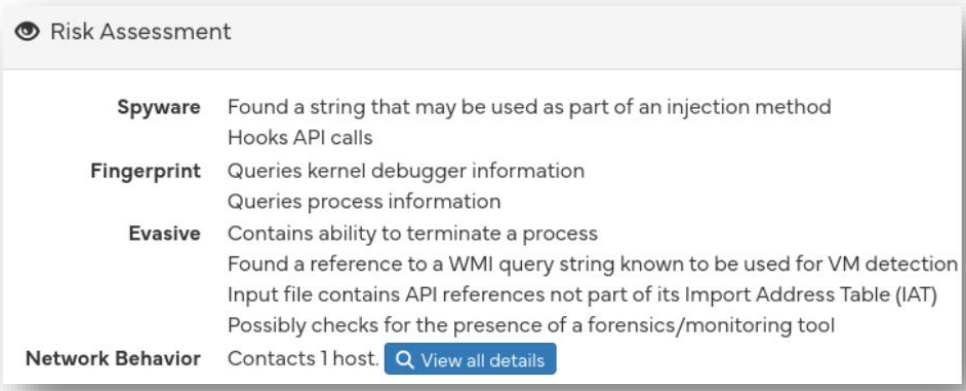
Next, we can analyse the file hash of the attachment **961d8e0f1ec3c196499bfcbd0a9d19fa** using **VirusTotal** and **Hybrid-Analysis**.

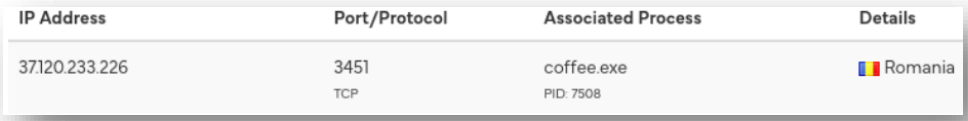
https://www.virustotal.com/gui/file/cd903ad2211cf7d166646d75e57fb866000f4a3b870b5ec759929be2fd81d334

58/72 security vendors flagged this file as malicious

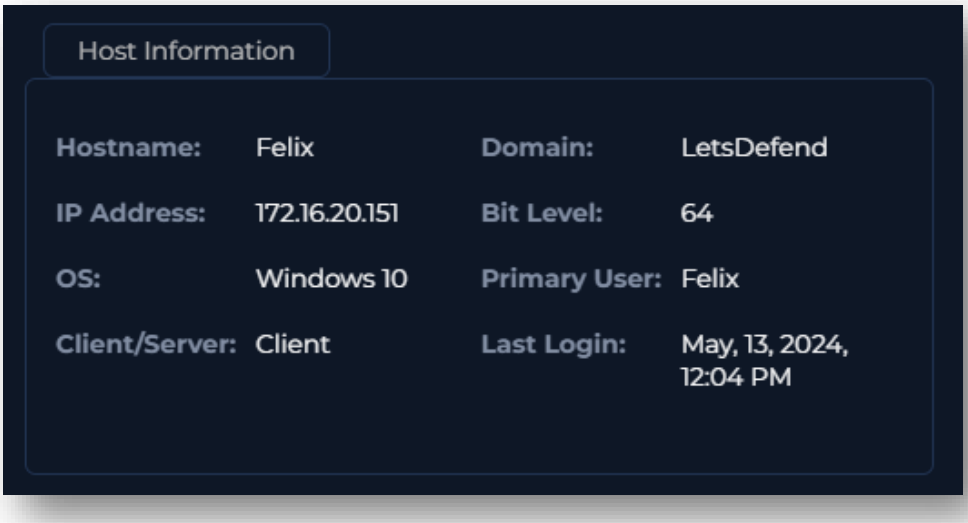
https://hybrid-analysis.com/sample/cd903ad2211cf7d166646d75e57fb866000f4a3b870b5ec759929be2fd81d334







