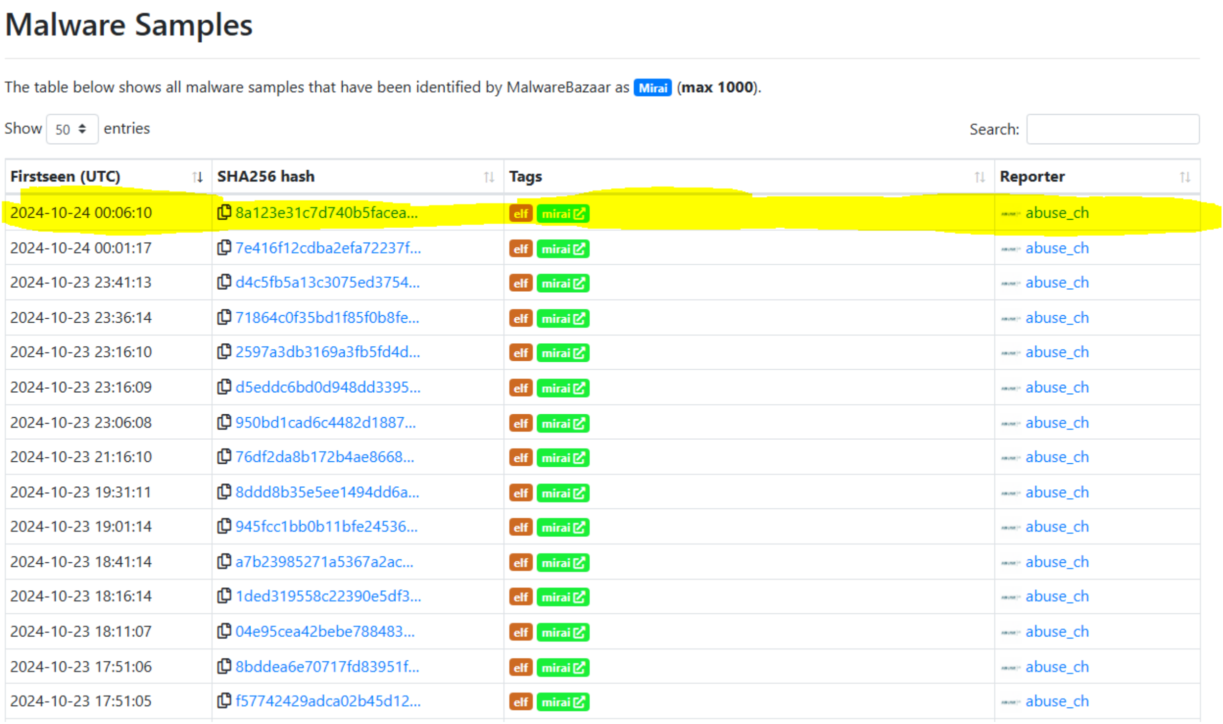
Lab 2: Malware Analysis

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.



