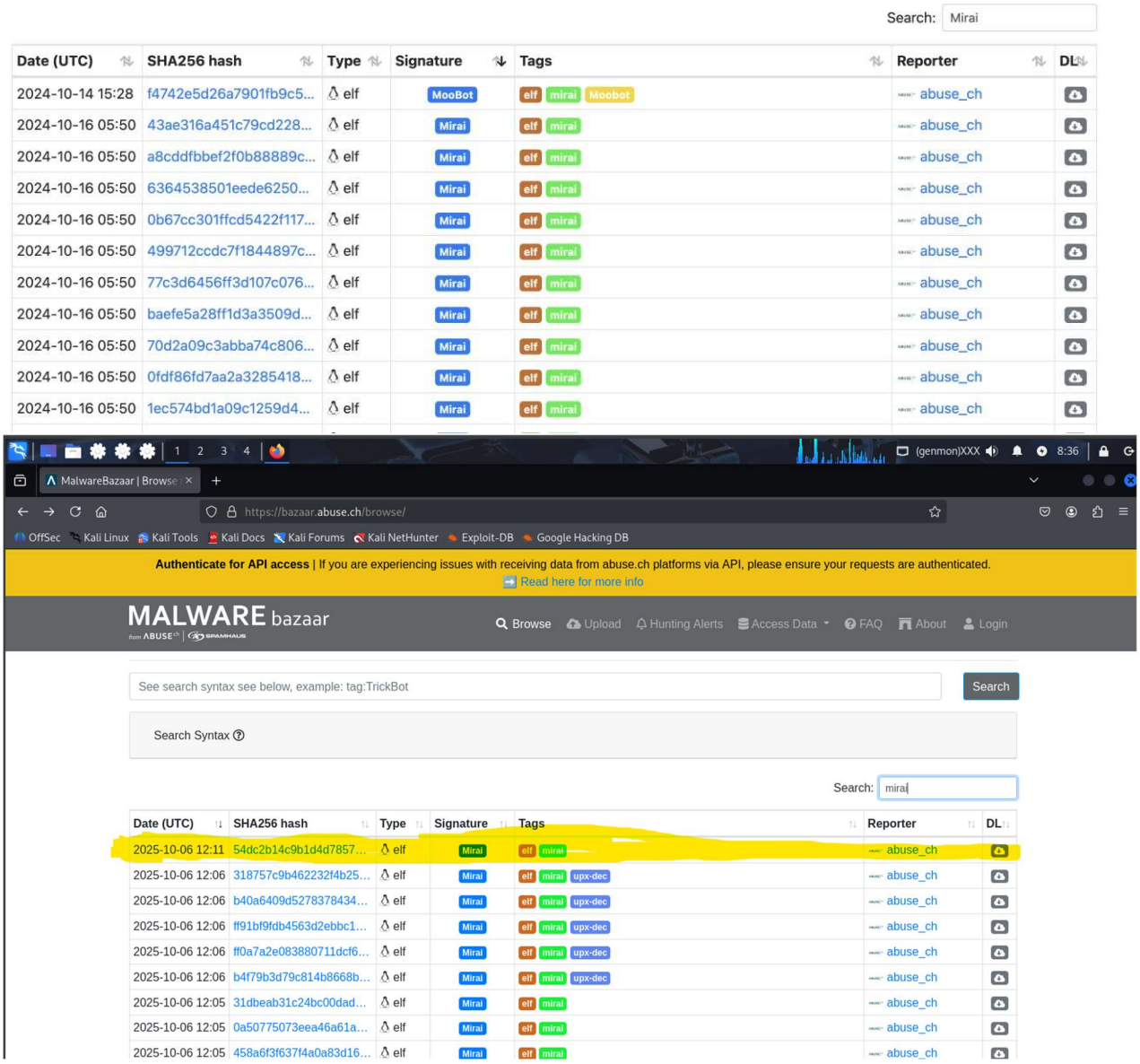
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

