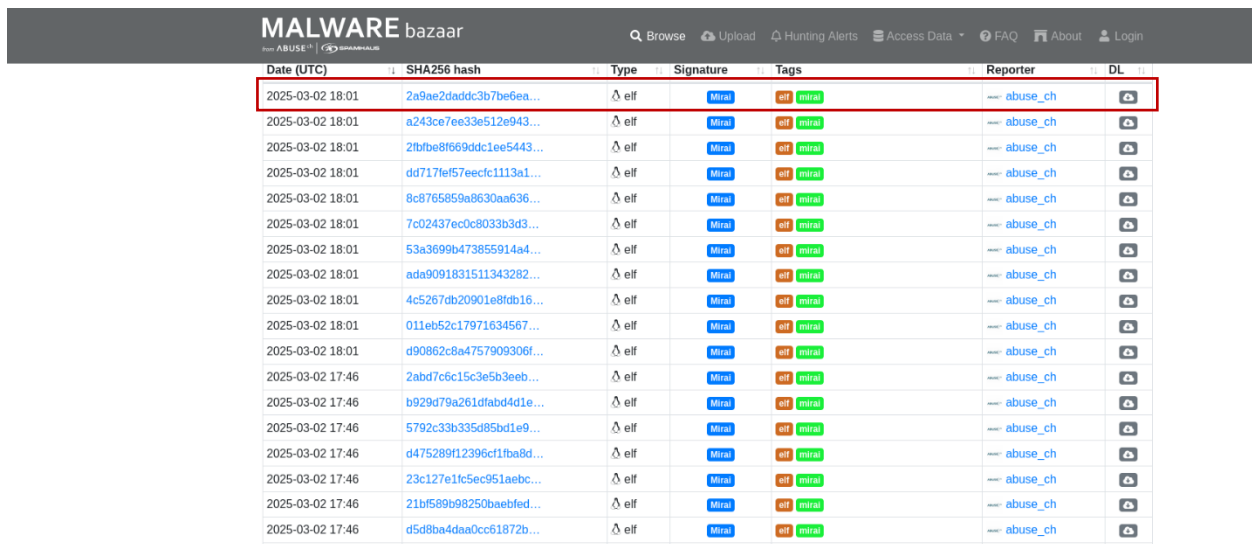


Nick Carpenter  
Old Dominion University  
CYSE 450: Ethical Hacking and Penetration Testing  
Lab 3: Malware Analysis  
Handout Date: February 27, 2025  
Due Date: March 07, 2025, 11:59 pm  
Total Points: 30

---

## Tasks

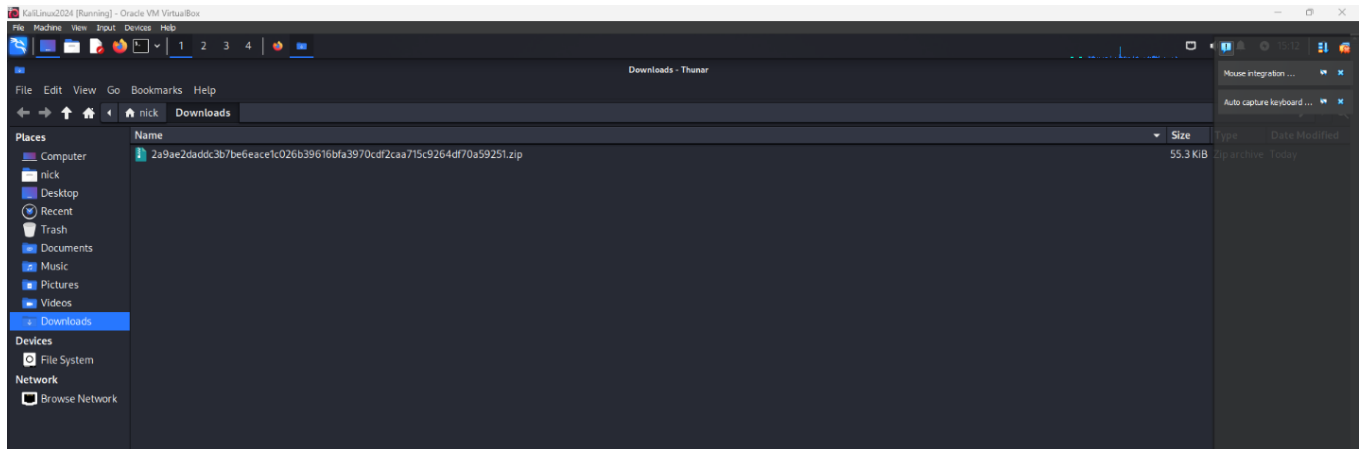
Task-1: Go to <https://bazaar.abuse.ch/browse/> and select a malware with the “Mirai” signature. Use the “Signature” column to find out all the malwares with the “Mirai” signature or use the search option with the “Mirai” keyword. Take a screenshot similar to the following screenshot and make sure you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