Malware Samples

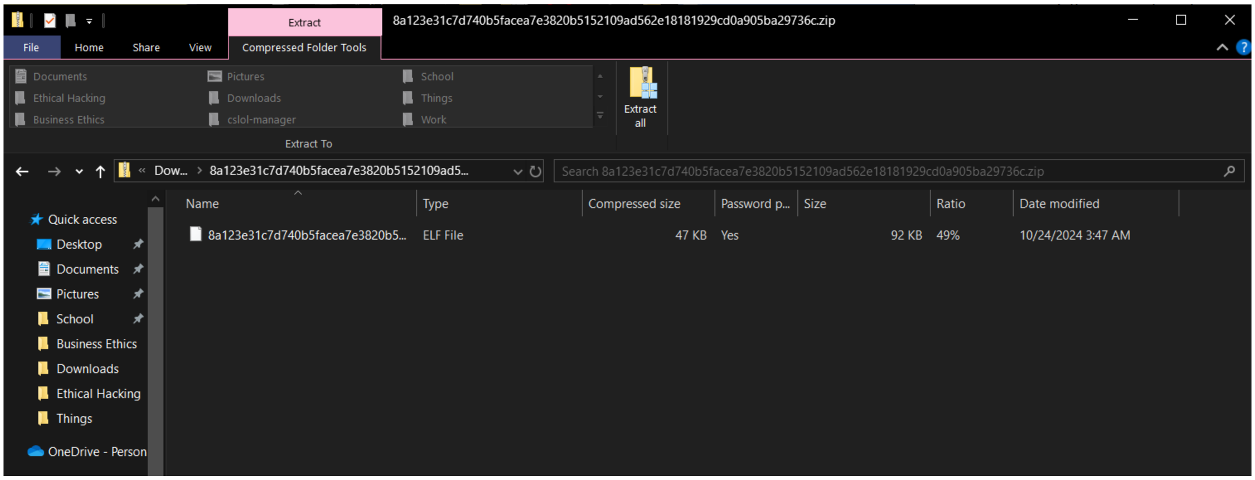
The table below shows all malware samples that have been identified by MalwareBazaar as Mirai (**max 1000**).

Show 50 entries

Search:

Firstseen (UTC)	SHA256 hash	Tags	Reporter
2024-10-24 00:06:10	8a123e31c7d740b5facea...	elf mirai	abuse_ch
2024-10-24 00:01:17	7e416f12cdba2efa72237f...	elf mirai	abuse_ch
2024-10-23 23:41:13	d4c5fb5a13c3075ed3754...	elf mirai	abuse_ch
2024-10-23 23:36:14	71864c0f35bd1f85f0b8fe...	elf mirai	abuse_ch
2024-10-23 23:16:10	2597a3db3169a3fb5fd4d...	elf mirai	abuse_ch
2024-10-23 23:16:09	d5eddc6bd0d948dd3395...	elf mirai	abuse_ch
2024-10-23 23:06:08	950bd1cad6c4482d1887...	elf mirai	abuse_ch
2024-10-23 21:16:10	76df2da8b172b4ae8668...	elf mirai	abuse_ch
2024-10-23 19:31:11	8ddd8b35e5ee1494dd6a...	elf mirai	abuse_ch
2024-10-23 19:01:14	945fcc1bb0b11bfe24536...	elf mirai	abuse_ch
2024-10-23 18:41:14	a7b23985271a5367a2ac...	elf mirai	abuse_ch
2024-10-23 18:16:14	1ded319558c22390e5df3...	elf mirai	abuse_ch
2024-10-23 18:11:07	04e95cea42bebe788483...	elf mirai	abuse_ch
2024-10-23 17:51:06	8bddea6e70717fd83951f...	elf mirai	abuse_ch
2024-10-23 17:51:05	f57742429adca02b45d12...	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.



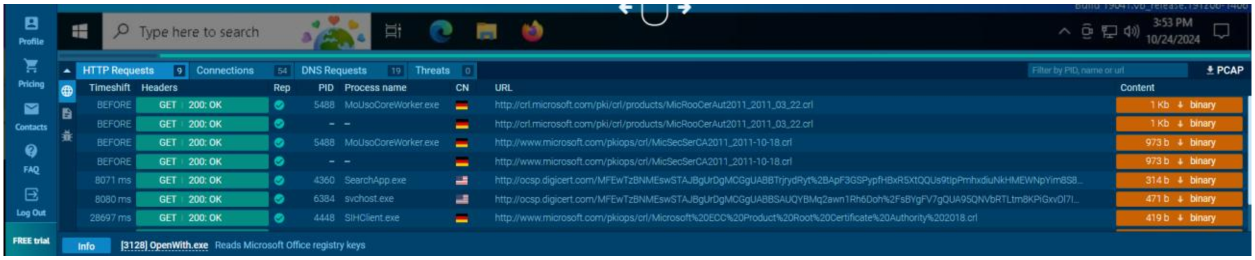
8a123e31c7d740b5facea7e3820b5152109ad562e18181929cd0a905ba29736c.zip

Dow... › 8a123e31c7d740b5facea7e3820b5152109ad5...