Lab 4: Malware Analysis

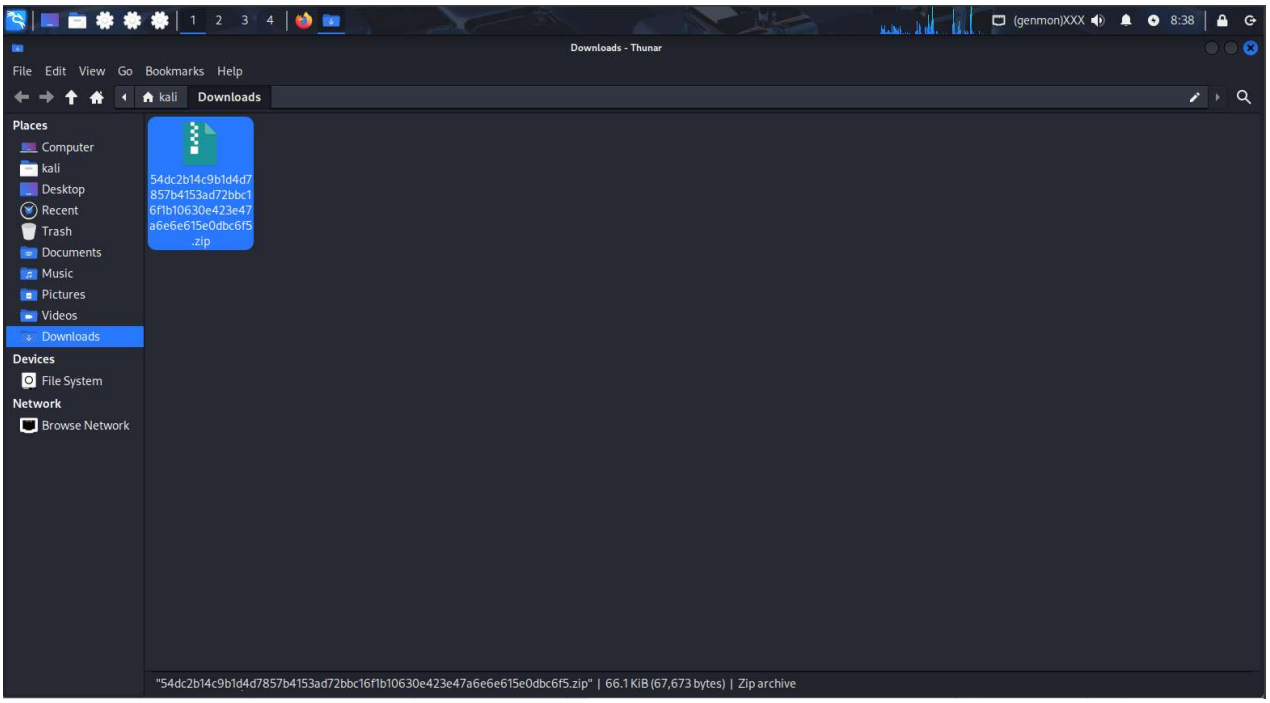
Total Points: 30

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 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**



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

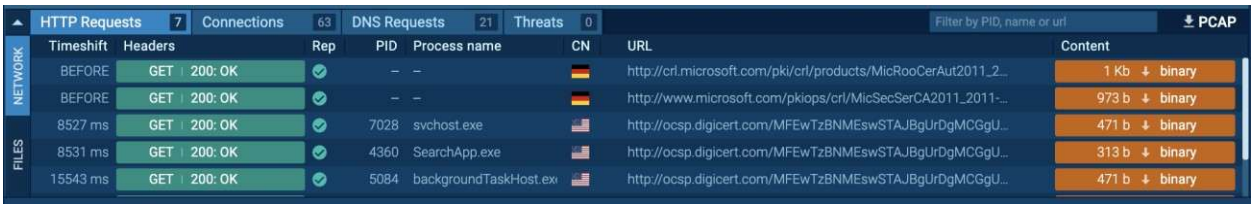
SHA256 hash:	6364538501eede6250e26b778d75072bb05ae619ffe1b01e6994ec8928e8a76a
SHA3-384 hash:	f57a7084ea1fdde72cb781b0f153561656f58c37a9ed95c1680dca3f6bfbf22d9b63107ca4804b67a582aa40c2542db5
SHA1 hash:	d8b8b9e557cc7be39fa38f7983ca5b3bbfe67a8b
MD5 hash:	945504a6b9584031dd8d4ada43454acb
humanhash:	mango-lion-orange-muppet
File name:	na
Download:	download sample
Signature	Mirai Alert
File size:	90'804 bytes
First seen:	2024-10-16 05:50:46 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.