The screenshot shows the MALWARE bazaar interface. The table below lists malware samples with columns for Date (UTC), SHA256 hash, Type, Signature, Tags, Reporter, and DL. The first row is highlighted with a red box.

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-03-02 18:01	2a9ae2daddc3b7be6ea...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	a243ce7ee33e512e943...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	2fbf8e8f69ddc1ee5443...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	dd717ef57eefc1113a1...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	8c876589a8630aa636...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	7c02437ec0c8033b3d3...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	53a3699b473855914a4...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	ada9091831511343282...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	4c5267db20901e8f0b16...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	011eb52c17971634567...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 18:01	d90862c8a4757909306f...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	2abd7c6c15c3e5b3eeb...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	b929d79a261dfabd441e...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	5792c33b335d85bd1e9...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	d475289f12396cf1fba8d...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	23c127e1fc5ec951aebc...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	21b1589b98250baebfed...	elf	Mirai	elf mirai	abuse_ch	DL
2025-03-02 17:46	d5d8ba4daa0cc61872b...	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



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**

## HTTP Requests and details:

### Request details AI

Here are the details of your request

#### Request

- URL: /pkips/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl
- Method: GET
- Connection: Keep-Alive
- Accept: \*/\*
- User-Agent: Microsoft-CryptoAPI/10.0
- Host: www.microsoft.com

#### Response

- Status code: 200: OK
- Content-Length: 419
- Content-Type: application/octet-stream
- Content-MD5: tpxzjHHJR/0Stm1JGd+EpQ==
- Last-Modified: Fri, 10 Jan 2025 20:45:10 GMT
- ETag: 0x8DD31B7AD03C01E
- X-ms-request-id: 97b0f825-901e-005a-35a7-63310d000000
- X-ms-version: 2009-09-19
- X-ms-lease-status: unlocked
- X-ms-blob-type: BlockBlob
- Date: Mon, 03 Mar 2025 12:04:37 GMT

#### Connection

keep-alive

HTTP Requests 2   Connections 18   DNS Requests 11   Threats 0									
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content	
NETWORK	29189 ms	GET   200-OK	✔	8120	SIHClient.exe	🇮🇹	http://www.microsoft.com/pkips/crl/Microsoft%20ECC%20Product%20Root%20Cert...	419 b	↓ binary
	29192 ms	GET   200-OK	✔	8120	SIHClient.exe	🇮🇹	http://www.microsoft.com/pkips/crl/Microsoft%20ECC%20Update%20Secure%20Se...	408 b	↓ binary
FILES									

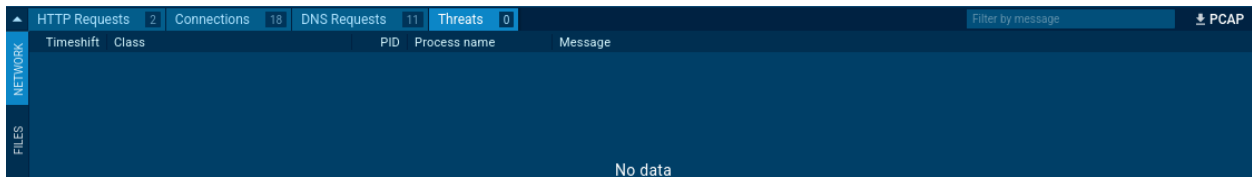
## DNS Requests:

HTTP Requests 2   Connections 18   DNS Requests 11   Threats 0						
	Timeshift	Status	Rep	Domain	IP	
NETWORK	BEFORE	Responded	✔	google.com	142.250.185.142	
	BEFORE	Responded	✔	settings-win.data.microsoft.com	51.104.136.2	
FILES	5560 ms	Responded	✔	client.wns.windows.com	40.113.110.67	

