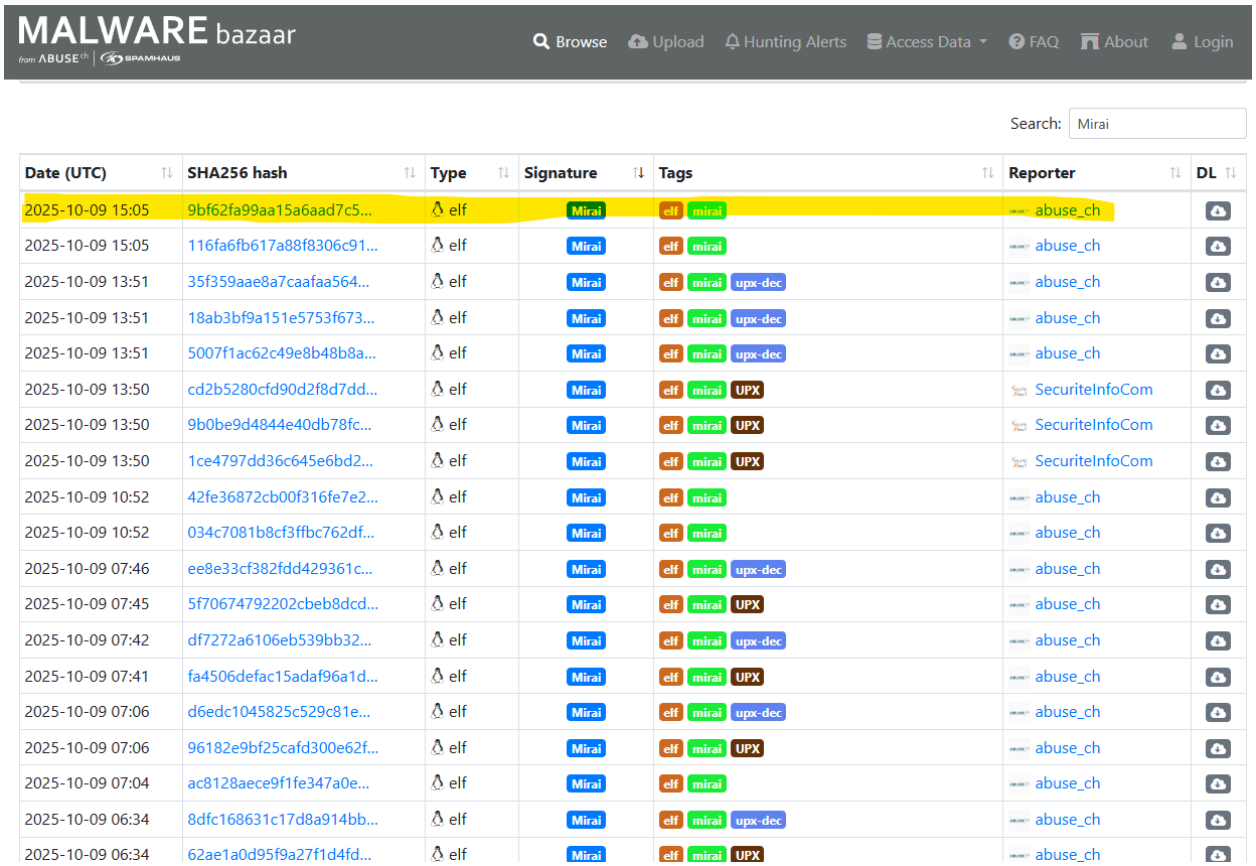
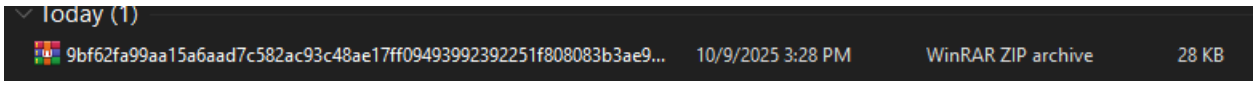
Mirai Malware

T1. Highlighted the top malware when searching Mirai signature, I will be using the highlighted one for this lab.

