PCAP Analysis – RedLine Stealer

https://unit42.paloaltonetworks.com/wireshark-quiz-redline-stealer/

Captured 07/10/2023
Date Analyzed 03/23/2024

The pcap capture was taken 07/10/2023, beginning at 22:39:22.849048 and ended 22:39:58.364177 (UTC). Initial view of the protocol hierarchy showed 94.9% of the captured traffic was TCP. Other notable protocols were for LDAP and Kerberos.

I set the filter to *Frame contains "file"*. This showed hits between 10.7.10.47 and 194.26.135.119. I clicked Follow Conversation and saw lots of packets were between these two systems. Knowing 10.7.10.47 was a local domain system, I ran the other IP into VirusTotal. This was confirmed malicious. Comments in VirusTotal indicated Red Canary.

The conversation between the attacker and the infected system, began with a ACK packet to the attacker. The conversation lasted from 22:39:50.151051 to 22:39:58.364177 (UTC). This shows the infected system was already compromised and was ready to gather information and send to the attacker. Following the TCP conversation it was obvious the malware was gathering all crypto wallets and anything it could find that would hold the credentials. It also gathered data from within Chrome and Firefox, specifically for Microsoft Azure and Amazon tokens. I was not able to review the malware, but based on what was seen in the packets it was possibly putting some of this information into a .docx file. At 22:39:57.806520 (UTC) I see the infected system sending a file Top_Secret_ducment.docx. This looks like it would contain sensitive information like system info, username and password and more.

At 22:39:57.806518 (UTC) – The infected system runs a powershell command: *powershell.exe, CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'C:\Users\rwalters\Documents\mystery_file.ps1*. The command runs the usual execution bypass and runs a mystery_file.ps1 located in the user's Documents directory.

In the TCP conversation the username and password are shown in plain text.

Continued investigating I saw another IP, 204.79.197.200. There was a bit of communication with this IP and the infected system at 22:39:34.644850 until 22:39:43.986040 (UTC). I saw references to docx in the TCP conversation between the infected host and 194.26.135.119. Ran a filter in Wireshark frame contains "docx". Doing this revealed the second IP. Checked the new IP against VirusTotal and it showed malicious. This was a Microsoft IP, but the account associated with this IP was compromised.

The packets between 10.7.10.47 and 204.79.197.200 used TLS V1.2. I was not able to see what the conversation was about because I did not have any of the encryption keys needed.

The entire pcap files ends with the last packet sent from 10.7.10.47 talking to 194.26.135.119 was an ACK to a PSH, ACK packet from the attacker.

Attacker and Infected Host profiles

Attacker 194.26.135.119

- Moscow, Russia
- ISP Chang Way Technologies Co. Ltd
- 17/93 vendors flag this as malicious – tags: red line stealer (C2 server)
- Mac Address 00:b:64:98:ad:54 (Cisco router or firewall)

Infected Host 10.7.10.47

- DESKTOP-9PEA63 – part of domain coolweathercoat.com
- Mac Address: 80:86:5b:ab:1e:c4
- User = rwalter@coolweathercoat[.]com
- Password used is weak My_p@ssw0rd

Additional Observations

- Infected host did communicate with its DC server, 10.7.10.9 -- Dell system - Mac Address: 10:98:36:f4:95:c1. This server is both a DC and a DNS server. The attacker did not communicate directly with it.
- Total packets exchanged between attacker 194.26.135.119 and 10.7.10.47 were 747, 549KBs of data transferred
- Additional compromised MS Office account was talked to by the infected system. 204.79.197.200
- User's credentials were compromised
- Malware was finding tokens and crypto wallets
- Total packet record time under 36 seconds.