

## 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**

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-10-14 15:28	f4742e5d26a7901fb9c5...	elf	MooBot	elf mirai Moobot	abuse_ch	DL
2024-10-16 05:50	43ae316a451c79cd228...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	a8cddfbbef2f0b88889c...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	6364538501eede6250...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	0b67cc301ffcd5422f117...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	499712ccdc7f1844897c...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	77c3d6456ff3d107c076...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	baefe5a28ff1d3a3509d...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	70d2a09c3abba74c806...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	0fdf86fd7aa2a3285418...	elf	Mirai	elf mirai	abuse_ch	DL
2024-10-16 05:50	1ec574bd1a09c1259d4...	elf	Mirai	elf mirai	abuse_ch	DL

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated. [Read here for more info](#)

**MALWARE** bazaar

Search:

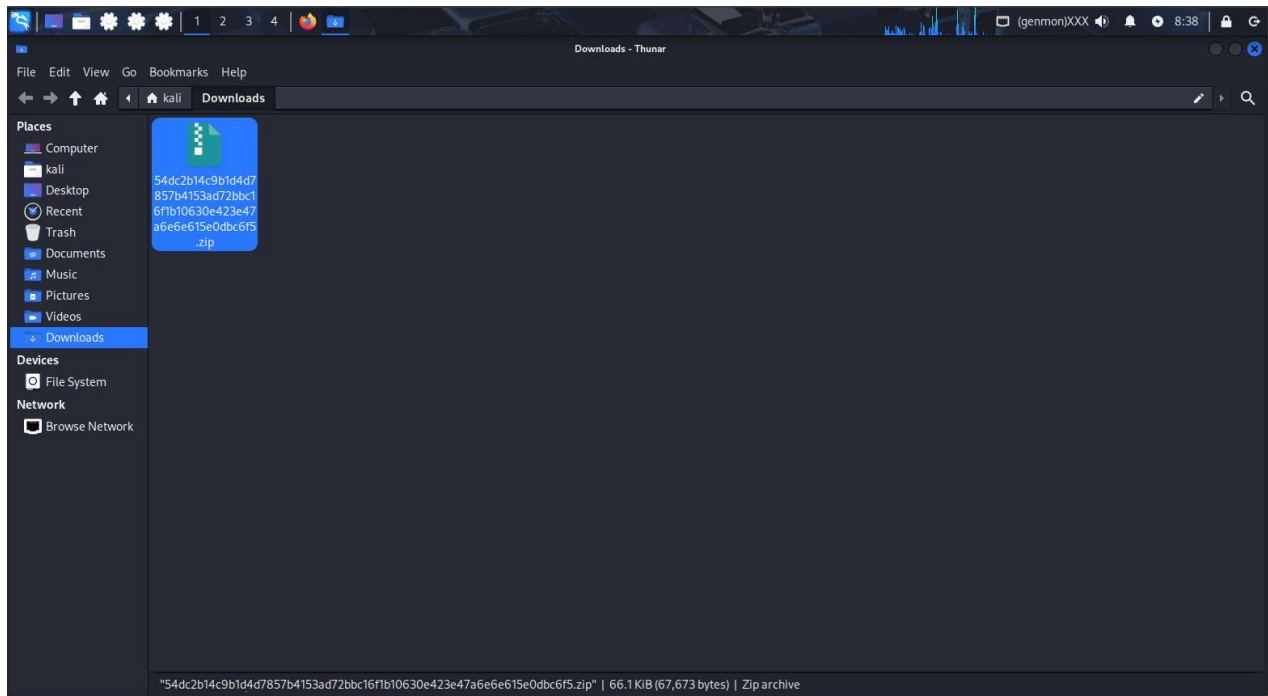
See search syntax see below, example: tag:TrickBot

Search Syntax [?](#)

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-10-06 12:11	54dc2b14c9b1d4d7857...	elf	Mirai	elf mirai	abuse_ch	DL
2025-10-06 12:06	318757c9b46223244b25...	elf	Mirai	elf mirai upx-dec	abuse_ch	DL
2025-10-06 12:06	b40a6409d5278378434...	elf	Mirai	elf mirai upx-dec	abuse_ch	DL
2025-10-06 12:06	#91b9fdb4563d2ebbc1...	elf	Mirai	elf mirai upx-dec	abuse_ch	DL
2025-10-06 12:06	#0a7a2e083880711dcf6...	elf	Mirai	elf mirai upx-dec	abuse_ch	DL
2025-10-06 12:06	b4f79b3d79c814b8668b...	elf	Mirai	elf mirai upx-dec	abuse_ch	DL
2025-10-06 12:05	31dbeab31c24bc00dad...	elf	Mirai	elf mirai	abuse_ch	DL
2025-10-06 12:05	0a50775073eea46a61a...	elf	Mirai	elf mirai	abuse_ch	DL
2025-10-06 12:05	458a6f3f637f4a0a83d16...	elf	Mirai	elf mirai	abuse_ch	DL

