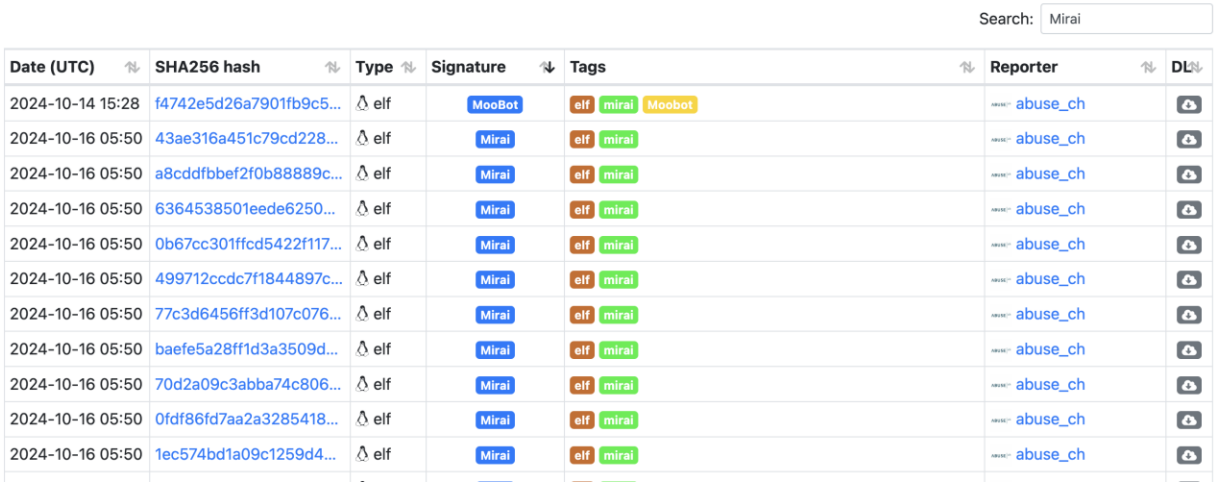
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

Lab 3: Malware Analysis

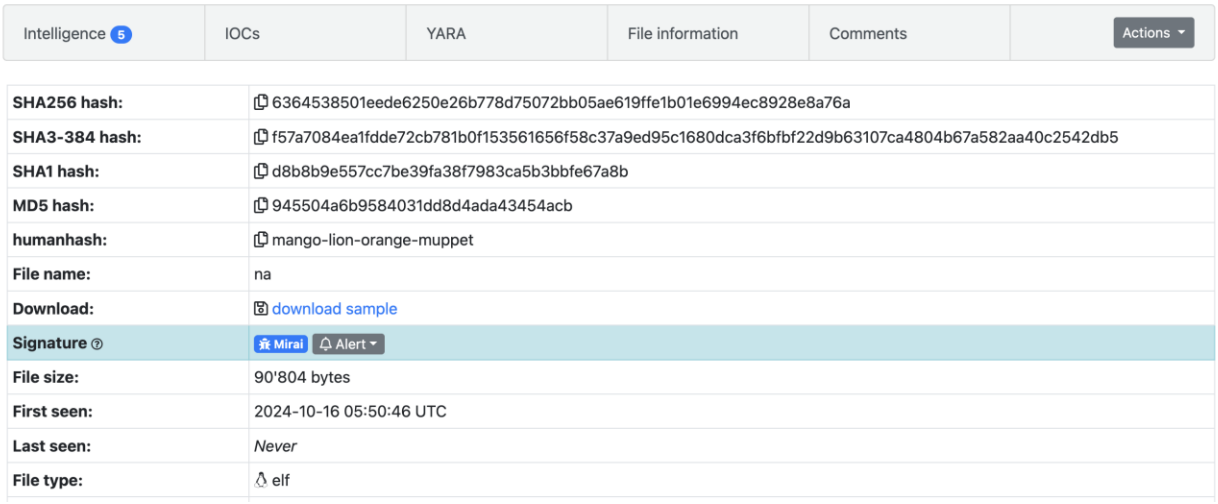
Handout Date: February 27, 2025
Due Date: March 07, 2025, 11:59 pm
Total Points: 30

Tasks

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 similar to 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**



Task-3: Go to https://app.any.run/ and sign up using your ***odu.edu*** email. You will be sent a verification link through email. Use the link to log in to the ***any.run*** dashboard.

Task-4: In ***any.run*** dashboard, choose the "**Submit File / Email**" option to select the previously downloaded malware sample in order to upload for the analysis.

Task-5: Once the malware sample is selected, click on the "**Run a public analysis**" button to upload the sample and run a malware analysis.

Task-6: In the bottom part of the ***any.run*** screen, you will find information about ***HTTP Requests***, ***Connections***, ***DNS Requests***, and ***Threats*** under the ***Network*** tab. Here goes an example:

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**

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**

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**

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

Turn-in

- Submit all the screenshots and explanations highlighted using the yellow background.