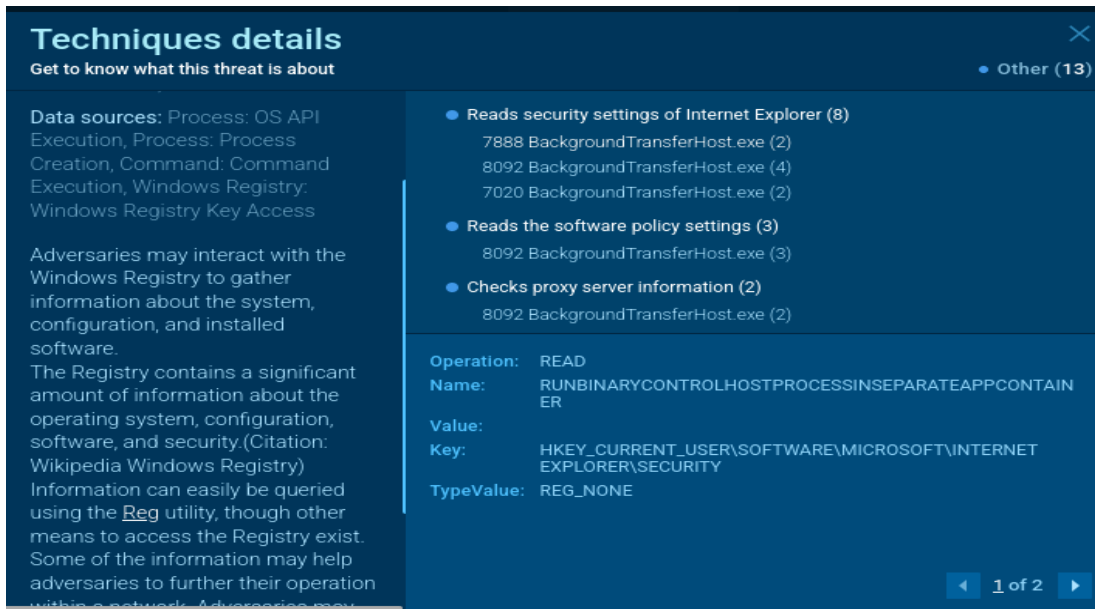
## Connections:

HTTP Requests 2   Connections 18   DNS Requests 11   Threats 0											
	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
NETWORK	BEFORE	UDP	✔	4	System	?	192.168.100.255	137	–	–	↑ 218 b ↓ –
	BEFORE	TCP	✔	–	–	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 4 Kb
FILES	BEFORE	UDP	✔	4	System	?	192.168.100.255	138	–	–	↑ 945 b ↓ –
	BEFORE	TCP	✔	–	–	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 5 Kb
	BEFORE	TCP	✔	–	–	🇮🇹	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 860 b ↓ 4 Kb

Threats: (no current 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



## INFO

### Creates files or folders in the user directory

- BackgroundTransferHost.exe (PID: 5216)

Explanation: ATT&CK provides an overview of the malware and the threats associated with it. In addition, the text file outlines that the malware will create folders in the user directory to help gain access for remotely controlling the system or other means of attack.

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 interacts with the windows registry to gain information about a system to execute commands. Additionally, this malware reads security settings and creates files and folders in the user directory, performing reconnaissance. The commands executed are most commonly associated with Denial of Services attacks.

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**

### Keylogger HTTP Requests:

		HTTP Requests	Connections	DNS Requests	Threats	Filter by PID, name or url		PCAP
	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
FILES	5903 ms	GET   200: OK	✓	6544	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn...	471 b ↓ binary
	7987 ms	GET   200: OK	✓	7896	backgroundTaskHost...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn...	471 b ↓ binary
	9983 ms	GET   200: OK	✓	7376	backgroundTransferH...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn...	313 b ↓ binary
	29386 ms	GET   200: OK	✓	4880	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Cert...	419 b ↓ binary
	29387 ms	GET   200: OK	✓	4880	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Se...	408 b ↓ binary