**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**

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing



Intelligence	IOCs	YARA	File information	Comments	Actions
<b>SHA256 hash:</b>	<a href="#">6364538501eede6250e26b778d75072bb05ae619ffe1b01e6994ec8928e8a76a</a>				
<b>SHA3-384 hash:</b>	<a href="#">f57a7084ea1fdde72cb781b0f153561656f58c37a9ed95c1680dca3f6bfbf22d9b63107ca4804b67a582aa40c2542db5</a>				
<b>SHA1 hash:</b>	<a href="#">d8b8b9e557cc7be39fa38f7983ca5b3bbfe67a8b</a>				
<b>MD5 hash:</b>	<a href="#">945504a6b9584031dd8d4ada43454acb</a>				
<b>humanhash:</b>	<a href="#">mango-lion-orange-muppet</a>				
<b>File name:</b>	na				
<b>Download:</b>	<a href="#">download sample</a>				
<b>Signature</b>	<a href="#">Miral</a> <a href="#">Alert</a>				
<b>File size:</b>	90'804 bytes				
<b>First seen:</b>	2024-10-16 05:50:46 UTC				
<b>Last seen:</b>	Never				
<b>File type:</b>	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.

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing

**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	7	Connections	63	DNS Requests	21	Threats	0	Filter by PID, name or url		PCAP
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content				
NETWORK	BEFORE	GET 200: OK	✓	--	--	🇩🇪	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2...	1 Kb ↓ binary				
	BEFORE	GET 200: OK	✓	--	--	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-...	973 b ↓ binary				
FILES	8527 ms	GET 200: OK	✓	7028	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGU...	471 b ↓ binary				
	8531 ms	GET 200: OK	✓	4360	SearchApp.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGU...	313 b ↓ binary				
	15543 ms	GET 200: OK	✓	5084	backgroundTaskHost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGU...	471 b ↓ binary				

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	5	Connections	30	DNS Requests	15	Threats	1	Filter by PID, name or url		PCAP
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content				
NETWORK	10544 ms	GET   200: OK	✓	1320	svchost.exe	?	http://ocsp.digicert.com/MFEwTzBNM...	471 b ↓				
	10547 ms	GET   200: OK	✓	1320	svchost.exe	?	http://ocsp.digicert.com/MFEwTzBNM...	471 b ↓				
	11533 ms	GET   200: OK	✓	7472	backgroundTaskHost...	?	http://ocsp.digicert.com/MFEwTzBNM...	314 b ↓				
	12635 ms	GET   200: OK	✓	7828	backgroundTaskHost...	?	http://ocsp.digicert.com/MFEwTzBNM...	471 b ↓				
	19755 ms	GET   200: OK	✓	7140	backgroundTaskHost...	?	http://ocsp.digicert.com/MFEwTzBNM...	471 b ↓				
	21777 ms	GET   200: OK	✓	8312	BackgroundTransferH...	?	http://ocsp.digicert.com/MFEwTzBNM...	314 b ↓				

		HTTP Requests	5	Connections	30	DNS Requests	15	Threats	1	Filter by PID, domain, name or ip		PCAP
	shift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
NETWORK	FORE	TCP	✓	3000	RUXIMICS.exe	🇮🇪	40.127.240.158	443	settings-win...	MICROSOFT-CO...	No Data	
	FORE	UDP	✓	4	System	?	192.168.100.255	137	--	--	↑ 1 Kb ↓	
	FORE	TCP	✓	6016	MoUsocoreWorker.exe	🇮🇪	40.127.240.158	443	settings-win...	MICROSOFT-CO...	No Data	
	FORE	TCP	✓	5224	SearchApp.exe	🇩🇪	92.123.104.34	443	www.bing.com	Akamai Internati...	↑ 6 Kb ↓	
	0 ms	UDP	✓	4	System	?	192.168.100.255	138	--	--	↑ 2 Kb ↓	
	0 ms	TCP	✓	1320	svchost.exe	🇮🇪	40.126.31.129	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb ↓	
	5 ms	TCP	✓	1320	svchost.exe	🇮🇪	40.126.31.129	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb ↓	

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing

The screenshot displays a network analysis tool interface. The top section shows a list of traffic entries with columns for Timeshift, Status, Rep, Domain, and IP. Two entries are visible, both with a 'Responded' status and a green checkmark. The bottom section shows a summary of traffic types: HTTP Requests (5), Connections (30), DNS Requests (15), and Threats (1). Below this is a table of messages with columns for Timeshift, Class, PID, Process name, and Message. One message is visible, classified as 'Unknown Traffic' and originating from 'ET USER\_AGENTS Microsoft Dr Watson User-Agent (MSDW)'.

