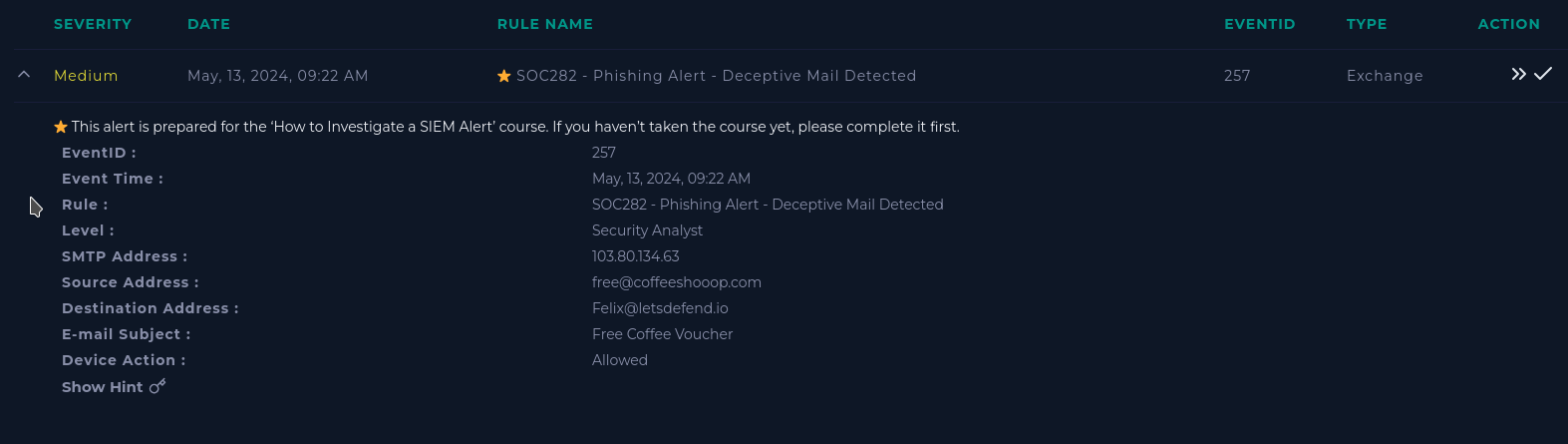
I am going to be creating a case on LetsDefend “SOC282 - Phishing Alert - Deceptive Mail Detected”.



First lets review information we can gleem from the alert.

When did the alert occur?

May, 13, 2024, 09:22 AM

What is the email’s SMTP (simple mail transfer protical) address?

103.80.134.63

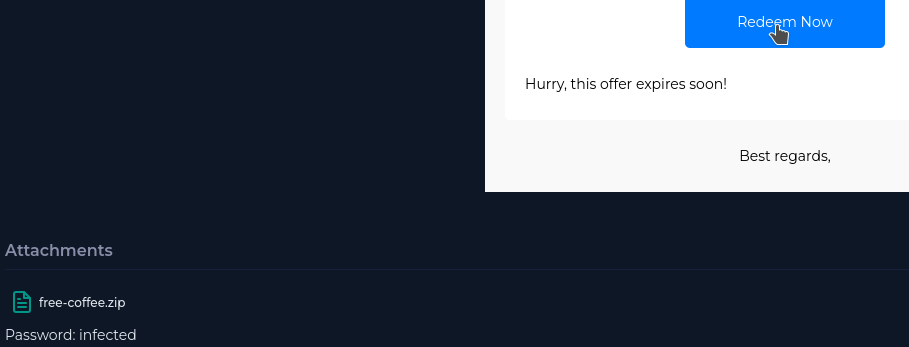
What is the source address?

free@coffeeshooop.com

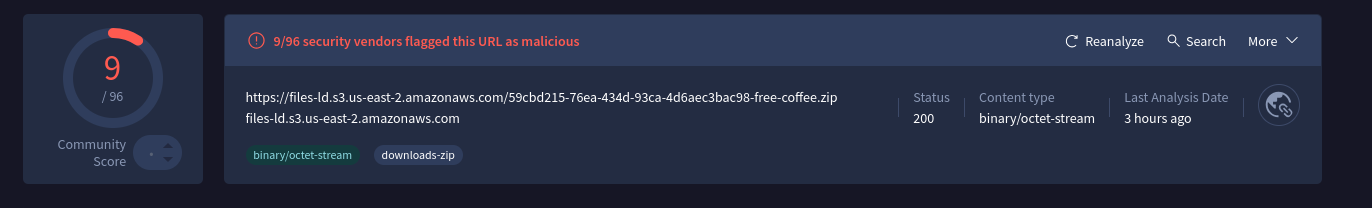
What is the destination address?

Felix@letsdefend.io

Navigating to email security, I search the source address to find the suspicious message. This email contains a redeem now leading to a free-coffee zip file attachment. After analysis I deleted this email from the user's inbox.

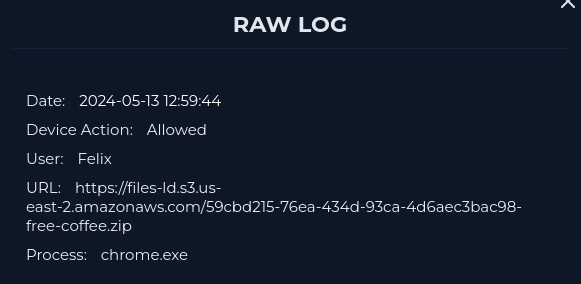




Placing this link into Virus total warns us that this link has been connected to malicious activity such as malware. 

Did anyone open this attachment? To find out we move to Felix’s endpoint management to gain his IP address (172.16.20.151). Taking Felix’s IP address into Log Management and searching for logs that occurred around the time of the alert, we find four logs.

