

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

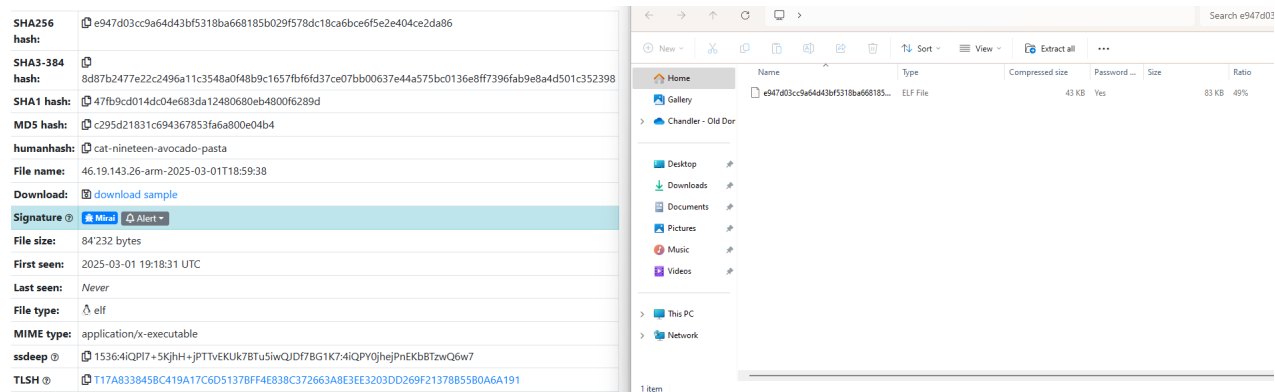
and make sure you highlight the malware you selected.

2 points

Firstseen (UTC)	SHA256 hash	Tags	Reporter
2025-03-01 21:32:01	 fba00bbd3da123f4eeb72...	elf 	 abuse_ch
2025-03-01 21:32:00	 b15c8d8509bdb156f474...	elf 	 abuse_ch
2025-03-01 20:52:01	 d8874bf7853421605f4c2...	elf 	 abuse_ch
2025-03-01 20:47:04	 7940f811f5d64ab61def1...	elf 	 abuse_ch
2025-03-01 20:47:03	 27f706d14a8d323096ad...	elf 	 abuse_ch
2025-03-01 20:47:01	 b34e0cc576f9b56c0f00d...	elf 	 abuse_ch
2025-03-01 20:47:00	 dfdfc5ab28e96ee1a19df...	elf 	 abuse_ch
2025-03-01 20:42:02	 9217c9dcc2b188282dba...	elf 	 abuse_ch
2025-03-01 20:42:01	 1644a29a694a993c9719...	elf 	 abuse_ch
2025-03-01 20:37:04	 03f8c65f8b9666eed036e...	elf 	 abuse_ch
2025-03-01 19:18:31	 e947d03cc9a64d43bf531...	elf 	 threatquery
2025-03-01 19:06:05	 ba0ac329d7541bb45088...	 	 abuse_ch
2025-03-01 17:42:11	 da80863061dc0e02682b...	 	 abuse_ch
2025-03-01 17:32:15	 1d4d2d5d88fe95f07140e...	elf 	 abuse_ch
2025-03-01 16:32:13	 1ad5621421e5f0d4c673d...	 	 abuse_ch

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

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

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

category.

