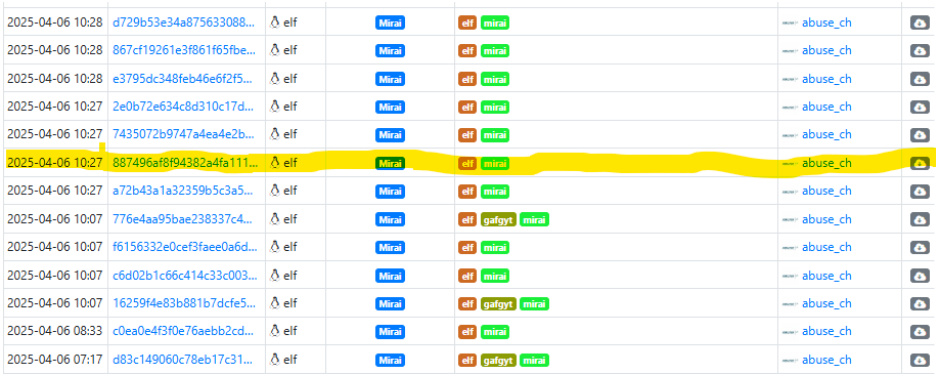
Lab 3: Malware Analysis

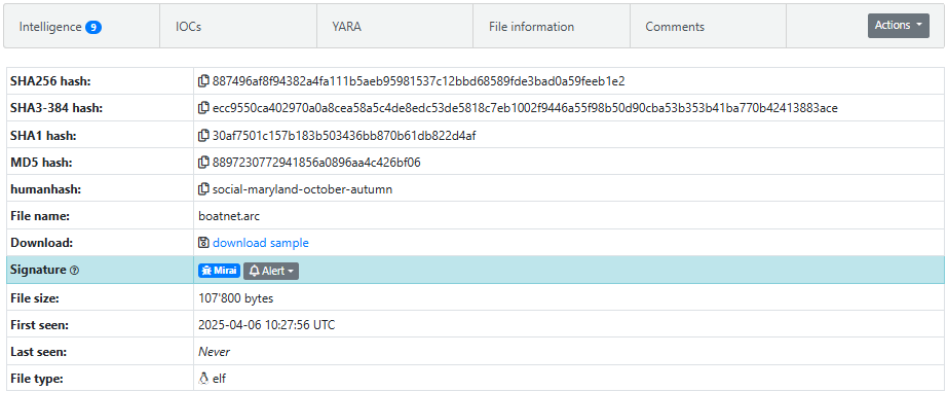
Task-1: Go to https://bazaar.abuse.ch/browse/ and select a malware with the "**Mirai**" signature. Use the "**Signature**" column to find out all the malwares with the "***Mirai***" signature or use the search option with the "**Mirai**" keyword. Take a screenshot similar to the following screenshot

and make sure you highlight the malware you selected. **2 points**



2025-04-06 10:28	d729b53e34a875633088...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:28	867cf19261e3f861f65fbe...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:28	e3795dc348feb46e6f2f5...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:27	2e0b72e634c8d310c17d...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:27	7435072b9747a4ea4e2b...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:27	887496af8f94382a4fa111...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:27	a72b43a1a32359b5c3a5...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:07	776e4aa95bae238337c4...	elf	Mirai	elf gafgyt mirai	abuse_ch	
2025-04-06 10:07	f6156332e0cef3faee0a6d...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:07	c6d02b1c66c414c33c003...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 10:07	16259f4e83b881b7dcfe5...	elf	Mirai	elf gafgyt mirai	abuse_ch	
2025-04-06 08:33	c0ea0e4f3f0e76aebb2cd...	elf	Mirai	elf mirai	abuse_ch	
2025-04-06 07:17	d83c149060c78eb17c31...	elf	Mirai	elf gafgyt mirai	abuse_ch	

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**



Intelligence 5 | IOCs | YARA | File information | Comments | Actions

SHA256 hash:	887496af8f94382a4fa111b5aeb95981537c12bbd68589fde3bad0a59feeb1e2
SHA3-384 hash:	ecc9550ca402970a0a8cea58a5c4de8edc53de5818c7eb1002f9446a55f98b50d90cba53b353b41ba770b42413883ace
SHA1 hash:	30af7501c157b183b503436bb870b61db822d4af
MD5 hash:	8897230772941856a0896aa4c426bf06
humanhash:	social-maryland-october-autumn
File name:	boatnet.arc
Download:	download sample
Signature	Mirai Alert
File size:	107'800 bytes
First seen:	2025-04-06 10:27:56 UTC
Last seen:	*Never*
File type:	elf

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.