Within this first log we see when Felix downloaded the email attachment.



Within the 2nd raw log we can see that Felix’s IP connects with an unknown Command to Control (C2) IP over port 3451 (TCP/UDP).

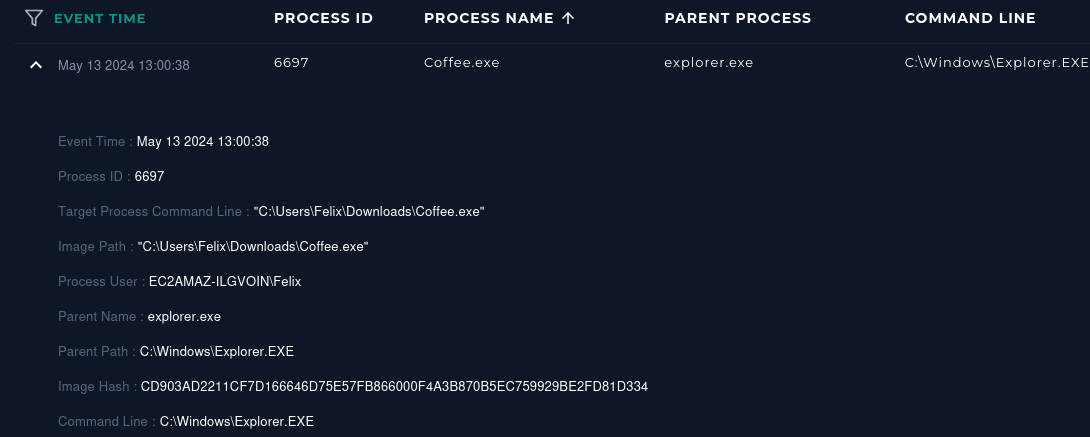


The third log shows traffic from Filex’s computer being sent to an unknown IP 127.0.0.1 but ultimately blocked by firewall rules.

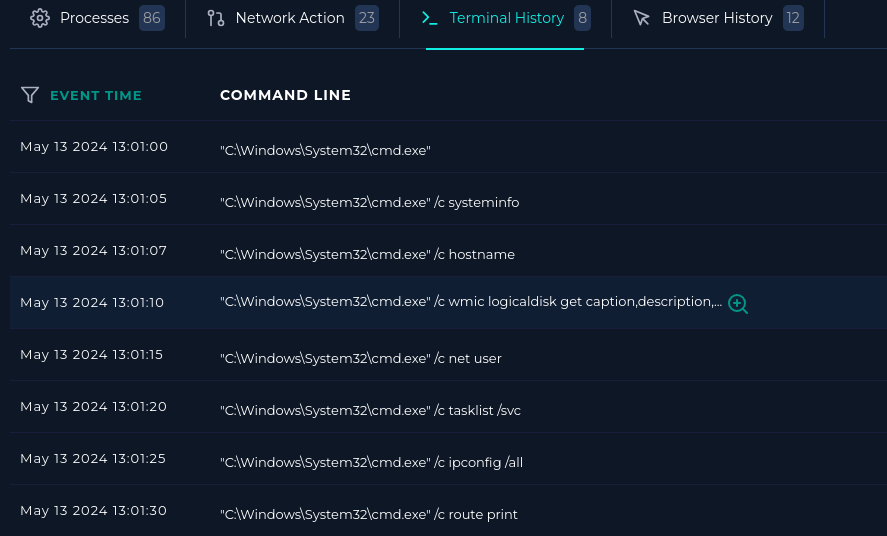


The fourth shows Feilixes computer communicating with the C2 control being permitted by the firewall.

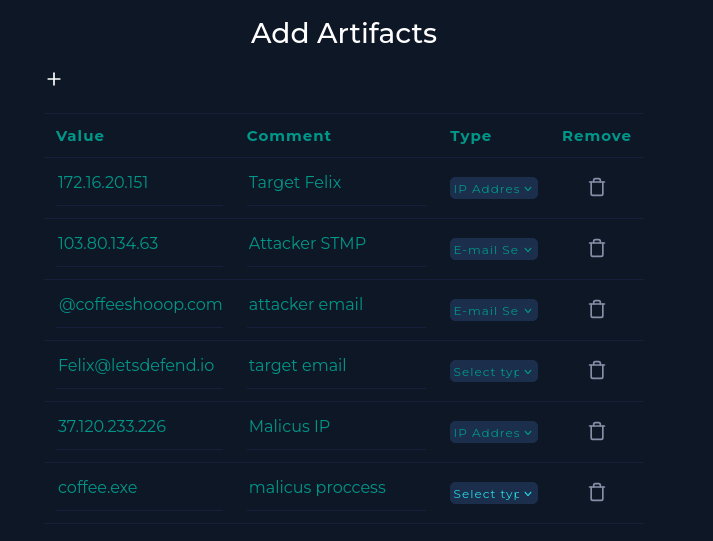


From these log files Felix’s endpoint must be isolated as it’s compromised. Here we can find the coffee.exe process which contains various information such as its image hash.

Within the terminal history we can also see what the attacker did once he was in the system. All these commands lead the attacker to gain vast amounts of system information from the file structure to network structure.



Artifacts:



Analysis Note:  
Felix was sent an email with a free coffee offer containing a malicious link. When clicked, this link connected Felix's IP to a C2 server (IP: 37.120.233.226) via port 3451 (TCP/UDP). After the connection was established, several console commands were run to gather more information about Felix's system and network infrastructure by the attacker. This information could be used in further attacks.

Felix's machine has been placed into containment for further analysis.