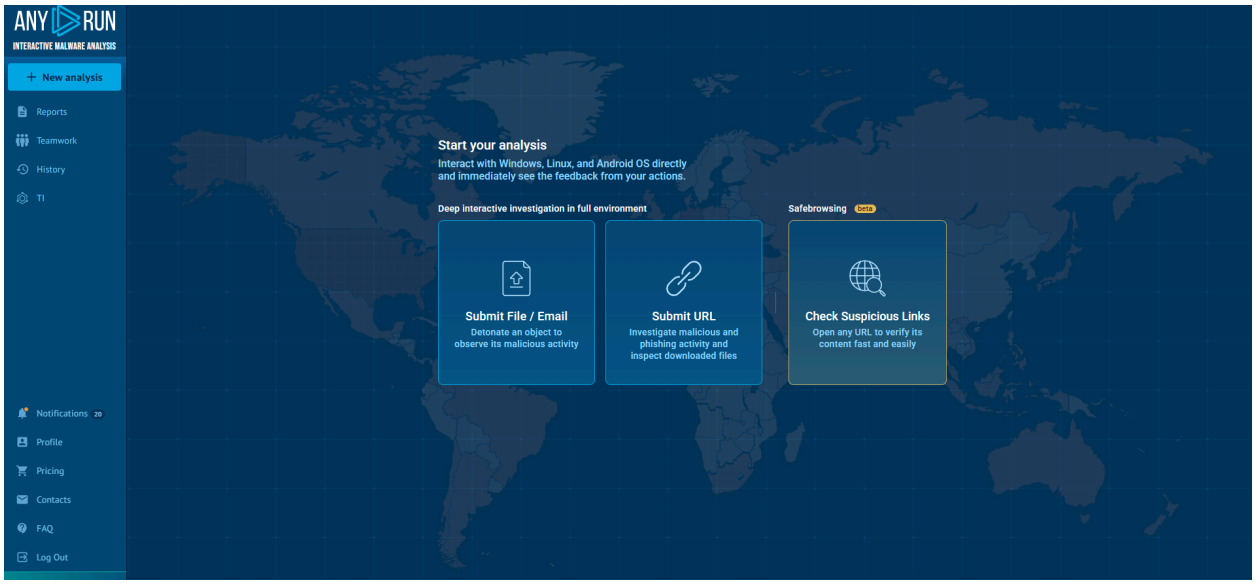


Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-10-09 15:05	9bf62fa99aa15a6aad7c5...	elf	Mirai	elf mirai	abuse_ch	
2025-10-09 15:05	116fa6fb617a88f8306c91...	elf	Mirai	elf mirai	abuse_ch	
2025-10-09 13:51	35f359aae8a7caafaa564...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 13:51	18ab3bf9a151e5753f673...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 13:51	5007f1ac62c49e8b48b8a...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 13:50	cd2b5280cfd90d2f8d7dd...	elf	Mirai	elf mirai UPX	SecuriteInfoCom	
2025-10-09 13:50	9b0be9d4844e40db78fc...	elf	Mirai	elf mirai UPX	SecuriteInfoCom	
2025-10-09 13:50	1ce4797dd36c645e6bd2...	elf	Mirai	elf mirai UPX	SecuriteInfoCom	
2025-10-09 10:52	42fe36872cb00f316fe7e2...	elf	Mirai	elf mirai	abuse_ch	
2025-10-09 10:52	034c7081b8cf3ffbc762df...	elf	Mirai	elf mirai	abuse_ch	
2025-10-09 07:46	ee8e33cf382fdd429361c...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 07:45	5f70674792202cbeb8dcd...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-10-09 07:42	df7272a6106eb539bb32...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 07:41	fa4506defac15adaf96a1d...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-10-09 07:06	d6edc1045825c529c81e...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 07:06	96182e9bf25cafd300e62f...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-10-09 07:04	ac8128aece9f1fe347a0e...	elf	Mirai	elf mirai	abuse_ch	
2025-10-09 06:34	8dfc168631c17d8a914bb...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-10-09 06:34	62ae1a0d95f9a27f1d4fd...	elf	Mirai	elf mirai UPX	abuse_ch	