8 points

HTTP Requests 19 Connections 56 DNS Requests 80 Threats 0										Filter by PID, name or url		PCAP
NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content				
	5405 ms	GET 200: OK	✓	6544	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2aw...	471 b	↓	binary		
	8471 ms	GET 200: OK	✓	5988	backgroundTaskHost...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBSQ500x%2Fh0Ztl...	471 b	↓	binary		
	10492 ms	GET 200: OK	✓	4932	BackgroundTransferH...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGGUABBTjrydRyt%2BAP...	313 b	↓	binary		
FILES	28991 ms	GET 200: OK	✓	3884	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Ce...	419 b	↓	binary		
	28992 ms	GET 200: OK	✓	3884	SIHClient.exe		http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20S...	408 b	↓	binary		
DEBUG	41227 ms	GET 200: OK	✓	5260	firefox.exe		http://detectportal.firefox.com/canonical.html	90 b	↓	text		
	41318 ms	GET 200: OK	✓	5260	firefox.exe		http://detectportal.firefox.com/success.txt?ipv4	8 b	↓	text		
	41908 ms	POST 200: OK	✓	5260	firefox.exe		http://o.pki.goog/we2	84 b	↑	binary		
								280 b	↓	binary		











HTTP Requests 19 Connections 56 DNS Requests 80 Threats 0										Filter by PID, domain, name or ip		PCAP
NETWORK	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
	BEFORE	UDP	✓	4	System	🇩🇪	192.168.100.255	137	–	–	↑ 436 b ↓ –	
	BEFORE	TCP	✓	2104	svchost.exe	🇩🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data	
FILES	BEFORE	TCP	✓	–	–	🇩🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 888 b ↓ 4 Kb	
	BEFORE	TCP	✓	–	–	🇩🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 4 Kb	
DEBUG	BEFORE	UDP	✓	4	System	🇩🇪	192.168.100.255	138	–	–	↑ 945 b ↓ –	
	BEFORE	TCP	✓	–	–	🇩🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 860 b ↓ 4 Kb	
	BEFORE	TCP	✓	5496	MoUsCoreWorker.exe	🇩🇪	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 18 Kb	
	5366 ms	TCP	✓	2112	svchost.exe	🇩🇪	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 5 Kb	
	5399 ms	TCP	✓	3216	svchost.exe	🇩🇪	40.113.110.67	443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 2 Kb ↓ 4 Kb	

HTTP Requests 19 Connections 56 DNS Requests 80 Threats 0										Filter by IP or domain	PCAP
Timeshift	Status	Rep	Domain	IP							
BEFORE	Responded	✓	settings-win.data.microsoft.com	40.127.240.158							
BEFORE	Responded	✓	google.com	142.250.185.110							
4351 ms	Responded	✓	settings-win.data.microsoft.com	4.231.128.59							
5353 ms	Responded	✓	client.wns.windows.com	40.113.110.67							
				40.126.31.67							
				40.126.31.71							
				40.126.31.0							
				40.126.31.129							
5354 ms	Responded	✓	login.live.com	40.126.31.128							
				40.126.31.2							

HTTP Requests 19 Connections 56 DNS Requests 80 Threats 0										Filter by message	PCAP
Timeshift		Class		PID	Process name		Message				
No data											

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

IOCs	
Summary of indicators of compromises 17	
 	 Copy selected
 SHA256	2/8T/E31DeYr0eT584//19T/0b02U3bd4Deeaa2U4//2/C9eU16e29b4d35bae4ca C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-wal 83681da37b05930eea3567cc448f267931dc66756b2c98d66e909c06e539a6e5
 SHA256	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.sbstore ffe2d3077b81ae6f51b220c1c661b276c823fa67dad1d64fc5f17249fc54bdc0
 SHA256	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.tmp e6287e44b44abea20e1b2e3f415d22b9e5e5fbbc155ad9dadbaba63951b2af6f
 SHA256	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-wal 980d7bf28bda02a41309ec71197adf4c3a7ea924775d275f1a353cb41ca2b070
 SHA256	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite eaf3aa5de369c7c2a7b41c914a18a1a938f45202c0cb9b1e8b5e745ec8558554
 SHA256	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite 1c7f2ac8937d59018eaf96963b179b12f1c21c735085a05670e949f6a0c5ff6f
DNS requests (1)	
 DOMAIN	temuaffiliateprogram.pxfile

Behavior activities

☒ Add for printing

MALICIOUS

BOTNET has been found (auto)

- WinRAR.exe (PID: 4996)
- firefox.exe (PID: 5260)

SUSPICIOUS

No suspicious indicators.

