

Carmen Taylor

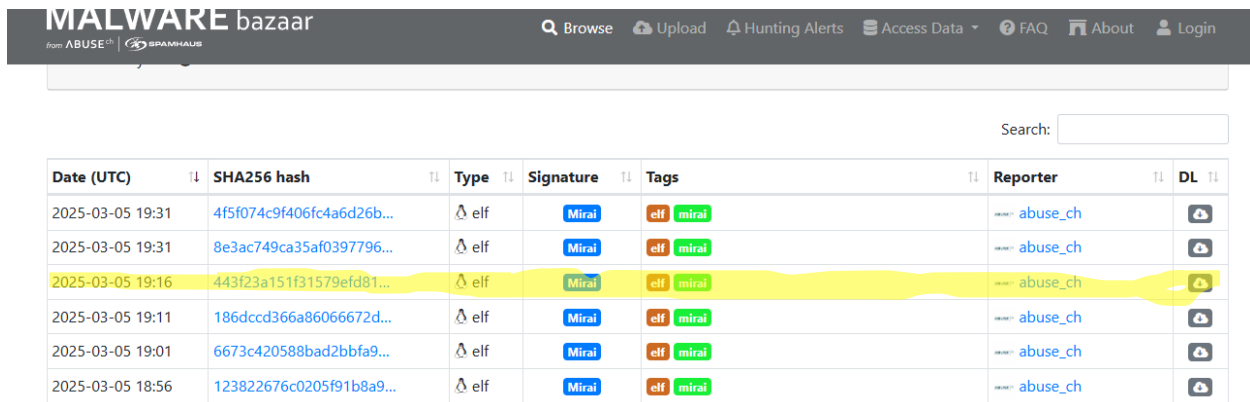
CYSE 450

Lab 3

3/5/25

Task-1: Go to <https://bazaar.abuse.ch/browse/> and select a malware with the “Mirai” signature.

I believe Mirai is a virus malware

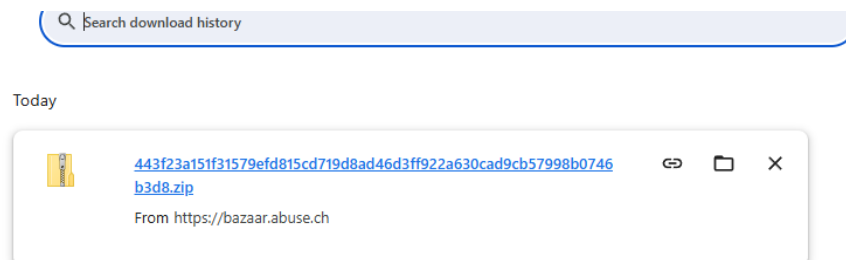


Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-03-05 19:31	4f5f074c9f406fc4a6d26b...	elf	Mirai	elf mirai	abuse_ch	
2025-03-05 19:31	8e3ac749ca35af0397796...	elf	Mirai	elf mirai	abuse_ch	
2025-03-05 19:16	443f23a151f31579efd81...	elf	Mirai	elf mirai	abuse_ch	
2025-03-05 19:11	186dccc366a86066672d...	elf	Mirai	elf mirai	abuse_ch	
2025-03-05 19:01	6673c420588bad2bbfa9...	elf	Mirai	elf mirai	abuse_ch	
2025-03-05 18:56	123822676c0205f91b8a9...	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.

Task-

Download history



Search download history

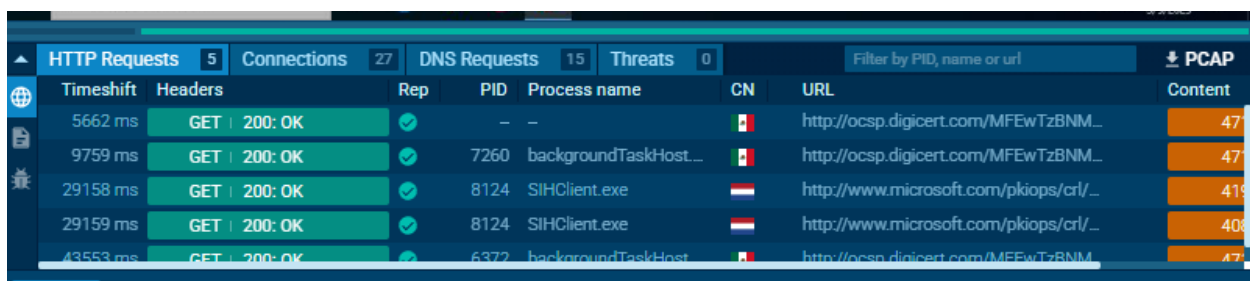
Today

[443f23a151f31579efd815cd719d8ad46d3ff922a630cad9cb57998b0746b3d8.zip](https://bazaar.abuse.ch)

From <https://bazaar.abuse.ch>

Task-6: Take screenshots of the any.run screen, include the HTTP Requests, Connections, DNS Requests, and Threats under the Network tab.