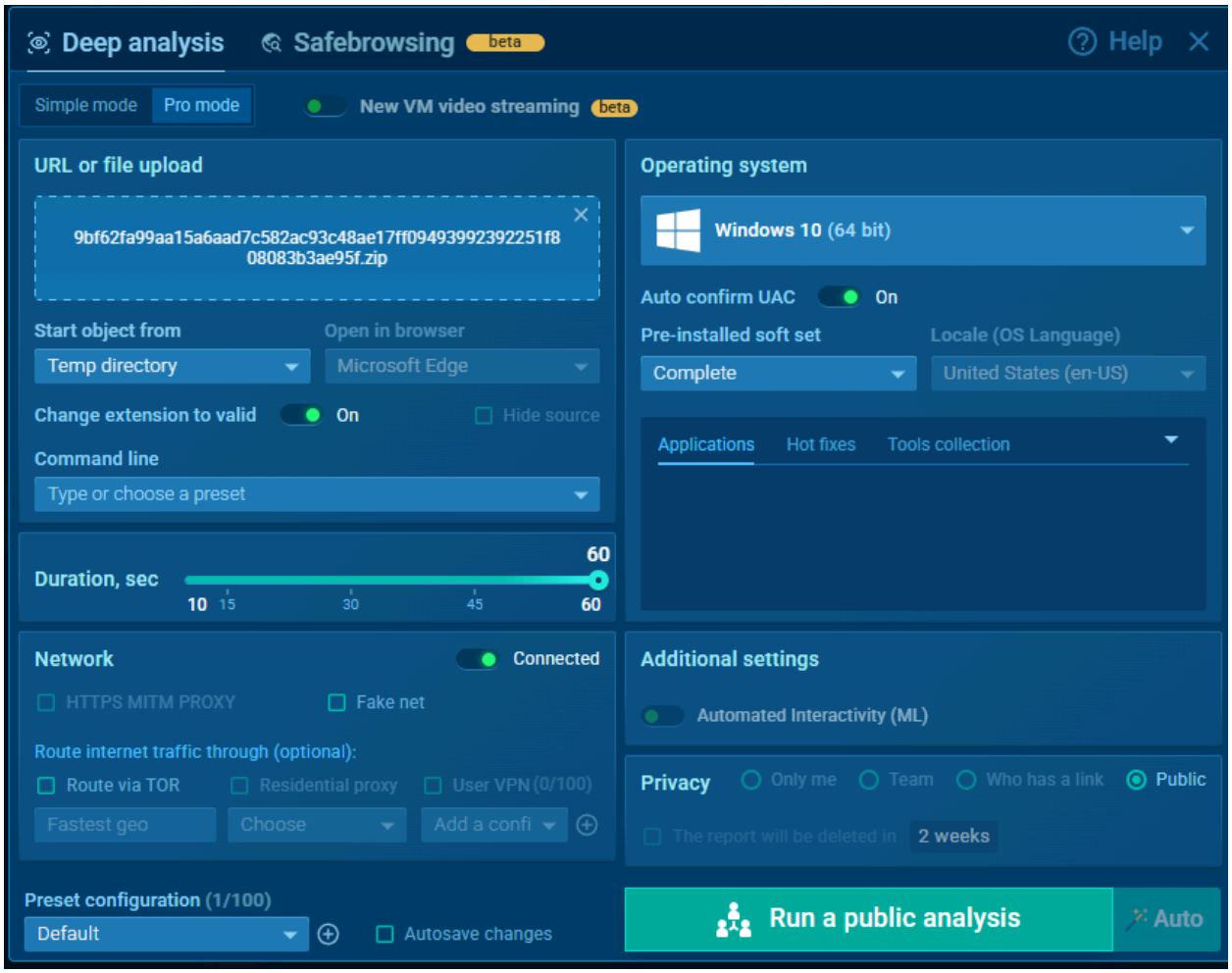
T2. Shows downloaded malware sample in my downloads directory.