Timeshift	Status	Rep	Domain	IP
				40.126.31.67
				20.190.159.0
				20.190.159.128
10521 ms	Responded	✓	ocsp.digicert.com	162.159.142.9
				172.66.2.5
				23.3.89.113
10521 ms	Responded	✓	www.bing.com	95.100.158.114
				23.3.89.122

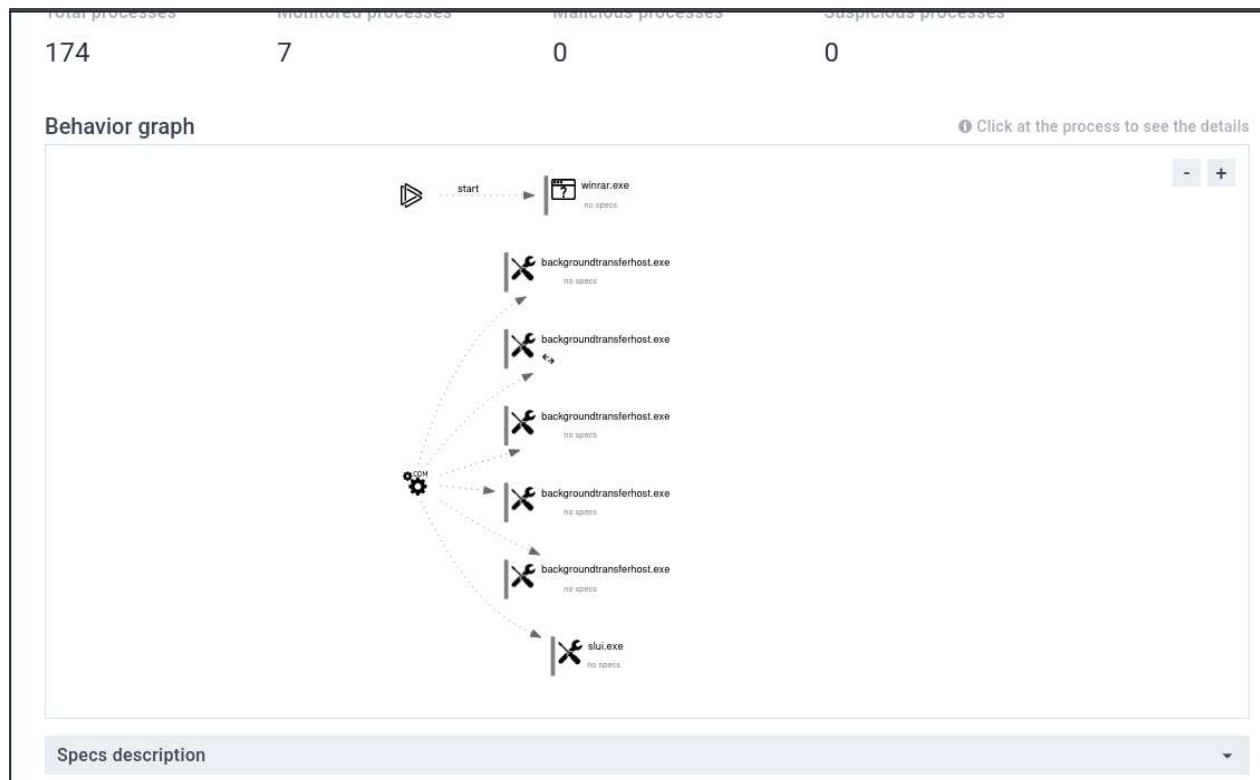
HTTP Requests	Connections	DNS Requests	Threats	Filter by message	PCAP
5	30	15	1		▼

Timeshift	Class	PID	Process name	Message
19699 ms	Unknown Traffic	-	-	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

