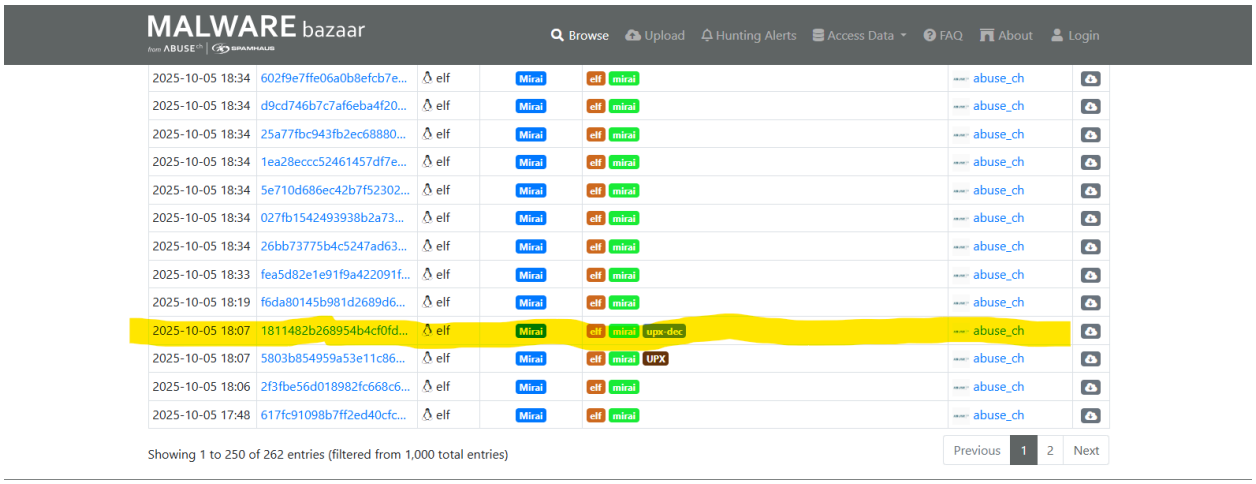
# Lab #4: Malware Analysis

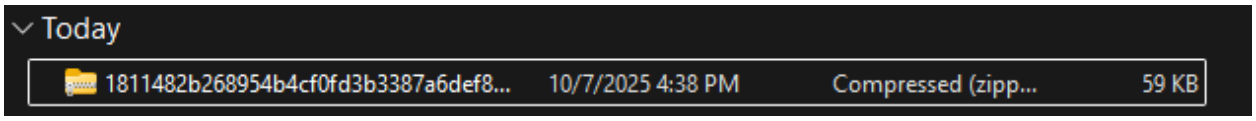
Destiny Hale

10/7/25

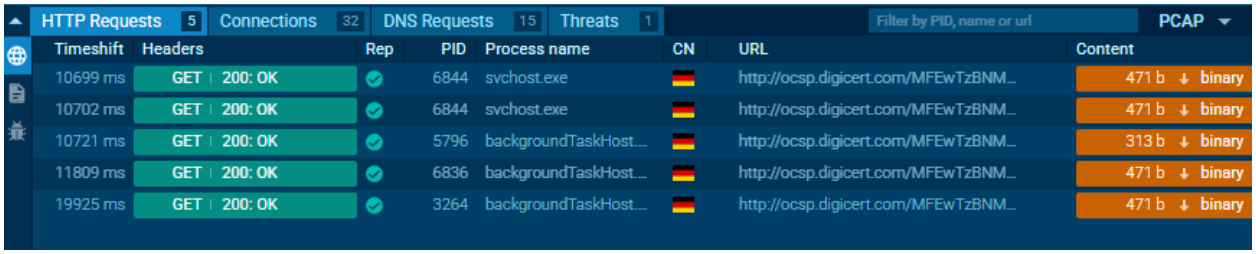
**Task-1: Go to https://bazaar.abuse.ch/browse/ and select a malware with the “Mirai” signature. Use the “Signature” column to find out all the malwares with the “Mirai” signature or use the search option with the “Mirai” keyword. Take a screenshot like the following screenshot and make sure you highlight the malware you selected. 2 points**




**Task-2: Read the details of the selected malware and download the malware sample using the “download sample” link. Take a screenshot showing the downloaded malware sample in your computer. 2 points**

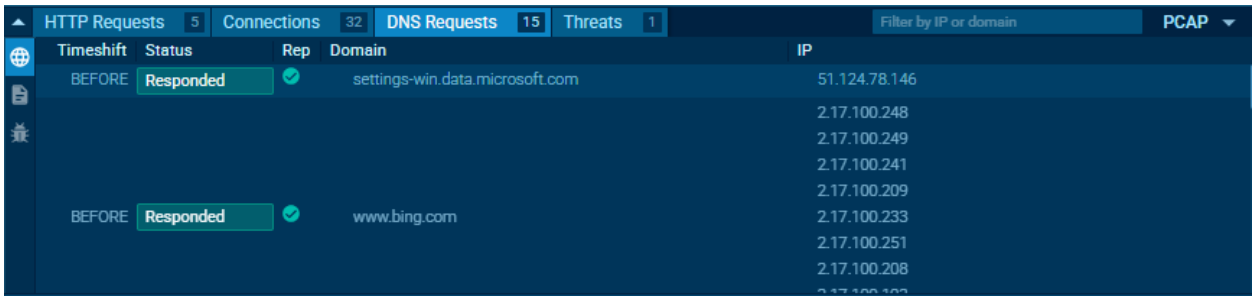



**Go through all the information you find for each category (i.e., Http Requests, Connections, DNS Requests, and Threats) and take at least one screenshot showing information from each category. 8 points**
**HTTP Requests:**