Search 8a123e31c7d740b5facea7e3820b5152109ad562e18181929cd0a905ba29736c.zip

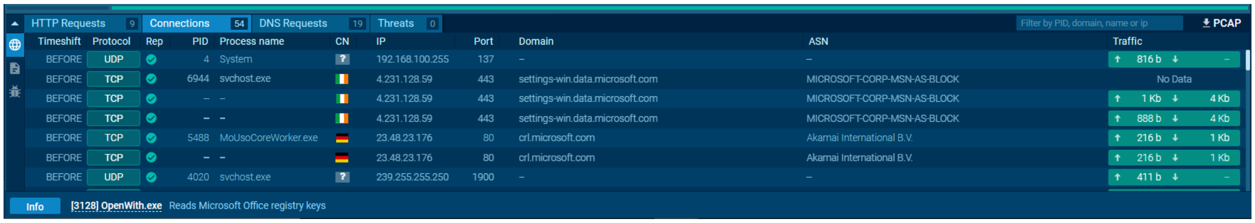
Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
8a123e31c7d740b5facea7e3820b5...	ELF File	47 KB	Yes	92 KB	49%	10/24/2024 3:47 AM

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.



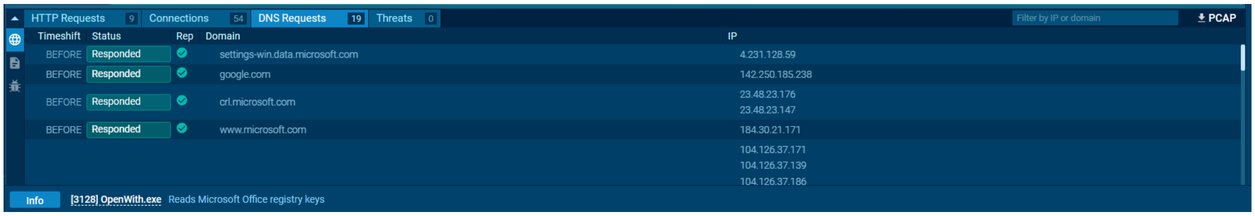
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	5488	MoUsoCoreWorker.exe	🇩🇪	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	1 Kb binary
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	1 Kb binary
BEFORE	GET 200: OK	✓	5488	MoUsoCoreWorker.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	973 b binary
8071 ms	GET 200: OK	✓	4360	SearchApp.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8...	314 b binary
8080 ms	GET 200: OK	✓	6384	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I...	471 b binary
28697 ms	GET 200: OK	✓	4448	SIHClient.exe	🇩🇪	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	419 b binary

Info [3128] OpenWith.exe Reads Microsoft Office registry keys



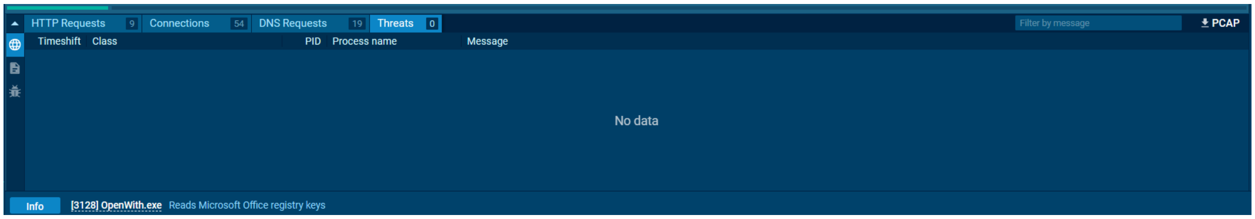
Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑ 816 b ↓ –
BEFORE	TCP	✓	6944	svchost.exe	🇮🇪	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	No Data
BEFORE	TCP	✓	–	–	🇮🇪	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 1 Kb ↓ 4 Kb
BEFORE	TCP	✓	–	–	🇮🇪	4.231.128.59	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	↑ 888 b ↓ 4 Kb
BEFORE	TCP	✓	5488	MoUsoCoreWorker.exe	🇩🇪	23.48.23.176	80	crl.microsoft.com	Akamai International B.V.	↑ 216 b ↓ 1 Kb
BEFORE	TCP	✓	–	–	🇩🇪	23.48.23.176	80	crl.microsoft.com	Akamai International B.V.	↑ 216 b ↓ 1 Kb
BEFORE	UDP	✓	4020	svchost.exe	?	239.255.255.250	1900	–	–	↑ 411 b ↓ –