**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**

Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing



**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**

Old Dominion University  
 CYSE 450: Ethical Hacking and Penetration Testing

HTTP Requests		Connections		DNS Requests		Threats	
Timeshift	Headers	Rep	PID	Process name	CN	URL	
11794 ms	GET   200: OK	✓	4392	svchost.exe	🇩🇪	http://ocsp.digicert.com	
11796 ms	GET   200: OK	✓	4392	svchost.exe	🇩🇪	http://ocsp.digicert.com	
11822 ms	GET   200: OK	✓	5792	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com	
12808 ms	GET   200: OK	✓	6720	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com	
19912 ms	GET   200: OK	✓	7424	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com	

HTTP Requests		Connections		DNS Requests		Threats		
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	MoUserCoreWorker.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	login
11785 ms	TCP	✓	4392	svchost.exe	🇩🇪	20.190.160.128	443	login
11790 ms	TCP	✓	4392	svchost.exe	🇩🇪	2.17.190.73	80	ocsp

HTTP Requests		Connections		DNS Requests		Threats	
Timeshift	Status	Rep	Domain	IP			
11686 ms	Responded	✓	login.live.com	20.190.160.17	40.126.32.134	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			

# Old Dominion University

## CYSE 450: Ethical Hacking and Penetration Testing

**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

Generic archive extractor  
• WinRAR.exe (PID: 5232)

#### SUSPICIOUS

No suspicious indicators.

#### INFO

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](#)