INFO

Creates files or folders in the user directory

- BackgroundTransferHost.exe (PID: 4932)

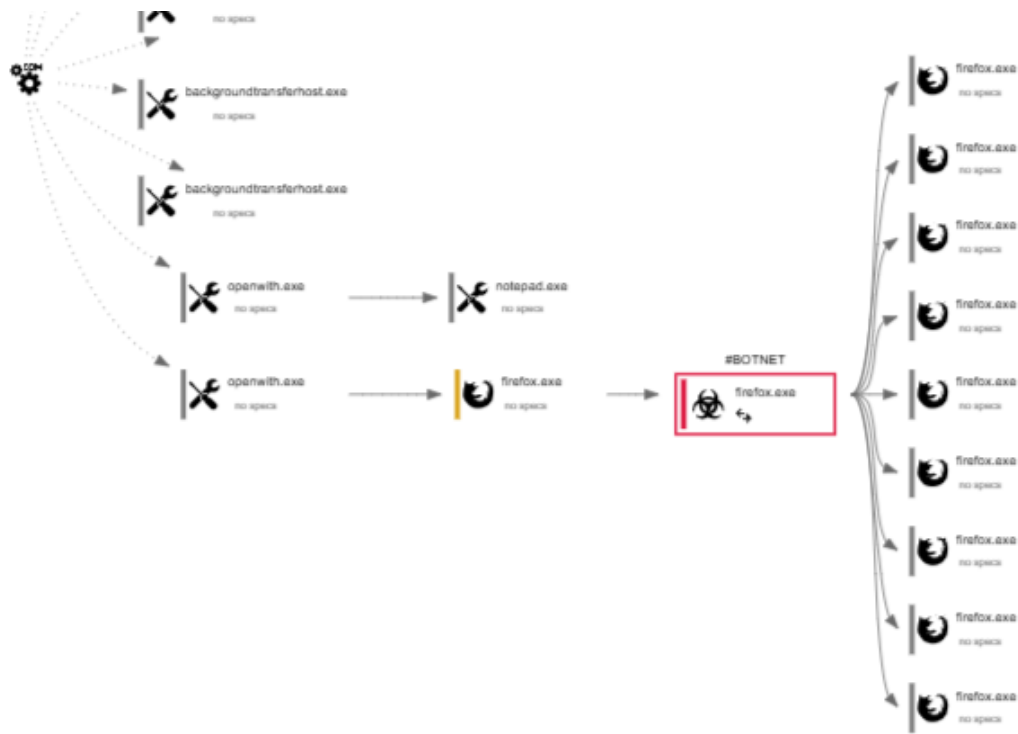
Reads security settings of Internet Explorer

- BackgroundTransferHost.exe (PID: 4932)

Application launched itself

- firefox.exe (PID: 5260)
- firefox.exe (PID: 5380)

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing



MITRE ATT&CK Matrix

Tactics 1 | Techniques 1 | Events 2

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection
						Query Registry 2		

Techniques details

Get to know what this threat is about

[T1012](#)

"Query Registry"

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry)

- Reads security settings of Internet Explorer (2)
4932 BackgroundTransferHost.exe (2)

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 malware is used to add the computer to a botnet. When I opened firefox, it automatically opened other firefox processes to add to it's botnet. It was detected when downloaded and when firefox was opened. The mirai part scanned my internet browser to see where it was weak.

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

The malware is using powershell without my authorization to try and steal information from me. WScript.exe and Powershell.exe try to make registry changes and HTTP requests. It also uses sleep to avoid detection.

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

5 points

Mirai is a malware that scans devices for vulnerabilities and then infects them to add them to a botnet. The main use of Mirai is used to perform DDoS attacks. VIP Keylogger is a malware that tries to steal passwords and sensitive data from your computer through "keylogging", which tracks input on your computer.

Turn-in

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