

Lab #4: Malware Analysis

Destiny Hale

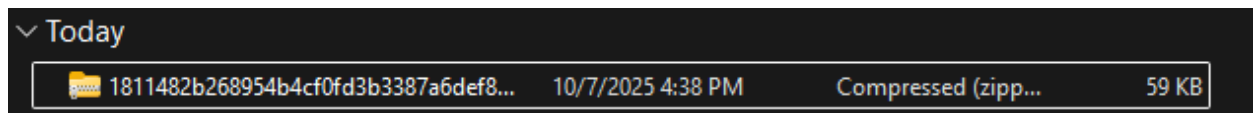
10/7/25

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

Time	Hash	Architecture	Signature	Category	Download
2025-10-05 18:34	602f9e7ffe06a0b8efcb7e...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	d9cd746b7c7af6eba4f20...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	25a77fbc943fb2ec68880...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	1ea28ecc52461457df7e...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	5e710d686ec42b7f52302...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	027fb1542493938b2a73...	elf	Mirai	abuse_ch	Download
2025-10-05 18:34	26bb73775b4c5247ad63...	elf	Mirai	abuse_ch	Download
2025-10-05 18:33	fea5d82e1e91f9a422091f...	elf	Mirai	abuse_ch	Download
2025-10-05 18:19	f6da80145b981d2689d6...	elf	Mirai	abuse_ch	Download
2025-10-05 18:07	1811482b268954b4cf0fd...	elf	Mirai	abuse_ch	Download
2025-10-05 18:07	5803b854959a53e11c86...	elf	Mirai	abuse_ch	Download
2025-10-05 18:06	2f3fbc56d018982fc668c6...	elf	Mirai	abuse_ch	Download
2025-10-05 17:48	617fc91098b7f2ed40fc...	elf	Mirai	abuse_ch	Download

Showing 1 to 250 of 262 entries (filtered from 1,000 total entries)

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



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:

HTTP Requests									
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content		
10699 ms	GET 200: OK	✓	6844	svchost.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNM...	471 b	↓	binary
10702 ms	GET 200: OK	✓	6844	svchost.exe	🇩🇪	http://ocsp.digicert.com/MFEwTzBNM...	471 b	↓	binary
10721 ms	GET 200: OK	✓	5796	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNM...	313 b	↓	binary
11809 ms	GET 200: OK	✓	6836	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNM...	471 b	↓	binary
19925 ms	GET 200: OK	✓	3264	backgroundTaskHost...	🇩🇪	http://ocsp.digicert.com/MFEwTzBNM...	471 b	↓	binary

Connections:

Connections											
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
BEFORE	TCP	✓	6480	RUXIMICS.exe	🇩🇪	51.124.78.146	443	settings-win...	MICROSOFT-CO...	No Data	
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	--	--	↑ 1 Kb ↓	
BEFORE	TCP	✓	6016	MoUsocoreWorker.exe	🇩🇪	51.124.78.146	443	settings-win...	MICROSOFT-CO...	No Data	
BEFORE	TCP	✓	5224	SearchApp.exe	🇩🇪	2.17.100.248	443	th.bing.com	Akamai Internati...	↑ 6 Kb ↓	
1443 ms	UDP	✓	4	System	?	192.168.100.255	138	--	--	↑ 3 Kb ↓	
10675 ms	TCP	✓	6844	svchost.exe	🇮🇪	20.190.159.0	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb ↓	
10686 ms	TCP	✓	6844	svchost.exe	🇮🇪	20.190.159.0	443	login.live.com	MICROSOFT-CO...	↑ 11 Kb ↓	

DNS Requests:

DNS Requests					
Timeshift	Status	Rep	Domain	IP	
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.124.78.146	
				2.17.100.248	
				2.17.100.249	
				2.17.100.241	
				2.17.100.209	
BEFORE	Responded	✓	www.bing.com	2.17.100.233	
				2.17.100.251	
				2.17.100.208	
				2.17.100.100	

Threats:

Threats					
Timeshift	Class	PID	Process name	Message	
19297 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

Behavior activities

☑ Add for printing

MALICIOUS

No malicious indicators.

SUSPICIOUS

No suspicious indicators.

INFO

Checks proxy server information
• slui.exe (PID: 2840)

Reads the software policy settings
• slui.exe (PID: 2840)

📄 Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#)

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 checks proxy server information and reads software policy settings. From these two actions, it was able to bypass network security measures, modify software settings, and bypass security measures within the system. No further activity was found.

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

SHA256 hash:	7d957cceab90148d9e96c61da9c1b62a8d31a64ef79cb3eafdb5a6b4fd586b8a
SHA3-384 hash:	aff659d420069f428ad07f8b76af61a93a058a97e64ace0f1216e7f0e07df642ba35443446e7e246a4d9667b24be7000
SHA1 hash:	d796edd80fdb3d3b8a5a17a065f2facc7217e22f
MD5 hash:	5ed3bdd498aa0834de8f3b6fa950a2c4
humanhash:	wisconsin-coffee-iowa-california
File name:	P83790-002.exe
Download:	download sample
Signature ⓘ	VIPKeylogger Alert

Behavior activities

☑ Add for printing

MALICIOUS

Generic archive extractor
• WinRAR.exe (PID: 7792)

SUSPICIOUS

No suspicious indicators.

INFO

No info indicators.

📄 Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the [full report](#)

- This keylogging malware is a generic archive extractor. However, no other activity was found.

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

- Although Mirai and VIPKeylogging are both forms of malware, they have different tactics. Keylogging is a spyware that involves monitoring every keystroke made on a user's device. This creates an advantage for attackers to steal credentials and other

sensitive information. On the other hand, Mirai involves infecting devices and turning them into a botnet to carry out malicious attacks such as DDoS. This disrupts system operations and makes applications unavailable to the user.