**HTTP Requests:**



Timeshift	Headers	Rep	PID	Process name	CN	URL	PCAP Content
5662 ms	GET   200: OK		-	-		<a href="http://ocsp.digicert.com/MFEwTzBNM...">http://ocsp.digicert.com/MFEwTzBNM...</a>	47
9759 ms	GET   200: OK		7260	backgroundTaskHost...		<a href="http://ocsp.digicert.com/MFEwTzBNM...">http://ocsp.digicert.com/MFEwTzBNM...</a>	47
29158 ms	GET   200: OK		8124	SIHClient.exe		<a href="http://www.microsoft.com/pkiops/crl/...">http://www.microsoft.com/pkiops/crl/...</a>	419
29159 ms	GET   200: OK		8124	SIHClient.exe		<a href="http://www.microsoft.com/pkiops/crl/...">http://www.microsoft.com/pkiops/crl/...</a>	408
43553 ms	GET   200: OK		6372	backgroundTaskHost...		<a href="http://ocsp.digicert.com/MFEwTzBNM...">http://ocsp.digicert.com/MFEwTzBNM...</a>	47

### Connections:

The screenshot shows a network monitoring interface with the 'Connections' tab selected. The interface includes a search bar at the top, a taskbar with application icons, and a status bar showing the time as 8:07 PM on 3/5/2025. The main area displays a table of connections with columns for Timeshift, Protocol, Rep, PID, Process name, CN, IP, Port, Domain, ASN, and Traffic. The table contains five rows of data, all with a 'BEFORE' timeshift and a green checkmark in the 'Rep' column. The processes listed are 'System' and 'settings-win...'. The domains include 'settings-win...' and 'MICROSOFT-CO...'. The traffic column shows an upward arrow for each entry.

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	-	-	↑
BEFORE	TCP	✓	-	-	?	51.124.78.146	443	settings-win...	MICROSOFT-CO...	↑
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	-	-	↑
BEFORE	TCP	✓	-	-	?	51.124.78.146	443	settings-win...	MICROSOFT-CO...	↑
BEFORE	TCP	✓	-	-	?	51.124.78.146	443	settings-win...	MICROSOFT-CO...	↑

### DNS Requests:

The screenshot shows the 'DNS Requests' tab selected in the network monitoring tool. The interface is similar to the previous screenshot, with a search bar, taskbar, and status bar. The main area displays a table of DNS requests with columns for Timeshift, Status, Rep, Domain, and IP. The table contains three rows of data, all with a 'BEFORE' timeshift and a green checkmark in the 'Rep' column. The domains are 'google.com', 'settings-win.data.microsoft.com', and 'client.wns.windows.com'. The IP addresses are 142.250.185.174, 51.124.78.146, and 40.113.103.199. The status column shows 'Responded' for all entries.

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	google.com	142.250.185.174
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.124.78.146
5617 ms	Responded	✓	client.wns.windows.com	40.113.103.199

### Threats:

The screenshot shows the 'Threats' tab selected in the network monitoring tool. The interface is similar to the previous screenshots, with a search bar, taskbar, and status bar. The main area displays a table of threats with columns for Timeshift, Class, PID, Process name, and Message. The table is empty, and the text 'No data' is displayed in the center of the table area.

Timeshift	Class	PID	Process name	Message
No data				

Task-7: Screenshot any interesting finds

## Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	whitelisted
–	–	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
–	–	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	40.126.31.131:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
–	–	23.40.158.218:80	ocsp.digicert.com	AKAMAI-AS	MX	whitelisted
6544	svchost.exe	40.126.31.131:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted

## Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

### Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)

### Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package

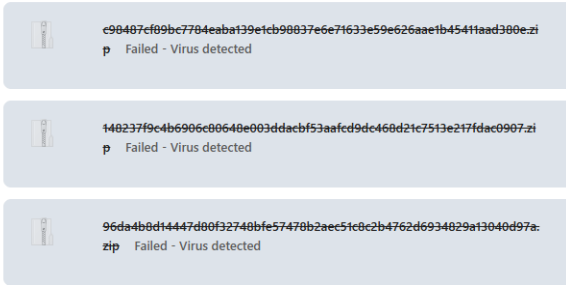
Task-8: Based on the information you found from Task-6 and Task-7, briefly explain the main characteristics of the malware sample.

Since the Mirai malware is a virus, it makes sense why many of the connections were Microsoft connections, when it came to the settings and other files. I believe this virus uses system resources, to steal data and corrupt files. It spreads through document macros like Microsoft Office, Adobe, and Java when looking at the connections and software features.

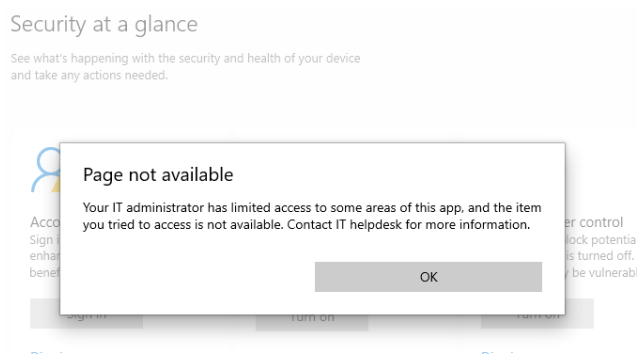
Task-9: In the bottom part of the any.run screen, you will find information about HTTP Requests, Connections, DNS Requests, and Threats under the Network tab. Screenshot the findings for each category with the VIPKeylogger Malware.

## My computer wouldn't let me download the malicious file

March 2, 2020



I also tried to stop my antivirus software but it wouldn't work either.



### **HTTP Requests:**

### **Connections:**

### **DNS Requests:**

### **Threats:**

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

Since I was unable to view the Keylogger malware, I will compare Mirai to a keylogger(Spyware) malware. It seems a keylogger would record keystrokes to get sensitive information. While Marai virus uses files and the system resources to steal data, and corrupt files. I also believe that the Marai malware is safer than the VIPKeylogger malware simply due to the fact my computer wouldn't even let me download the malware sample.