EventID 257 SOC282 Phishing Alert Deceptive Email Detected

- SIEM alert creation time: 2024, May (Monday) 13th at 09:22h
- IP of source SMTP Server: 103.80.134.63
- Source email address: free@coffeeshooop.com
- Destination email address: Felix@letsdefend.io
- Destination IP address: 172.16.20.151
- Subject: "Free Coffee Voucher”
- Device action: "Allowed”
- Incident type: "Exchange”

This alert is part of “Introduction to SIEM Alerts” lesson of LetsDefend, I’m analyzing and documenting it, while following the lesson.

Email Security

After taking ownership of the alert and creating a case, I’ve looked for the suspicious email in Email Security section of LetsDefend. This is what I’ve found:

- The email body encourages the recipient to click in a URL. This URL downloads a ZIP file called “free-coffee.zip”
- The email has an attachment, which corresponds to the “free-coffee.zip” file downloaded when clicking in the URL
- The text in the email transmits a sense of pressure to the recipient, as if the sender were trying to manipulate the recipient into taking fast actions. This looks like a social engineering attack to me

Threat Intelligence

1/97 Security Vendors in VirusTotal flag the URL included in the email body as malware:

- “https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip”

Note that the last analysis is from 1 day ago, which I consider to be recent.

The ZIP file downloaded through the above URL is called "free-coffee.zip" and is password-protected (”infected”).

By looking at the community comments in VirusTotal about the above URL, I noticed many users classify the downloaded file as a Trojan. More specifically AsyncRAT, a C# program for remote control of computer systems.

❓ AsyncRAT means Asynchronous Remote Access Tool.

Log Management

First I've looked for the IP address of the victim (172.16.20.151) in the Endpoint Security section of LetsDefend.

Then, in the Log Management section of LetsDefend, I've found the logs of that computer system and scrolled down to the time just after the SIEM alert was created (May 13th at 09:22h).

Proxy and firewall activity is registered starting at 12:59h. First, a request from the victim host to the URL attached in the suspicious mail is done successfully, this means the victim at least clicked in the URL.

Following that, there are some firewall logs coming from process "Coffee.exe", requesting "37.120.233.226:3451" IP Address.

The "3451" port is used for TCP connections, this supports the community comments in VirusTotal, describing the file as a remote control Trojan.

This file is also identified as a Backdoor in Threat Insights Portal. Once executed, the attacker achieves persistence in the victim's machine.

These logs prove that the victim clicked in the URL, downloaded the attachment, executed "Coffee.exe", and established connection with the C2 Server.

Additionally, the Threat Intelligence Feed section of LetsDefend flags the destination IP "37.120.233.226" as "C2, AsyncRAT", supporting my suspicions.

Endpoint Analysis

Browser history logs reflect the download of “free-coffe.zip” from the attached URL.

Process logs have been found about the execution of “Coffee.exe” at 13:00h through Windows Explorer, after being downloaded.

Network logs are present, about the victim’s machine contacting “37.120.233.226” C2 Server multiple times, after the execution time of “Coffee.exe”.

Under terminal history logs, no execution of suspicious commands is spotted. This could indicate that the attack reached Command & Control phase of the Cyber Kill Chain, but no further actions were taken.

Since malicious activity is detected, the victim’s host has been contained.

I’ve leveraged EDR to look for presence of “Coffee.exe” and its image hash in other Endpoints, but only the victim’s host matches the search. This means that there’s no evidence of Lateral Movement.

Conclusion

The attacker used a phishing email and social engineering tactics to deliver a Trojan to the victim. The email promised a free coffee to the victim, and exercised pressure in downloading the provided attachment, while also having a button with a downloading URL.

The attachment was downloaded and executed by the victim, so the host has been contained in response, and the phishing email has been deleted from the victim's email box.

From multiple Threat Intelligence sources, it has been determined that the Trojan is a remote control software and a Backdoor identified as AsyncRAT, with the objective of achieving persistence in the victim's machine.

The victim's machine made contact with the C2 Server through a TCP connection, but there's no presence of further malicious commands in the terminal logs.

The attacker achieved Command & Control phase of the Cyber Kill Chain, but didn't reach Actions on Objectives.

I have looked for presence of Lateral Movement, which is negative, and the alert has been resolved.

Artifacts

I've attached the following Indicators of Compromise to this investigation:

- "free@coffeeshooop.com" Malware sender email
- "coffeeshooop.com" Malware sender domain
- "Free Coffee Voucher" Subject of phishing email
- "73f0f77181e1f06a9dbc41ea9e7a03fe" (MD5 Hash) free-coffee.zip
- "https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip" Malware providing URL
- "37.120.233.226" C2 Server
- "CD903AD2211CF7D166646D75E57FB866000F4A3B870B5EC759929BE2FD81D334" (SHA-256) Image hash of Coffee.exe