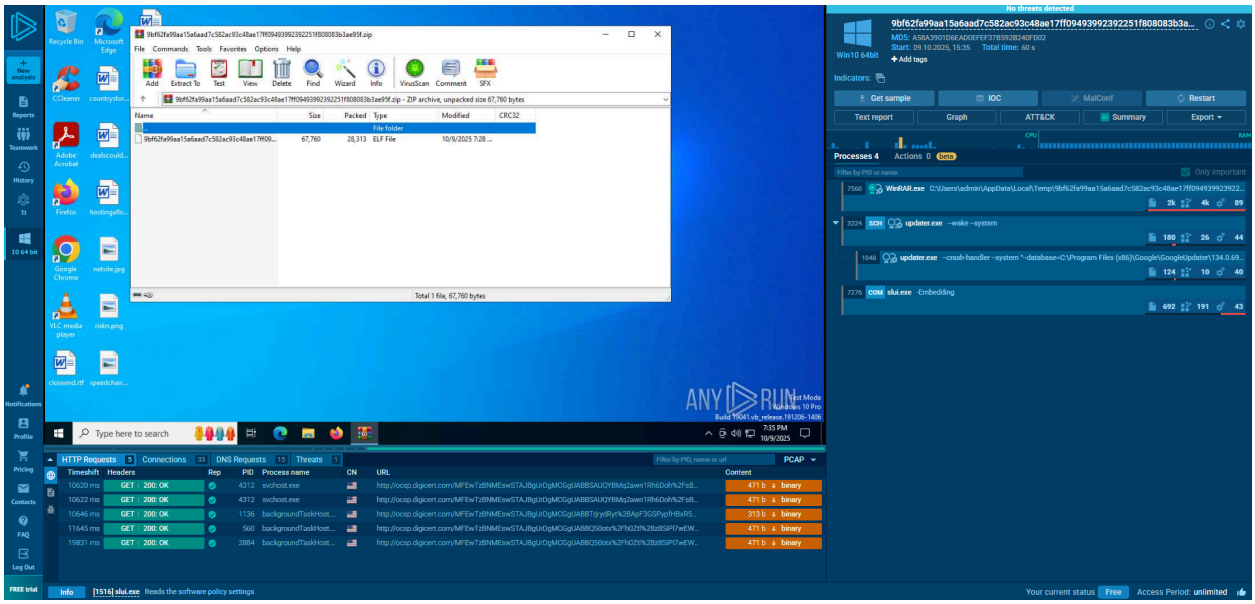
T3.


ANY RUN
INTERACTIVE MALWARE ANALYSIS
New analysis
Reports
Teamwork
History
TI
Notifications 20
Profile
Pricing
Contacts
FAQ
Log Out
Start your analysis
Interact with Windows, Linux, and Android OS directly and immediately see the feedback from your actions.
Deep interactive investigation in full environment
Safebrowsing beta
Submit File / Email
Detonate an object to observe its malicious activity
Submit URL
Investigate malicious and phishing activity and inspect downloaded files
Check Suspicious Links
Open any URL to verify its content fast and easily

T4.


Deep analysis
Safebrowsing
beta
Help
Simple mode
Pro mode
New VM video streaming
beta
URL or file upload
9bf62fa99aa15a6aad7c582ac93c48ae17ff0949399239225 1f808083b3ae95f.zip
Start object from
Temp directory
Open in browser
Microsoft Edge
Change extension to valid
On
Hide source
Command line
Type or choose a preset
Duration, sec
60
10
15
30
45
60
Network
Connected
HTTPS MITM PROXY
Fake net
Route internet traffic through (optional):
Route via TOR
Residential proxy
User VPN (0/100)
Fastest geo
Choose
Add a confi
Preset configuration (1/100)
Default
Autosave changes
Operating system
Windows 10 (64 bit)
Auto confirm UAC
On
Pre-installed soft set
Complete
Locale (OS Language)
United States (en-US)
Applications
Hot fixes
Tools collection
Additional settings
Automated Interactivity (ML)
Privacy
Only me
Team
Who has a link
Public
The report will be deleted in
2 weeks
Run a public analysis
Auto

T5.

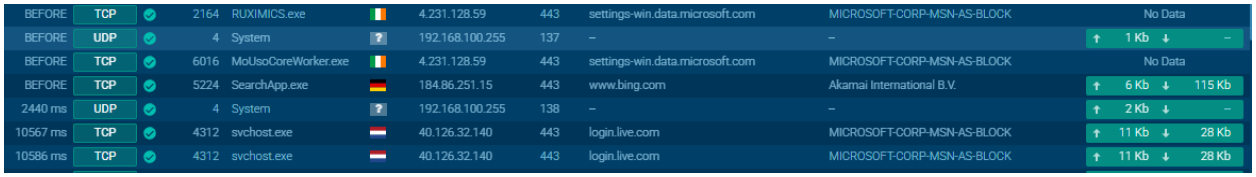


T6.

a.