Info [3128] OpenWith.exe Reads Microsoft Office registry keys



Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	4.231.128.59
BEFORE	Responded	✓	google.com	142.250.185.238
BEFORE	Responded	✓	crl.microsoft.com	23.48.23.176 23.48.23.147
BEFORE	Responded	✓	www.microsoft.com	184.30.21.171
				104.126.37.171 104.126.37.139 104.126.37.186

Info [3128] OpenWith.exe Reads Microsoft Office registry keys

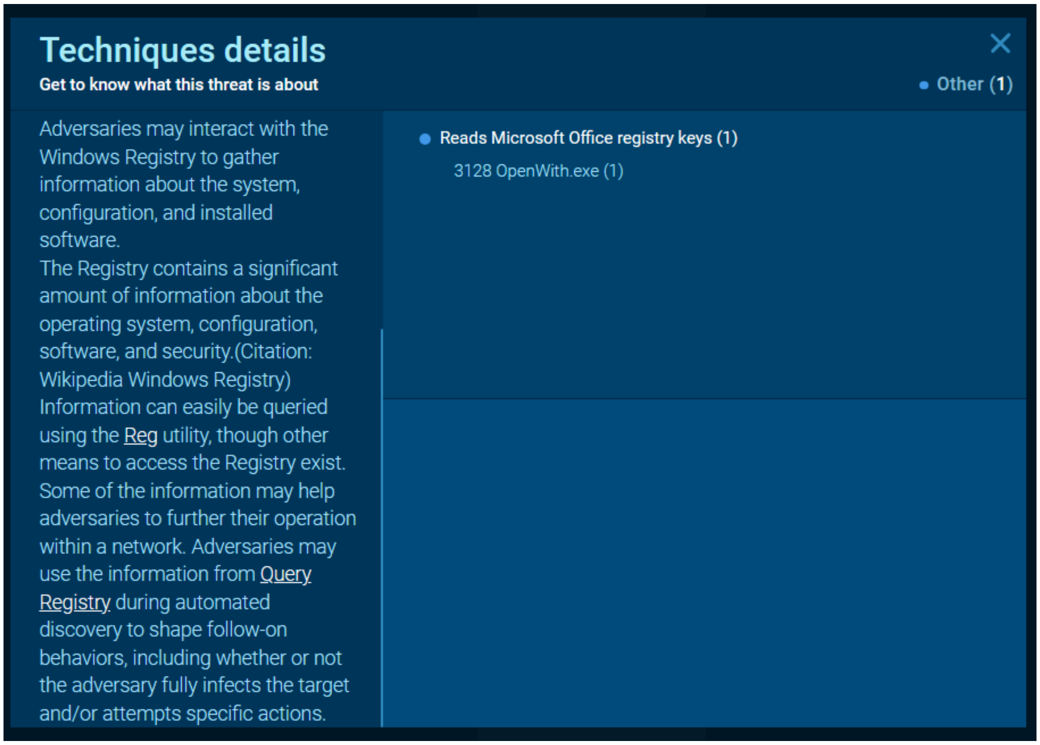


Timeshift	Class	PID	Process name	Message

No data

Info [3128] OpenWith.exe Reads Microsoft Office registry keys

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.