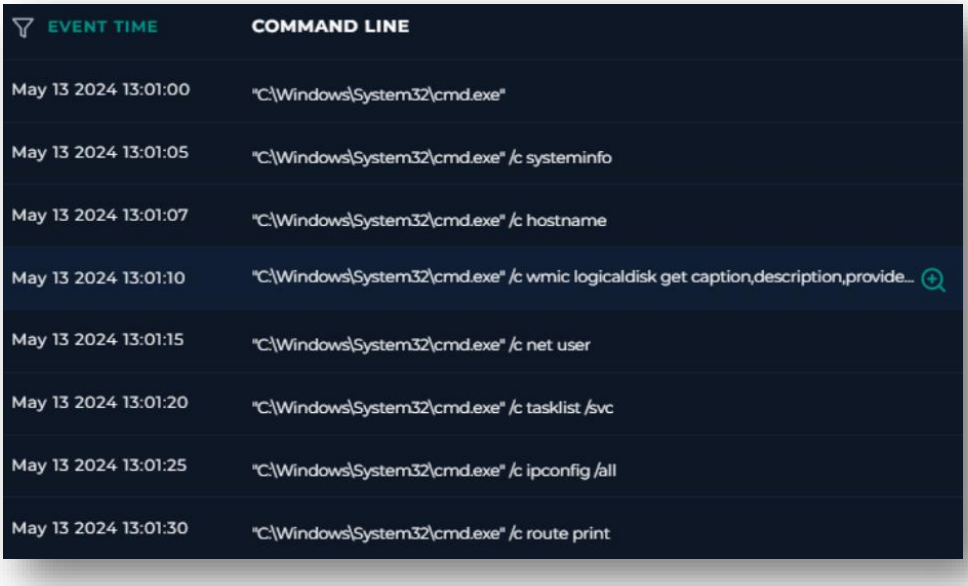
Our next step in the analysis process is to investigate Endpoint Security.



Our first step here is to investigate Browser History, where we find that at 2024-05-13 12:59, Felix clicked on the malicious link sent to his inbox.

EVENT TIME	DOMAIN NAME/URL
2024-05-13 12:52	google.com
2024-05-13 12:53	huffpost.com
2024-05-13 12:53	vice.com
2024-05-13 12:54	dailymail.co.uk
2024-05-13 12:54	tmz.com
2024-05-13 12:55	cnn.com
2024-05-13 12:55	bbc.com
2024-05-13 12:56	theguardian.com
2024-05-13 12:57	nytimes.com
2024-05-13 12:57	microsoft.com/en-us/microsoft-365/outlook/log-in
2024-05-13 12:57	login.live.com/
2024-05-13 12:59	files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip

Next, we can investigate Terminal History, where on May 13, 2024, 13:01:00, Felix's host machine executes **Coffee.exe** via **cmd.exe**, and then proceeded to run a list of commands gathering **system**, **user**, **task**, **network**, and **more information**.



EVENT TIME	COMMAND LINE
May 13 2024 13:01:00	"C:\Windows\System32\cmd.exe"
May 13 2024 13:01:05	"C:\Windows\System32\cmd.exe" /c systeminfo
May 13 2024 13:01:07	"C:\Windows\System32\cmd.exe" /c hostname
May 13 2024 13:01:10	"C:\Windows\System32\cmd.exe" /c wmic logicaldisk get caption,description,provide...
May 13 2024 13:01:15	"C:\Windows\System32\cmd.exe" /c net user
May 13 2024 13:01:20	"C:\Windows\System32\cmd.exe" /c tasklist /svc
May 13 2024 13:01:25	"C:\Windows\System32\cmd.exe" /c ipconfig /all
May 13 2024 13:01:30	"C:\Windows\System32\cmd.exe" /c route print

Our final investigative point of Endpoint Security will see us investigate Network Action, where on May 13, 2024, 13:00:39 & 13:01:48, Felix's host machine accessed the malicious file's C2 server **37.120.233.226**.