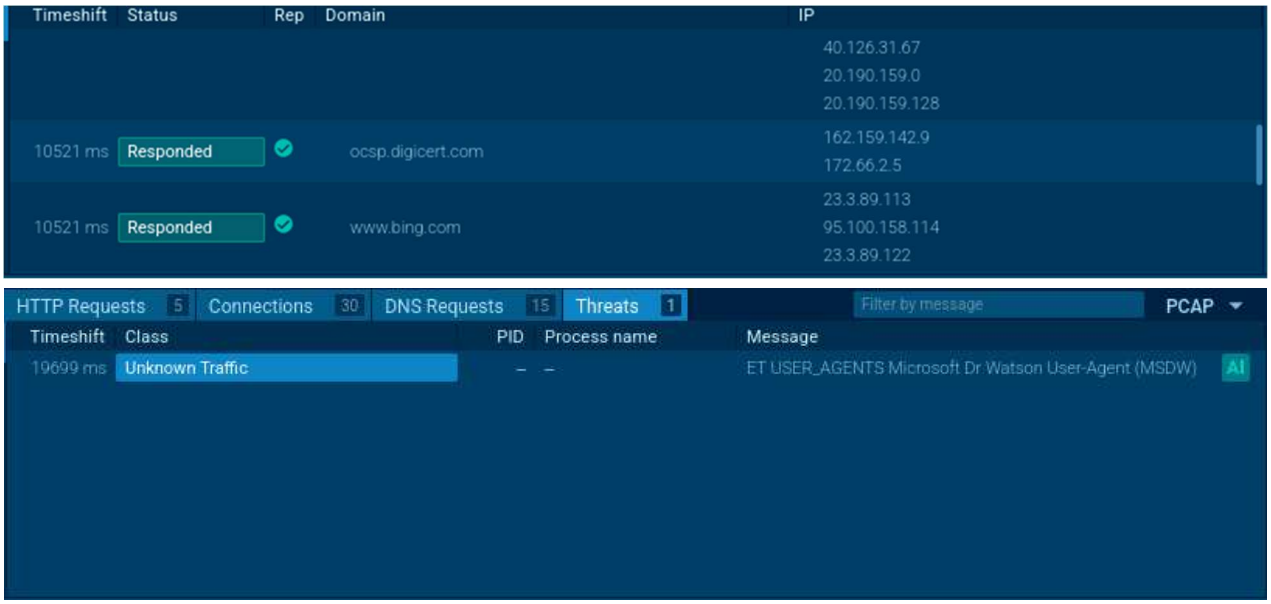
Task-4: In ***any.run*** dashboard, choose the "**Submit File / Email**" option to select the previously downloaded malware sample in order to upload for the analysis.

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.