Techniques details

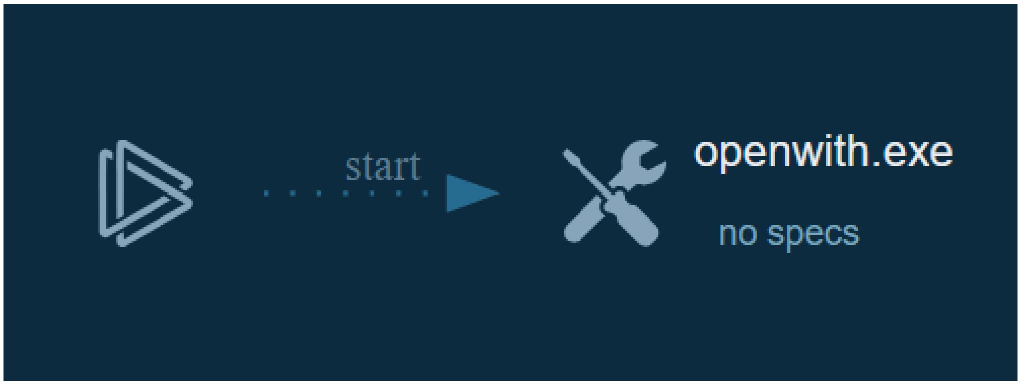
Get to know what this threat is about

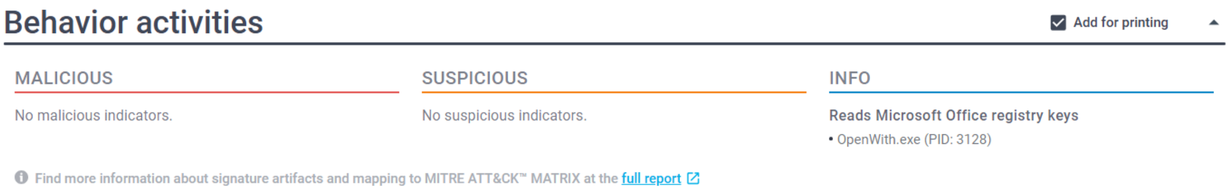
● Other (1)

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) Information can easily be queried using the Reg utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from Query Registry during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

● Reads Microsoft Office registry keys (1)

3128 OpenWith.exe (1)





Behavior activities

☑ Add for printing

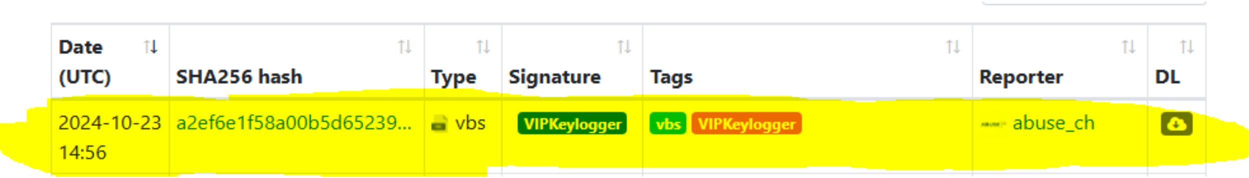
MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	No suspicious indicators.	Reads Microsoft Office registry keys • OpenWith.exe (PID: 3128)

