

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

Search:

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

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
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

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. **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**

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**

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

Turn-in

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