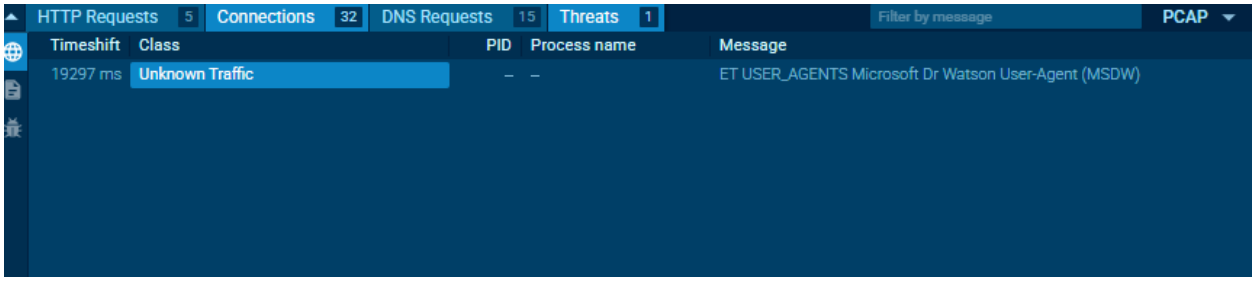



**Connections:**

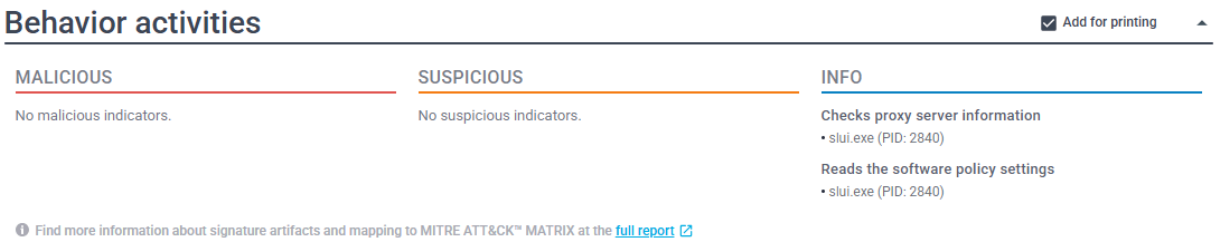

**DNS Requests:**




**Threats:**



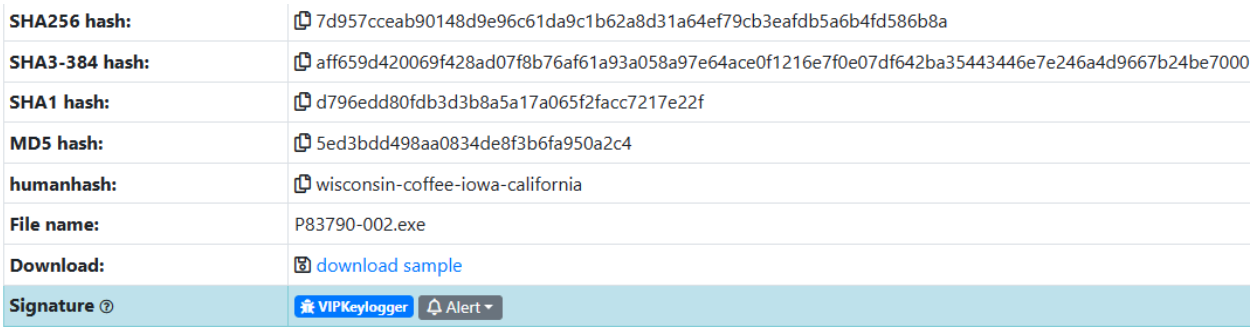

**Task-7: Explore information found in the IOC, Text Report, Graph, and ATT&CK tabs on the right side of the screen. Take necessary screenshots showing any interesting finding. 3 points**

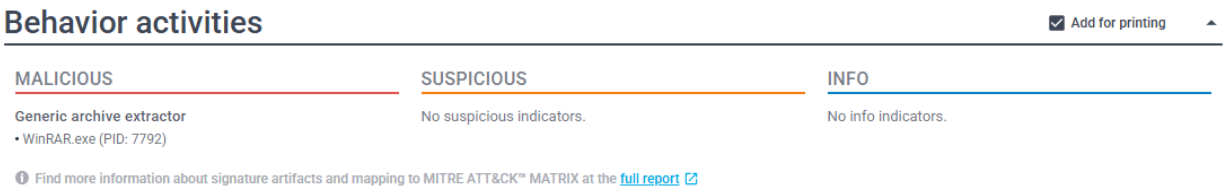



**Task-8: Based on the information you found from Task-6 and Task-7, briefly explain the main characteristics of the malware sample. 5 points**

- This malware checks proxy server information and reads software policy settings. From these two actions, it was able to bypass network security measures, modify software settings, and bypass security measures within the system. No further activity was found.

**Task-9: Go to https://bazaar.abuse.ch/browse/ again, but this time, select a malware sample with the "VIPKeylogger" signature. Perform malware analysis repeating Task-3 to Task-7. Based on your analysis, explain the main characteristics of this malware sample. 5 points**

- 

- 

- This keylogging malware is a generic archive extractor. However, no other activity was found.

**Task-10: Discuss the difference between Mirai and VIPKeylogger malwares in your own words. 5 points**

- Although Mirai and VIPKeylogging are both forms of malware, they have different tactics. Keylogging is a spyware that involves monitoring every keystroke made on a user's device. This creates an advantage for attackers to steal credentials and other

sensitive information. On the other hand, Mirai involves infecting devices and turning them into a botnet to carry out malicious attacks such as DDoS. This disrupts system operations and makes applications unavailable to the user.