May 13 2024 13:00:39	37.120.233.226
May 13 2024 13:00:51	127.0.0.1
May 13 2024 13:00:58	169.254.169.254
May 13 2024 13:01:41	127.0.0.1
May 13 2024 13:01:48	37.120.233.226
May 13 2024 13:02:51	34.104.35.123

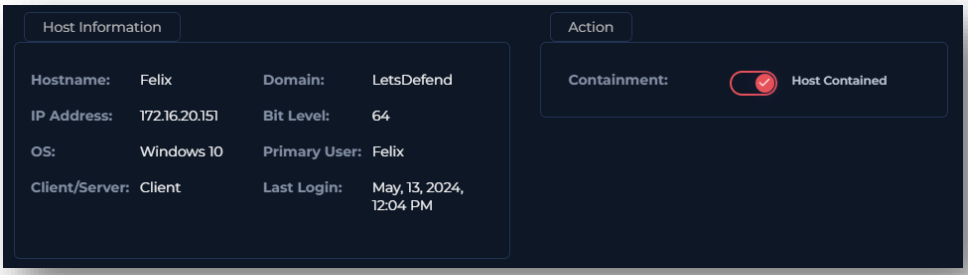
Our next step of the process is to investigate Log Management, where we identify 4 events correlated to this alert. Here, we will focus on 2 that indicate Felix successfully executed malicious file **Coffee.exe**, which accessed the C2 server at **37.120.233.226**, requiring containment of Felix's host machine.

destination_address	37.120.233.226
destination_port	3451
time	May, 13, 2024, 01:01 PM
Raw Log	
Source IP	172.16.20.151
Destination IP	37.120.233.226
Destination Port	3451
Protocol	TCP
Action	FW Permit
Process	Coffee.exe

source_address	172.16.20.151
source_port	49842
destination_address	3.5.129.143
destination_port	443
time	May, 13, 2024, 12:59 PM
Raw Log	
Date	2024-05-13 12:59:44
Device Action	Allowed
User	Felix
URL	https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip
Process	chrome.exe

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required to prevent further spread of malicious content.



Summary

The incident involves a compromised system called **Felix**. The alert was triggered by the detection of a suspicious **phishing email**, sent to **Felix@letsdefend.io**, based on the rule SOC282 - Phishing Alert - Deceptive Mail Detected.

Felix@letsdefend.io received a malicious phishing email containing an attachment of **Coffee.exe** from IP address **103.80.134.63** urging the user to redeem their free coffee voucher. The email was not quarantined and allowed to be served to the user's inbox. The SMTP address was confirmed as suspicious by various security vendors and online analysis tools.

Coffee.exe is a **MALWARE TROJAN EVADER RAT**, labeled as **Backdoor.Marte.VenomRAT**. **Coffee.exe** was opened on the host machine **172.16.20.151** and accessed C2 traffic at **37.120.233.226**. The host machine was isolated and contained.

In future, please block incoming emails containing QR codes, and require manual inspection from a security officer before forwarding to the end user. Please educate users on identifying and reporting suspicious emails.

This alert was identified as a **True Positive**.

Lessons Learned

- Human psychology is the main target, not technical weaknesses, attackers exploit emotions like fear, urgency, and trust to bypass rational decision-making

- A single employee clicking a bad link or processing a fraudulent payment can compromise an entire organization

Remediation Actions

- Delete the identified email from the user's inbox and maintain a block to the email sender and associated IPs

- Conduct targeted security awareness training, focusing on social engineering recognition and reporting suspicious emails promptly

- Run simulated phishing campaigns to test and improve readiness

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1598.002 - Spearfishing Attachment
Execution	T1204.002 - User Execution: Malicious File
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols

Artifacts

Value	Comment	Type
free@coffeeshooop.com		E-mail Sender
coffeeshooop.com		E-mail Domain
103.80.134.63	SMTP Address	IP Address
37.120.233.226	C2 Traffic	IP Address
961d8e0f1ec3c196499bfcbd0a9d19fa	Coffee.exe	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 257