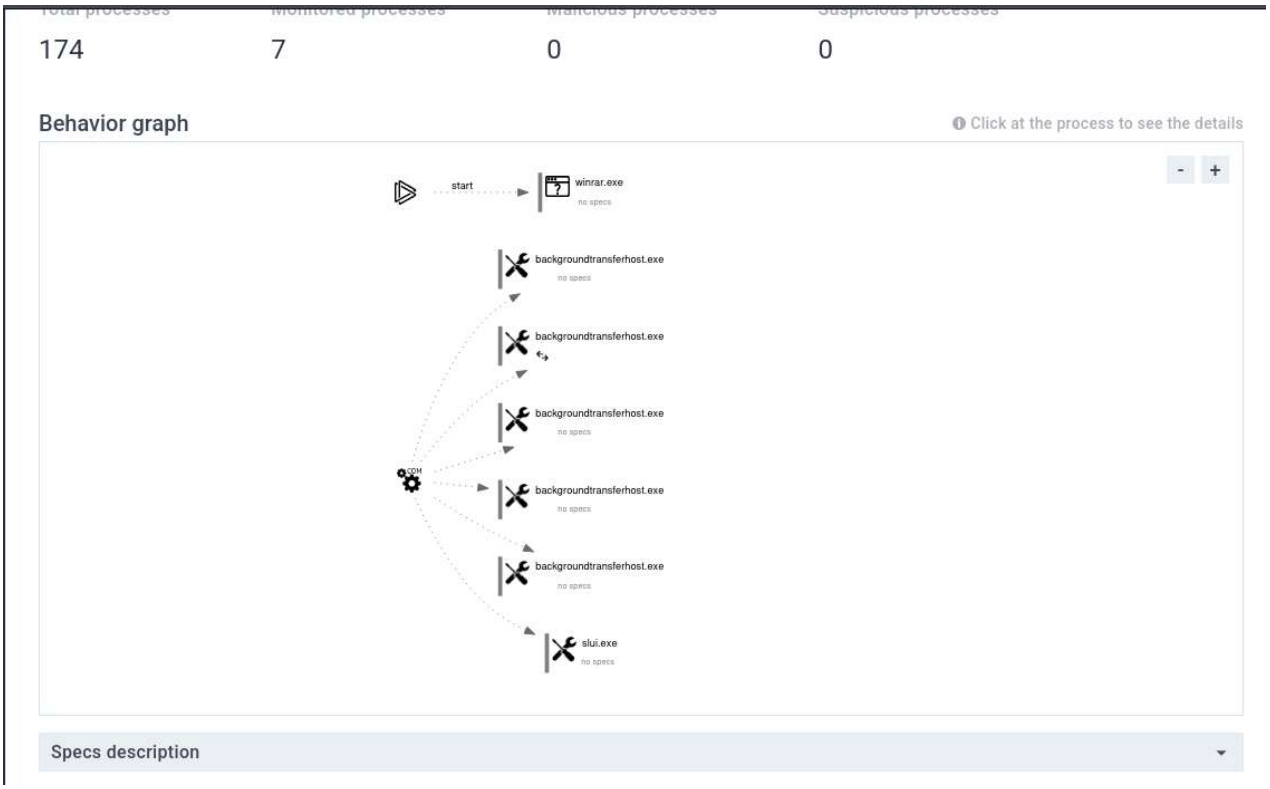
Task-6: In the bottom part of the ***any.run*** screen, you will find information about ***HTTP Requests***, ***Connections***, ***DNS Requests***, and ***Threats*** under the ***Network*** tab. Here goes an example:



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



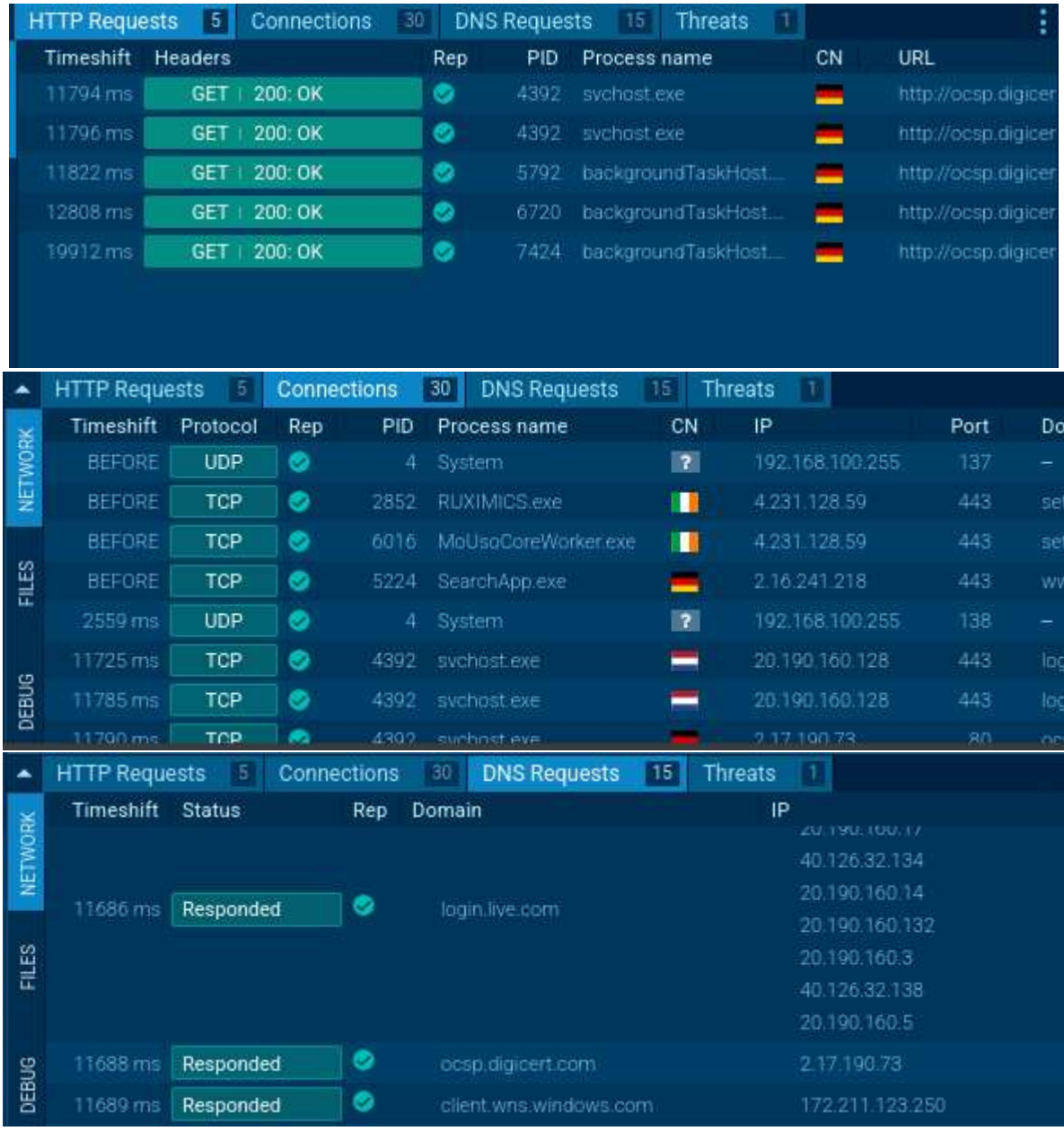
Task-7: Explore information found in the ***IOC***, ***Text Report***, ***Graph***, and ***ATT&CK*** tabs on the right side of the screen. Take necessary screenshots showing any interesting finding. **3 points**



