AsyncRAT 2024-02-21 PCAP analysis

PCAP file from malware-traffic-analysis.net

Analysis

Started analysis by throwing the pcap file through Zeek. /*opt/zeek/bin/zeek -C -r SocGholish-AsyncRAT-infection.pcap*. Eight logs were extracted from the pcap file.

Opened the DNS logs to see get a general overview of the what sites were accessed. I saw the victim system, **10.2.21.101**. The DNS server for the network was **10.2.21.1**. The victim machine made multiple DNS requests for various domains. Several of these sites immediately caught my attention. These were all .top domains with random character sites. There are some others that looked interesting. I began looking at the top sites in VirusTotal.

- bjlkchhaaigceke[.]top - **167.71.107.109** - Resulted in 13/92 flagged as malicious
- pbvzje4[.]top - **49.13.65.235** - 9/92 - malicious - ID's as SocGholish
- h4cg7rhbmieqskr[.]top - **5.161.113.150** 5/92 - flagged as a bot network

Since the DNS logs only had a few entries I decided to look at another site that seemed a bit suspicious, retraining.allstardriving[.]org **66.135.17.87**. VirusTotal showed 21/90 and marked as a phishing site.

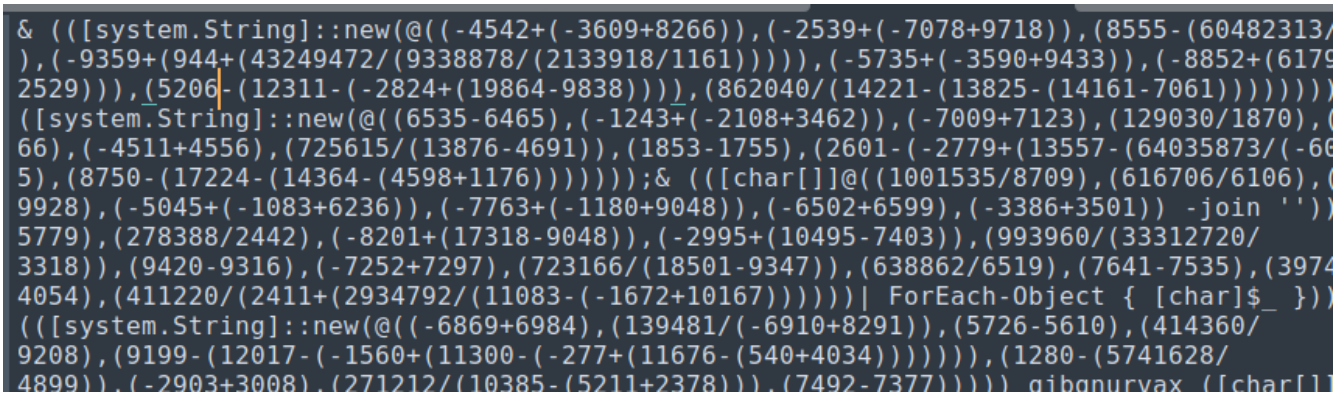
I reviewed the SocGhoulish malware family to see what it does and how it infects a system. This malware is downloaded via an infected site. A phishing email is received. The user clicks a link in the email taking them to the malicious site. The site has embedded javascript that downloads the infection. Usually it will download something that pretends to be a legitimate software update. From this I know there will be files downloaded to the infected system.

I used Wireshark and opened the pcap file. Set the time to UTC and began looking. The pcap file began at 2024-02-21 16:03:37.518881 (UTC) and ended at 2024-02-21 16:28:27.562951 (UTC). Total packets captured was 18,768. We had multiple malicious sites involved. The first packet in the file was the victim system sending a request to the local DNS server for the domain psiewdr[.]org, **72.52.136.210**. Communication between this site and the victim was via HTTPS and all packets were encrypted. Unable to see what was said between the two. Checked the URL against VirusTotal. It flagged it

10/90 as malicious. This information tells me the victim machine was already compromised with something trying to communicate back, or the user on the system clicked on a phishing link. Based on descriptions for SocGhoulish, I suspect the user had clicked the link and gone to the malicious site. This site was the initial stager with the embedded javascript. I tried to see what was on the site using wget, but the site domain was redirected by McAffee Blockpage.

Next decided to view the files Wireshark could see. Checked with HTTP Objects. Interesting files were an svg file, a text document and a php file. All three came two of the top domains I saw in the DNS logs. I downloaded all three to do a bit of investigation.

The svg file was not an svg file. I checked the file command and opened it in Sublime-text. When I reviewed it there was obfuscated PowerShell code. The other two also had PowerShell code. The way the code was encoded, was each letter was char code. The code for each letter was hidden within basic mathematical equations, like ~~4542+(~~3689+8266).



The code was long so I decided to run a few of the lines through Python to get me the char code values. I decoded each one by a char code table and got some basic commands like ForEach-Object and so on. I decided to throw the scripts into App.any.run and see what was going on.

https://app.any.run/tasks/e028dfed-240c-45e7-b803-d5ed85c4e708

The PowerShell scripts were downloading and compiling code. Creating the final stage binary that would communicate with a C2 server.

I went back to the pcap analysis and reviewed some of the TCP streams. In these the PowerShell scripts were in plaintext format and I could see them within various streams.

Reaching the end of my analysis I checked out one more domain that was listed in the DNS logs. This one was also aphqj.members.openarmscv[.]com **45.59.170.106**. This was also marked as malicious.

Unable to get anything from the offending sites. They are either down or blocked.