Packet Capture Analysis Report
Task 22

UBNETDEF

April 30, 2023

Executive Summary

On March 16th, 2023 UBNETDEF conducted analysis which revealed an endpoint, 10.10.5.3, was infected with a malicious piece of software called Redline Stealer. This malware is used to steal information on the system such as passwords, cryptocurrency wallets, and system information and sends it to the attacker. It is not known how the malware infected the machine, but it is likely the user of 10.10.5.3 visited a malicious website hosting the malware and it was able to infect their machine. Given the current capture it is not known exactly what information the attacker extracted with, if any.

To mitigate this incident and prevent future intrusions, UBNETDEF recommends isolating the infected machine and removing any malicious software, implementing firewall rules that block known malicious addresses, and installing and regularly updating an anti-virus program, such as Windows Defender. Additionally, training users on identifying and reporting different kinds of phishing emails can help eliminate before they enter the environment.

Contents

1 Technical Analysis

1.1 Indicators of Compromise

UBNETDEF was given a packet capture file spanning the times 10:32 UTC to 10:46 UTC on March 16th, 2023. UBNETDEF used the tools Wireshark and VirusTotal to identify indicators of compromise. The first action was establishing the clients involved in this packet capture which could be compromised, for which UBETNDEF found:

Client Name	IP	MAC
Client1	10.10.5.3	B6:BF:32:B5:A4:50
Client2	10.10.5.2	3E:6B:41:A4:EA:46
Clint3	10.10.5.70	D2:32:FC:FA:81:D8

Unfortunately, more information regarding users or host names of these clients could not be found based on the current information. Of these clients, UBNETDEF believes 10.10.5.3 was compromised based on its traffic to the addresses, 178.32.215.165 (ip165.ip-178-32-215.eu) and 45.77.166.103 (vultrusercontent.com). See Figure 1 & 2.

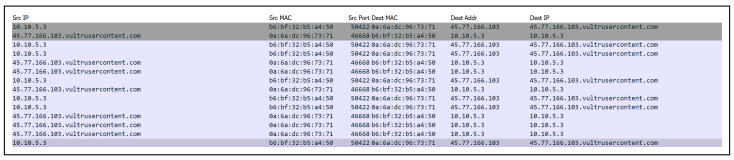

Figure 1: Traffic To vultrusercontent.com

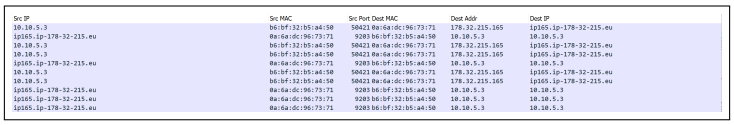

Figure 2: Traffic to ip165.ip-178-32-215.eu

Searching up these domain's IP addresses in VirusTotal shows they are malicious. Ip165.ip-178-32-215.eu contains malware called Redline stealer, which is MaaS (malawre-as-a-service) designed extract information from the victim's computer. It features the ability to steal credentials, cryptocurrency wallets, and operating system information. See Figure 3.

Figure 3: ip165.ip-178-32-215.eu VirusTotal

Vultrusercontent.com is also associated with Redline stealer shown in Figure 4, and is likely the command and control server given the heartbeat like traffic seen between 10.10.5.3 and vultusercontent.com seen in Figure 1.

Figure 4: vultrusercontent.com VirusTotal

These findings show that 10.10.5.3 is compromised with the Redline information stealer and is sending traffic to a command and control server.

1.2 Malicious Activity

As stated, the Redline information stealer extract sensitive information, such as cryptocurrency wallets. Digging deeper the traffic between 10.10.5.3 and ip165.ip-178.32.215.eu there is evidence that Redline is searching for information about the user's browser, system information, and electrum cryptocurrency wallet, to name a few. See Figure 6.

Figure 5: TCP Stream 201

Additionally, in the same stream you can see an executable called "123.exe" being run, which is a known executable that runs RedLine stealer. See Figure 7.

Figure 6: 123.exe Malicious executable

It's behavior coincides with what UBNETDEF saw in TCP stream 201, where the malware will scan the entire system looking for information to steal. See Figure 8.

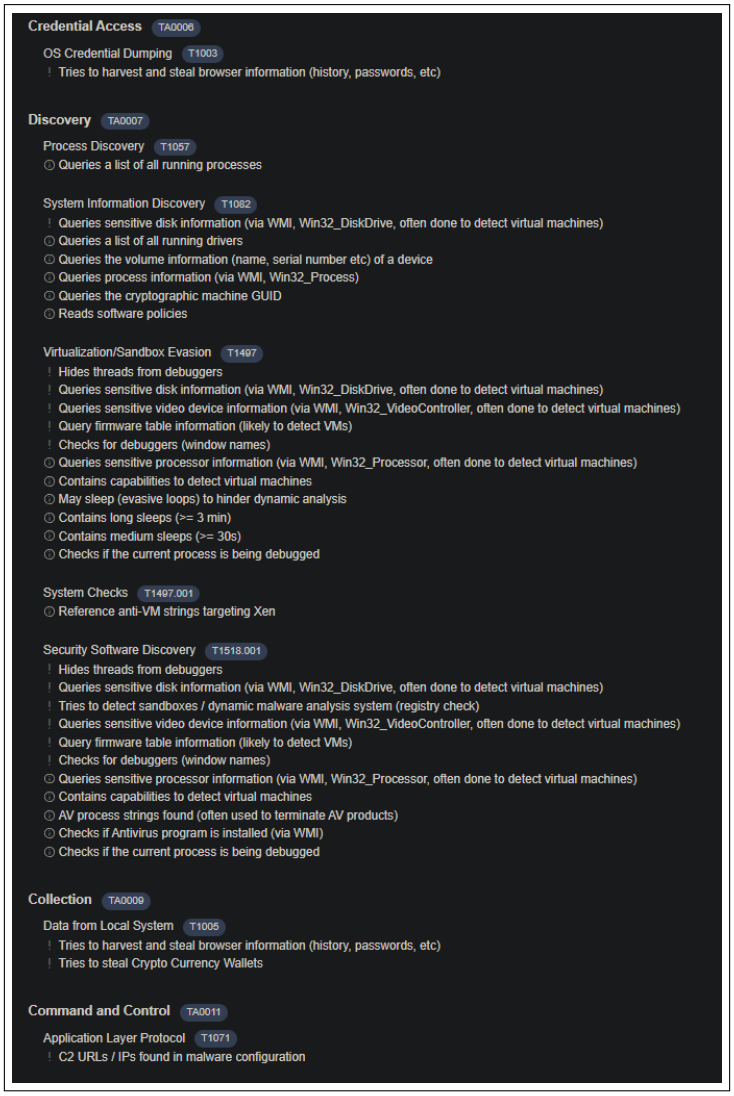

Figure 7: 123.exe Behavior from VirusTotal

Unfortunately, is it not possible to see what information was extracted due to the TLS encryption.

2 Mitigation

UBNETDEF has a set of recommended activities to clean up this incident, and to prevent intrusions like this in the future.

- Take the infected machine off the network so it can no longer transmit information to the C2 servers, and clean it of any malicious software.
- Block known any unknown addresses attempting to communicate with the infected machine, such as 45.77.166.103, 185.159.130.81, 205.95.112.1, 34.117.65.55, and 69.42.215.252.
- Implement anti-virus on all your clients so that in the event malware is installed, it can be blocked before damage can be done.

UBNETDEF determines these actions to be productive in mitigating incidents through this attack vector again in the future.

3 Contributing Analysts

Lead Analyst: Griffin Refol