### Keylogger Connections:

		HTTP Requests	Connections	DNS Requests	Threats	Filter by PID, domain, name or ip		PCAP		
	Timeshift	Protocol	Rep	PID	Process name	IP	Port	Domain	ASN	Traffic
NETWORK	BEFORE	TCP	✓	2104	svchost.exe	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data
	BEFORE	UDP	✓	4	System	192.168.100.255	137	—	—	↑ 286 b ↓ —
FILES	BEFORE	TCP	✓	—	—	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 888 b ↓ 4 Kb
	BEFORE	UDP	✓	—	—	192.168.100.255	138	—	—	↑ 945 b ↓ —
	BEFORE	TCP	✓	—	—	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 4 Kb
	BEFORE	TCP	✓	—	—	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 860 b ↓ 4 Kb
DEBUG	BEFORE	TCP	✓	—	—	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 18 Kb
	4844 ms	TCP	✓	2112	svchost.exe	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 5 Kb
	5855 ms	TCP	✓	3216	svchost.exe	40.113.103.199	443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 4 Kb
	5898 ms	TCP	✓	6544	svchost.exe	20.190.160.65	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 10 Kb ↓ 26 Kb
	5901 ms	TCP	✓	6544	svchost.exe	184.30.131.245	80	ocsp.digicert.com	AKAMAI-AS	↑ 236 b ↓ 875 b
	6841 ms	TCP	✓	3216	svchost.exe	40.113.103.199	443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 3 Kb ↓ 5 Kb
	6846 ms	TCP	✓	6544	svchost.exe	20.190.160.65	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 11 Kb ↓ 28 Kb
	7955 ms	TCP	✓	6544	svchost.exe	20.190.160.65	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 6 Kb ↓ 16 Kb
	7968 ms	TCP	✓	6544	svchost.exe	20.190.160.65	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 6 Kb ↓ 16 Kb
	7978 ms	TCP	✓	7896	backgroundTaskHost...	20.199.58.43	443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 479 b ↓ 6 Kb
	7980 ms	TCP	✓	7896	backgroundTaskHost...	20.199.58.43	443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 479 b ↓ 6 Kb
	7982 ms	TCP	✓	7896	backgroundTaskHost...	20.199.58.43	443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 6 Kb ↓ 18 Kb
	7986 ms	TCP	✓	7896	backgroundTaskHost...	184.30.131.245	80	ocsp.digicert.com	AKAMAI-AS	↑ 240 b ↓ 574 b
	9964 ms	TCP	✓	7376	BackgroundTransferH...	2.22.227.208	443	www.bing.com	Doredo Q.S.C.	↑ 708 b ↓ 7 Kb
	9982 ms	TCP	✓	7376	BackgroundTransferH...	184.30.131.245	80	ocsp.digicert.com	AKAMAI-AS	↑ 234 b ↓ 716 b
	10963 ms	TCP	✓	2104	svchost.exe	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 6 Kb
29378 ms	TCP	✓	4880	SIHClient.exe	4.175.87.197	443	slscc.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 752 b ↓ 3 Kb	
29386 ms	TCP	✓	4880	SIHClient.exe	23.95.229.160	80	www.microsoft.com	AKAMAI-AS	↑ 384 b ↓ 2 Kb	
29395 ms	TCP	✓	4880	SIHClient.exe	13.85.23.206	443	fe3cc.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 602 b ↓ 3 Kb	
30471 ms	TCP	✓	4880	SIHClient.exe	4.175.87.197	443	slscc.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 584 b ↓ 3 Kb	
30474 ms	TCP	✓	4880	SIHClient.exe	4.175.87.197	443	slscc.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 750 b ↓ 3 Kb	

### Keylogger DNS Requests:



## INFO

---

### **Reads security settings of Internet Explorer**

- BackgroundTransferHost.exe (PID: 7800)
- BackgroundTransferHost.exe (PID: 8068)

### **Creates files or folders in the user directory**

- BackgroundTransferHost.exe (PID: 8068)

### **Checks proxy server information**

- BackgroundTransferHost.exe (PID: 8068)

### **Reads the software policy settings**

- BackgroundTransferHost.exe (PID: 8068)

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

Mirai is malware that can produce a wide variety of threats by utilizing the system data from the windows registry. This information can be useful for several hackers, including organized crime and nation states. System information can help hackers achieve executable commands on the user's system, achieve lateral movement on a network to infect other systems, and temporarily take systems offline.

VIPKeylogger create background transfer for files/folders, proxy information, security settings, and software policies and settings. This information is primarily used for credential farming. Credentials that can be transferred to an attacker may include banking information, passwords, pages visited, etc. However, credential farming is usually only used for monetary gain rather than attempting to take a system offline or infect other systems.

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