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**

The main characteristic of the malware sample is that it focuses on network connectivity. It opens up a lot of backgroundtransferhost processes.

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


HTTP Requests 5
Connections 30
DNS Requests 15
Threats 1
Timeshift Headers Rep PID Process name CN URL
11794 ms GET | 200: OK 4392 svchost.exe http://ocsp.digicer
11796 ms GET | 200: OK 4392 svchost.exe http://ocsp.digicer
11822 ms GET | 200: OK 5792 backgroundTaskHost... http://ocsp.digicer
12808 ms GET | 200: OK 6720 backgroundTaskHost... http://ocsp.digicer
19912 ms GET | 200: OK 7424 backgroundTaskHost... http://ocsp.digicer
NETWORK
FILES
DEBUG
HTTP Requests 5
Connections 30
DNS Requests 15
Threats 1
Timeshift Protocol Rep PID Process name CN IP Port Dom
BEFORE UDP 4 System 192.168.100.255 137 –
BEFORE TCP 2852 RUXIMICS.exe 4.231.128.59 443 sett
BEFORE TCP 6016 MoUsoCoreWorker.exe 4.231.128.59 443 sett
BEFORE TCP 5224 SearchApp.exe 2.16.241.218 443 ww
2559 ms UDP 4 System 192.168.100.255 138 –
11725 ms TCP 4392 svchost.exe 20.190.160.128 443 logi
11785 ms TCP 4392 svchost.exe 20.190.160.128 443 login
NETWORK
FILES
DEBUG
HTTP Requests 5
Connections 30
DNS Requests 15
Threats 1
Timeshift Status Rep Domain IP
40.126.32.134
11686 ms Responded login.live.com 20.190.160.14
20.190.160.132
20.190.160.3
40.126.32.138
20.190.160.5
11688 ms Responded ocsp.digicert.com 2.17.190.73
11689 ms Responded client.wns.windows.com 172.211.123.250

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

MALICIOUS	SUSPICIOUS	INFO
Generic archive extractor • WinRAR.exe (PID: 5232)	No suspicious indicators.	**Reads the machine GUID from the registry** • 7b3a17448b0ddfcc9732ff9a79a8ef7a7809a405db0d589ec2e dedcd3820074c.exe (PID: 2312) **Checks supported languages** • 7b3a17448b0ddfcc9732ff9a79a8ef7a7809a405db0d589ec2e dedcd3820074c.exe (PID: 2312) **Reads the computer name** • 7b3a17448b0ddfcc9732ff9a79a8ef7a7809a405db0d589ec2e dedcd3820074c.exe (PID: 2312) **Manual execution by a user** • 7b3a17448b0ddfcc9732ff9a79a8ef7a7809a405db0d589ec2e dedcd3820074c.exe (PID: 2312)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

