














Lab 3: Malware Analysis

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

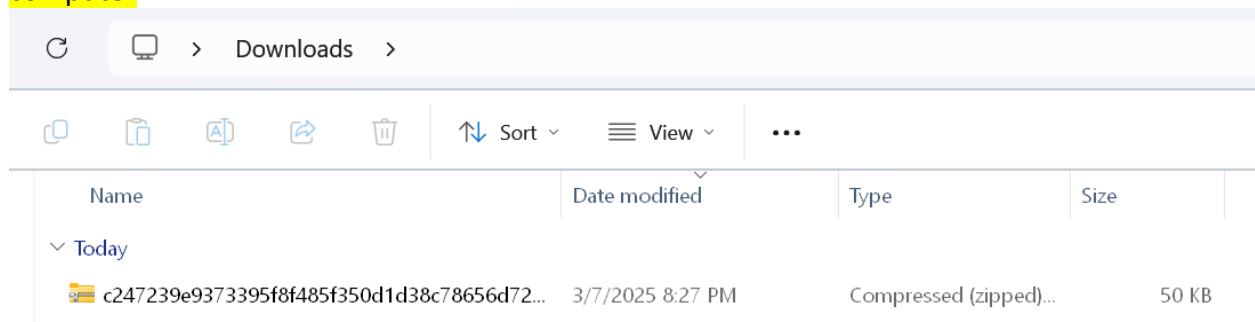
Tasks

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.

Firstseen (UTC)	SHA256 hash	Tags	Reporter
2025-03-07 16:26:57	 f6b834d4f916a99f78d94...	elf mirai	abuse_ch
2025-03-07 15:37:11	 0e864dfbd2379ceee456...	elf mirai	abuse_ch
2025-03-07 15:37:10	 06e08a407e1fc329e3d0f...	elf mirai	abuse_ch
2025-03-07 15:28:40	 533e7a32f1b2080de976...	elf mirai	abuse_ch
2025-03-07 15:18:33	 5ebfaa628075bc3731fb8...	elf mirai	abuse_ch
2025-03-07 15:04:41	 c247239e9373395f8f485...	elf mirai	abuse_ch
2025-03-07 14:59:08	 80852be512eca4d9373b...	elf mirai	abuse_ch
2025-03-07 14:58:57	 37bd6c01c06ced32826e...	elf mirai	abuse_ch
2025-03-07 14:48:57	 231aa568e46b3216ef778...	elf mirai	abuse_ch
2025-03-07 14:42:31	 b15eca8497ee7c754ae9...	elf mirai	abuse_ch
2025-03-07 14:37:08	 f327ab37d2c795344b9ec...	elf mirai	abuse_ch
2025-03-07 14:37:02	 5b6a3ddaea69d6a2b4bd...	elf mirai	abuse_ch
2025-03-07 14:36:56	 67b1132422327823f...	elf mirai	abuse_ch

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

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

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 Ⓢ	Miral 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:

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			
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			
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			

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

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.

The screenshot displays the Wireshark network protocol analyzer interface. The top section shows the 'HTTP Requests' tab with 5 items, 'Connections' with 27, 'DNS Requests' with 15, and 'Threats' with 0. Below this, a table of HTTP requests is visible, including details like Timeshift, Headers, Rep, PID, Process name, CN, URL, and Content. The middle section shows the 'Connections' tab with 27 items, displaying a table with columns for Timeshift, Protocol, Rep, PID, Process name, CN, IP, Port, Domain, ASN, and Traffic. The bottom section shows the 'DNS Requests' tab with 15 items, displaying a table with columns for Timeshift, Status, Rep, Domain, and IP. The interface includes various filters and search bars for each category.

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
6107 ms	GET 200: OK	✓	6544	svchost.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awm1Rh6Doh%2FsB...	471 b ↓ binary
8083 ms	GET 200: OK	✓	7452	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awm1Rh6Doh%2FsB...	471 b ↓ binary
10200 ms	GET 200: OK	✓	6728	BackgroundTransferH...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awm1Rh6Doh%2FsB...	312 b ↓ binary
29613 ms	GET 200: OK	✓	8112	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Auth...	419 b ↓ binary
29616 ms	GET 200: OK	✓	8112	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%20...	408 b ↓ binary

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	TCP	✓	2104	svchost.exe	🇩🇪	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data
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
BEFORE	UDP	✓	4	System	🇩🇪	192.168.100.255	138	—	—	↑ 945 b ↓ —
11 ms	TCP	✓	—	—	🇩🇪	51.104.136.2	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 860 b ↓ 4 Kb
16 ms	TCP	✓	—	—	🇩🇪	20.73.194.208	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 18 Kb
951 ms	TCP	✓	904	RUXIMICS.exe	🇩🇪	20.73.194.208	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 888 b ↓ 4 Kb

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2
BEFORE	Responded	✓	google.com	142.250.185.174
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2
BEFORE	Responded	✓	settings-win.data.microsoft.com	20.73.194.208
6062 ms	Responded	✓	client.wns.windows.com	40.113.110.67
				20.190.159.128
				40.106.251.133

HTTP Requests 5 Connections 27 DNS Requests 15 Threats 0


Timeshift Class PID Process name Message


No data

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.

General Info

File name: c247239e9373395f8f485f350d1d38c78656d72c6dcf6bf61551fb32100aad0e.zip
Full analysis: <https://app.any.run/tasks/0aea5191-86b4-4a72-9406-8a42268978cd>
Verdict: **No threats detected**
Analysis date: March 07, 2025 at 20:31:00
OS: Windows 10 Professional (build: 19045, 64 bit)
Indicators: 
MIME: application/zip
File info: Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
MD5: 7C1BB4EDEA07DE23D8D882D4F7A9C666
SHA1: 3B3C7CDB5B52FE3965044385F6F2A2810AF2B593
SHA256: D07DAF71C9CCACBD5A0F1A5AAE21920299B56A85B3070C1792C2D1EA0F75B4CB
SSDEEP: 1536:/8wpsX1jYvMp9l4PKMnVb3APiNVUHslgScfElrcC0:/52XuWL4P5nVjAPiDA0gScfzcb

 [ANY.RUN](#) is an interactive service which provides full access to the guest system. Information in this report could be distorted. [ANY.RUN](#) does not guarantee maliciousness or safety of the content.

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.

Based on the information found in both steps, the malware sample is neither malicious nor suspicious. According to the website we used, the contents within the sample do as follows: Creates files or folders in the user directory, Reads security settings of internet explorer, Reads the software policy settings, and checks proxy server information. 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.

After repeating the steps from task 3 through task 7, the main characteristics of this sample are that it is detected as “suspicious” as well as has one hit for malicious behavior, but given the information on this it seems to be nothing of importance. 5 points

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

Based on both reports made by me, I think that the main difference between Mirai and VIPKeylogger is that, VIPKeylogger has more malicious behaviors than mirai. This is based on

the simple fact given above. VIPKeylogger set off the “Suspicious activity while Mirai did not. I believe this to be the main difference.

5 points

Turn-in

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