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
10620 ms	GET | 200: OK	✓	4312	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsB...	471 b | binary
10622 ms	GET | 200: OK	✓	4312	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsB...	471 b | binary
10646 ms	GET | 200: OK	✓	1136	backgroundTaskHost....		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5...	313 b | binary
11645 ms	GET | 200: OK	✓	560	backgroundTaskHost....		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEW...	471 b | binary
19831 ms	GET | 200: OK	✓	2884	backgroundTaskHost....		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEW...	471 b | binary

b.

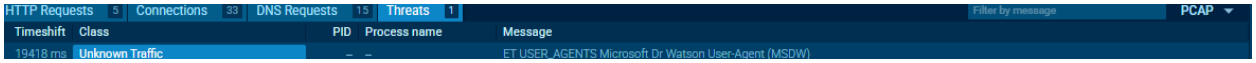


BEFORE	TCP	✓	2164	RUXIMICS.exe	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data
BEFORE	UDP	✓	4	System	192.168.100.255	137	--	--	↑ 1 Kb ↓ --
BEFORE	TCP	✓	6016	MoUsoCoreWorker.exe	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data
BEFORE	TCP	✓	5224	SearchApp.exe	184.86.251.15	443	www.bing.com	Akamai International B.V.	↑ 6 Kb ↓ 115 Kb
2440 ms	UDP	✓	4	System	192.168.100.255	138	--	--	↑ 2 Kb ↓ --
10567 ms	TCP	✓	4312	svchost.exe	40.126.32.140	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 11 Kb ↓ 28 Kb
10586 ms	TCP	✓	4312	svchost.exe	40.126.32.140	443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 11 Kb ↓ 28 Kb

c.

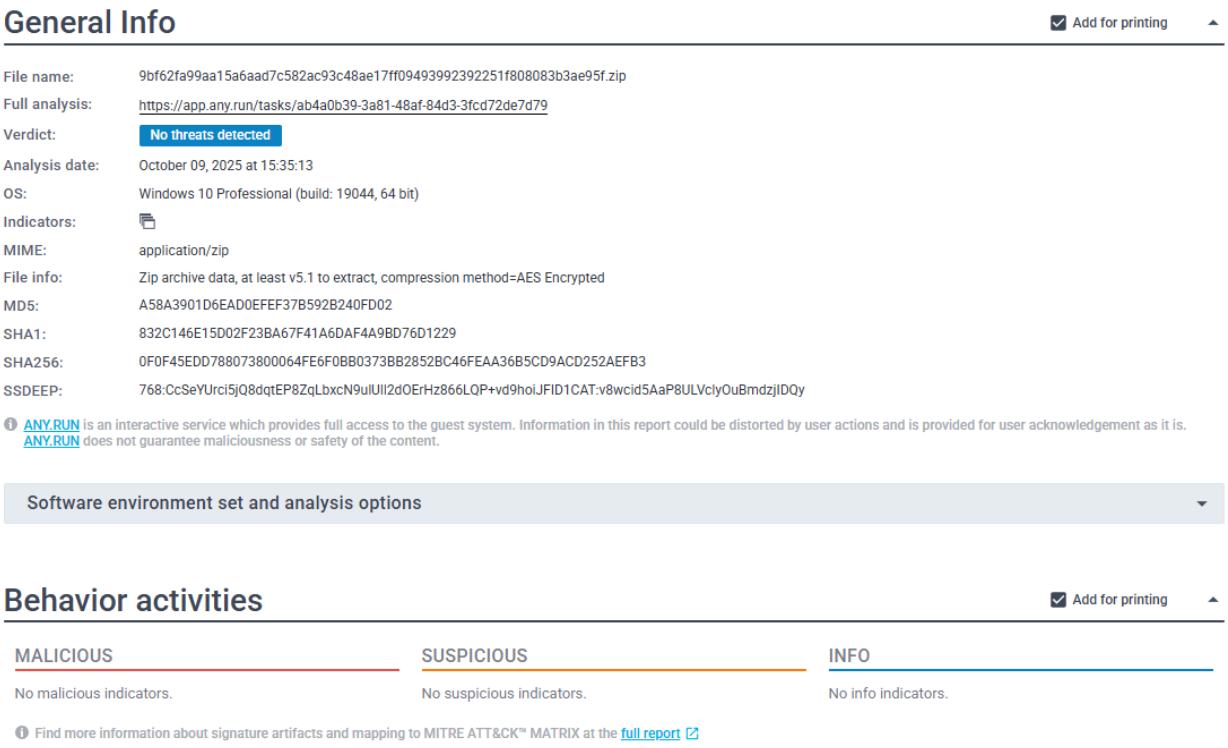
Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	4.231.128.59
BEFORE	Responded	✓	www.bing.com	184.86.251.15 184.86.251.11 184.86.251.13 184.86.251.10 184.86.251.20 184.86.251.16 184.86.251.14

d.