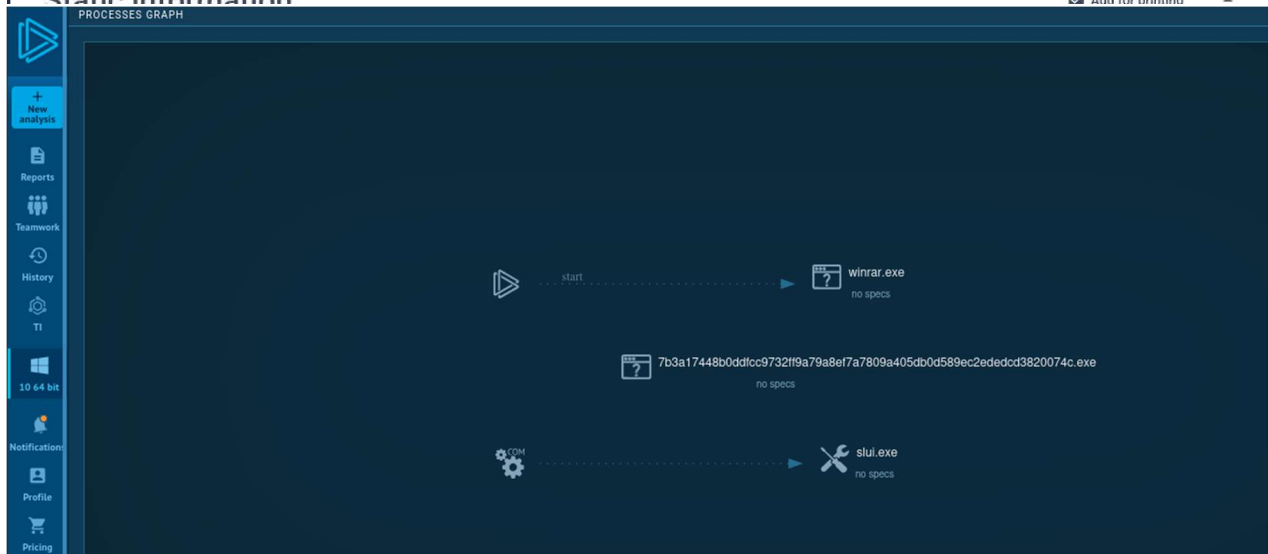
### Malware configuration

Add for printing

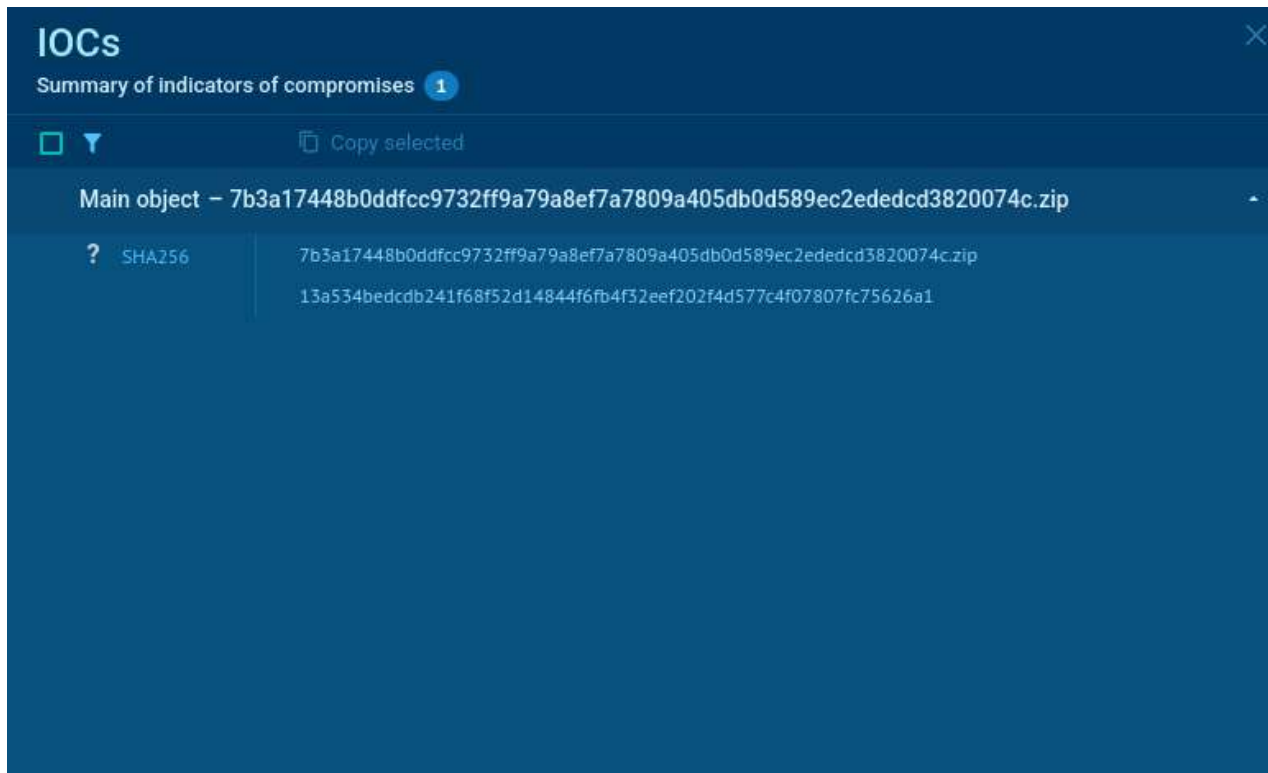
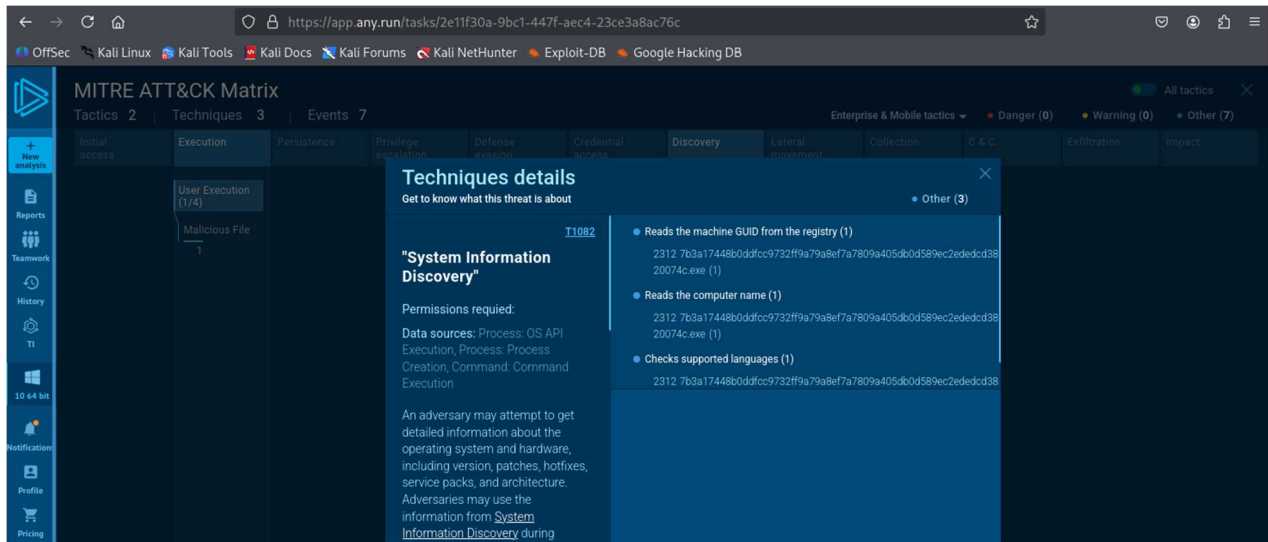
No Malware configuration.

### Static information

Add for printing



Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing



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.