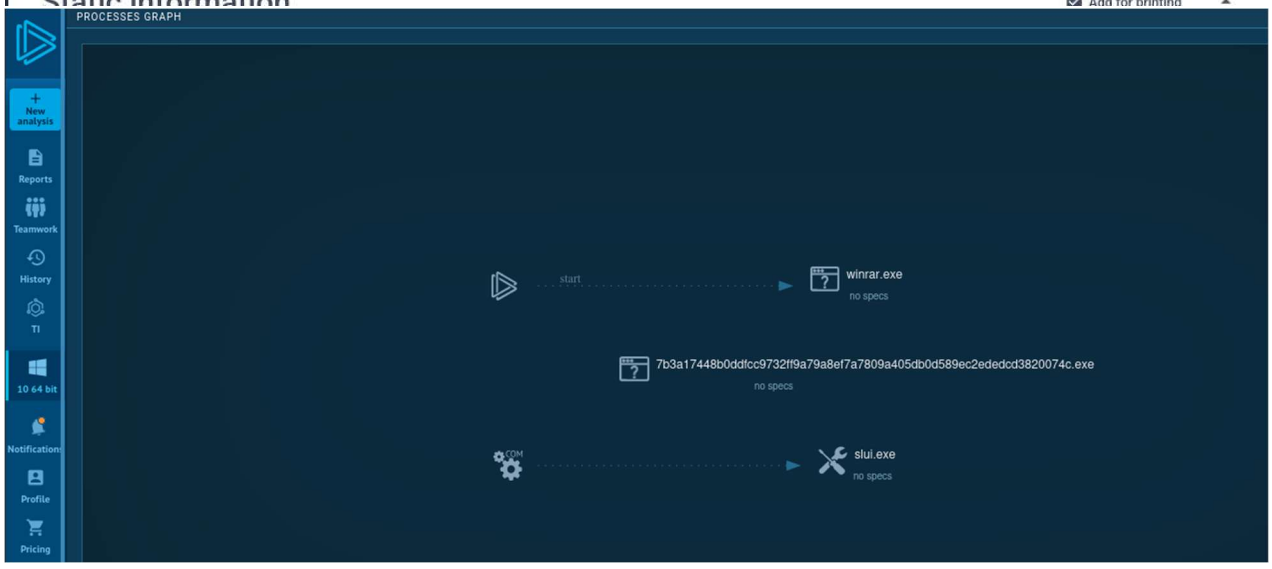
Malware configuration

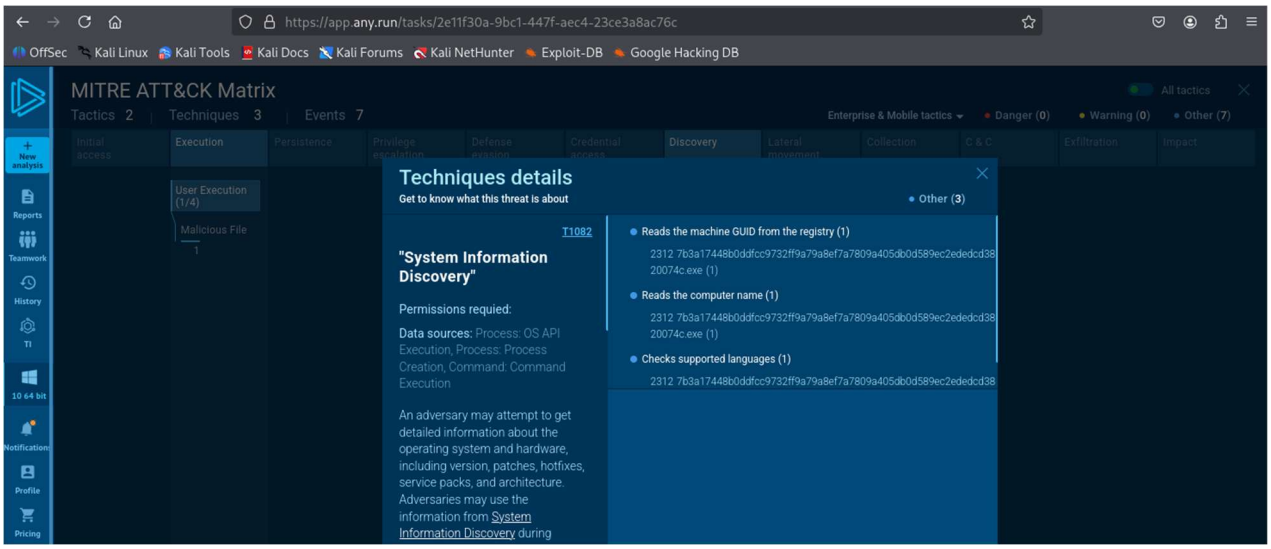
Add for printing

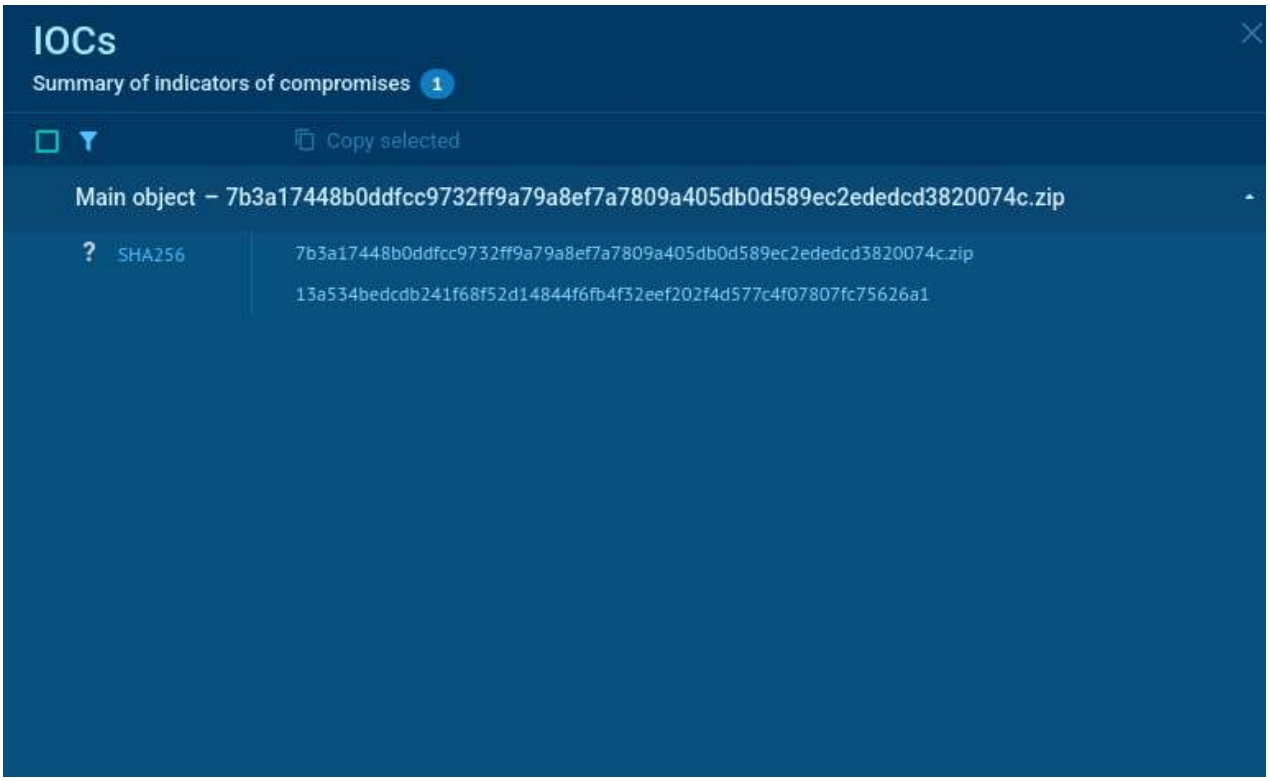
No Malware configuration.

Static information

Add for printing







The VIPKeylogger works by using a .exe file, and it reads information from the registry like the machine GUID, computer name, and the supported languages.

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

5 points

The difference between Mirai and VIPKeylogger is that Mirai focuses more on networks while the VIPKeylogger focuses more on internal functions in the computer. The Mirai virus has more network activity than the VIPKeylogger does.

Turn-in

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