Timeshift	Class	PID	Process name	Message
19418 ms	Unknown Traffic	--	--	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

T7.



General Info

Add for printing

File name:	9bf62fa99aa15a6aad7c582ac93c48ae17ff09493992392251f808083b3ae95f.zip
Full analysis:	https://app.any.run/tasks/ab4a0b39-3a81-48af-84d3-3fcd72de7d79
Verdict:	No threats detected
Analysis date:	October 09, 2025 at 15:35:13
OS:	Windows 10 Professional (build: 19044, 64 bit)
Indicators:	
MIME:	application/zip
File info:	Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
MD5:	A58A3901D6EAD0EFEF37B592B240FD02
SHA1:	832C146E15D02F23BA67F41A6DAF4A9BD76D1229
SHA256:	0F0F45EDD788073800064FE6F0BB0373BB2852BC46FEAA36B5CD9ACD252AEFB3
SSDEEP:	768:CcSeYUrci5jQ8dqtEP8ZqLbxcN9ulUll2dOErHz866LQP+vd9hoiJFID1CAT:v8wcid5AaP8ULVclyOuBmdzjIDQy

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

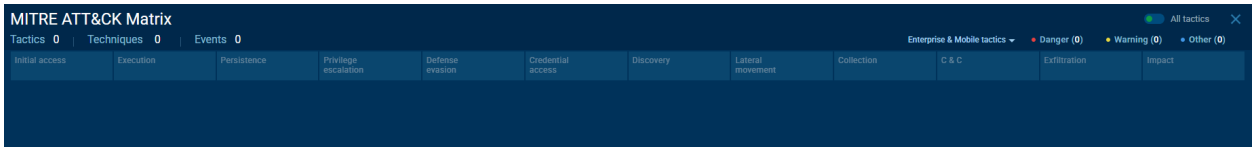
MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	No suspicious indicators.	No info indicators.

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

a.

b. 

c. 

d. 

T8. This malware seems to embed a slui.exe to evade detection, as well as use an updater.exe as well. Seemingly installing two potential backdoor programs that can be executed for malware. Seemingly the malware executed multiple connections to multiple countries for “updates from microsoft” with multiple connections in the settings-win.data.microsoft.com domain. The two executable files it used may be used to turn a pc into a bot in a botnet, forcing it to execute the programs.

T9.

a.

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-10-09 14:06	de8ed03b3ff86ae257807...	exe	VIPKeylogger	exe signed VIPKeylogger	adrian_luca	
2025-10-09 14:06	3e194727054b458a0c20...	exe	VIPKeylogger	exe signed VIPKeylogger	adrian_luca	
2025-10-09 14:02	cdbdc4261d286272c9a9...	exe	VIPKeylogger	exe signed VIPKeylogger	adrian_luca	
2025-10-09 13:59	190f1908e06f6168cbe53f...	exe	VIPKeylogger	exe signed VIPKeylogger	adrian_luca	
2025-10-09 10:00	1cbeccebb486971414ae...	r00	VIPKeylogger	r00 VIPKeylogger	FXOLabs	
2025-10-09 10:00	6516ed4563a9ed47e33c...	bat	VIPKeylogger	bat VIPKeylogger	FXOLabs	

b. This malware simply embedded a slui.exe to the computer on execution. This malware went through the same connections, dns requests, etc. However this slui.exe may potentially act as a subtle keylogger, with the slui.exe meant to evade detection.

T10. The two malwares committed similar processes in their execution. The Mirai installed an updater.exe and an embedded slui.exe in order to provide a backdoor for attempts at botnet operations. While the VIPKeylogger malware seemingly embedded a very subtle slui.exe to act as a keylogger, potentially drawing even less attention than the Mirai.