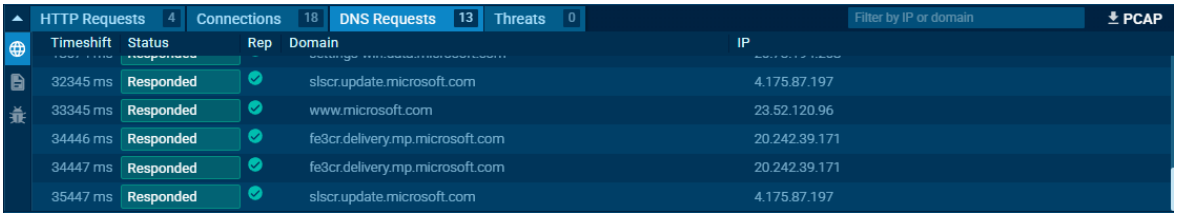
Task-6: In the bottom part of the ***any.run*** screen, you will find information about ***HTTP Requests***, ***Connections***, ***DNS Requests***, and ***Threats*** under the ***Network*** tab. Here goes an example:

Http Requests

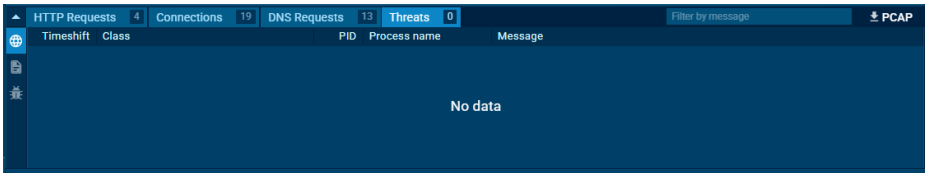
Go through all the information you find for each category (i.e., ***Http Requests***, ***Connections***, ***DNS Requests***, and ***Threats***) and take at least one screenshot showing information from each category. **8 points**

Connections

DNS Requests

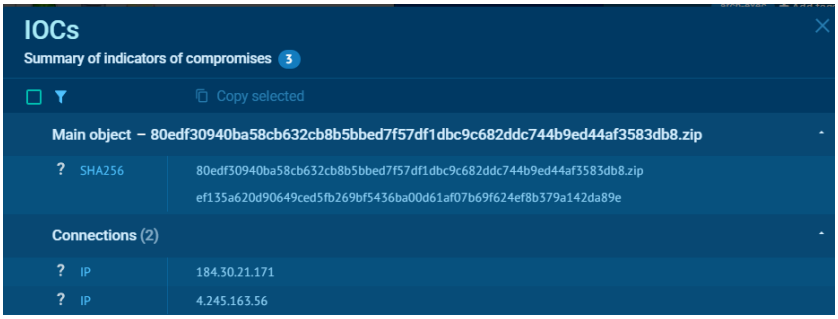


Threats

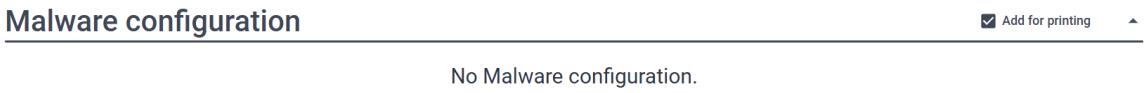


Task-7: Explore information found in the ***IOC***, ***Text Report***, ***Graph***, and ***ATT&CK*** tabs on the right side of the screen. Take necessary screenshots showing any interesting finding. **3 points**

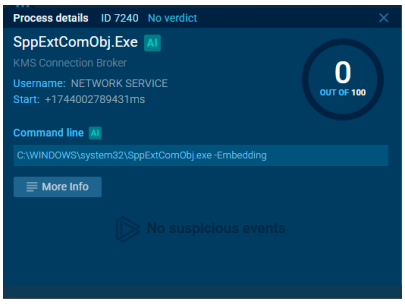
IOC



Text Report



Graph



ATT&CK

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**

The malware sample is a variant of Mirai, which is known for targeting Internet of Things (IoT) devices. It came as a ZIP file containing a program. When the file is run, it uses common Windows processes like svchost.exe and SIHClient.exe to make network requests to trusted domains like Microsoft and DigiCert. This helps it blend in and avoid detection. The sandbox analysis did not show any obvious malicious behavior, and no attack techniques were triggered, but Mirai is known to activate under specific conditions. It typically affects systems with weak or default credentials, especially older or poorly secured IoT devices. There is no specific patch for this variant, but keeping devices updated, changing default passwords, and avoiding unknown files can help protect against it.

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**

A ZIP file that opens with WinRAR.exe conceals the VIPKeylogger malware. When it runs, it uses normal-looking Windows programs like MoUsoCoreWorker.exe and SIHClient.exe to connect to Microsoft websites. These connections seem safe, which helps the malware hide. The test revealed no obvious threats or attacks, suggesting that the malware is likely attempting to remain undetected. Since it acts like a keylogger, it may secretly record what the user types. To stay safe, don't open unknown ZIP files, and make sure your system and antivirus are always up to date.

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

Mirai is a type of malware that attacks smart devices like routers, cameras, and smart TVs. It searches for devices that use weak or default passwords and takes control of them. Once it infects enough devices, it builds a large group called a botnet. By sending excessive traffic, this botnet can attack websites, causing them to slow down or crash. Mirai spreads quickly by scanning the internet for more devices to infect.

VIPKeylogger, on the other hand, is a spying tool that runs on regular computers. Its main job is to secretly record everything a person types, such as passwords, emails, or credit card details. It hides by using trusted system processes, so it's harder to detect. Unlike Mirai, VIPKeylogger doesn't spread across devices or attack websites; it focuses on stealing personal information from one computer at a time.

Turn-in

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