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

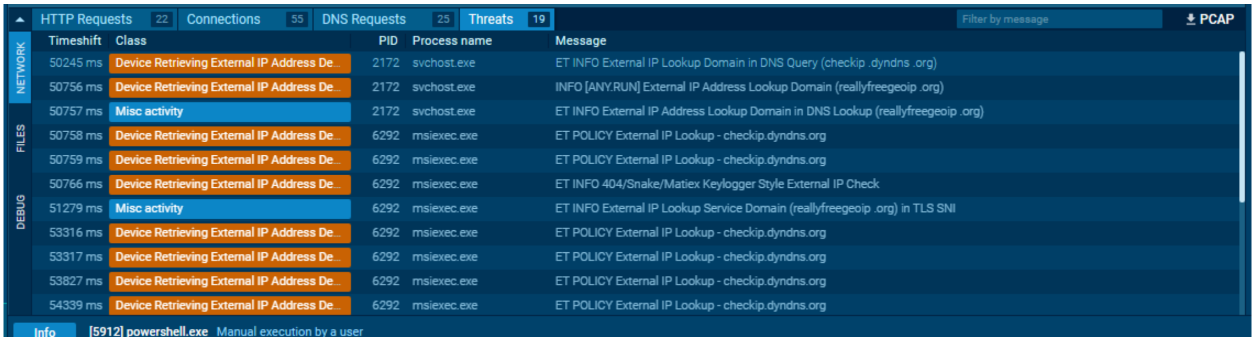
Task-8: Based on the information you found from Task-6 and Task-7, briefly explain the main characteristics of the malware sample.

This malware executed the Microsoft openwith.exe process in order to read Microsoft Office registry keys. No further actions were 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.

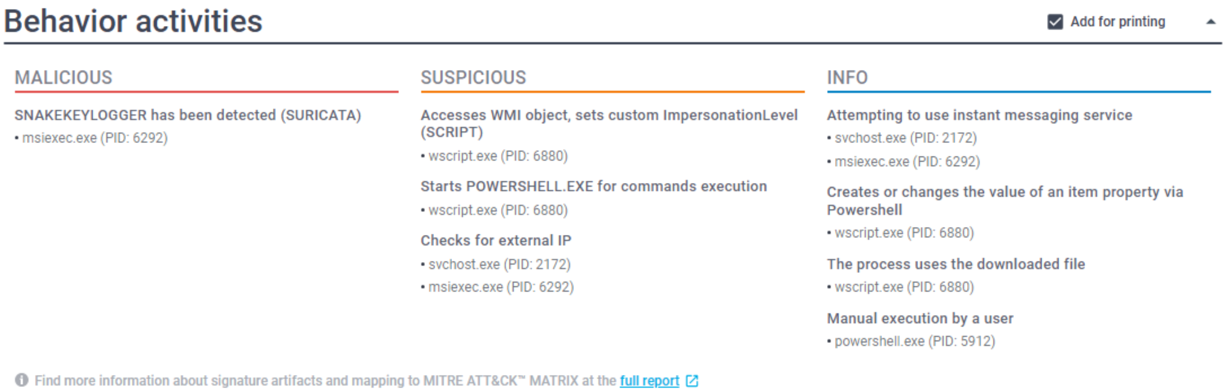


Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-10-23 14:56	a2ef6e1f58a00b5d65239...	vbs	VIPKeylogger	vbs VIPKeylogger	abuse_ch	



Timeshift	Class	PID	Process name	Message
50245 ms	Device Retrieving External IP Address De...	2172	svchost.exe	ET INFO External IP Lookup Domain in DNS Query (checkip .dyndns .org)
50756 ms	Device Retrieving External IP Address De...	2172	svchost.exe	INFO [ANY.RUN] External IP Address Lookup Domain (reallyfreegeoip .org)
50757 ms	Misc activity	2172	svchost.exe	ET INFO External IP Address Lookup Domain in DNS Lookup (reallyfreegeoip .org)
50758 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org
50759 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org
50766 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET INFO 404/Snake/Matiex Keylogger Style External IP Check
51279 ms	Misc activity	6292	msiexec.exe	ET INFO External IP Lookup Service Domain (reallyfreegeoip .org) in TLS SNI
53316 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org
53317 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org
53827 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org
54339 ms	Device Retrieving External IP Address De...	6292	msiexec.exe	ET POLICY External IP Lookup - checkip.dyndns.org

Info [5912] powershell.exe Manual execution by a user



Behavior activities

☑ Add for printing

MALICIOUS

SNAKEKEYLOGGER has been detected (SURICATA)
- msiexec.exe (PID: 6292)

SUSPICIOUS

Accesses WMI object, sets custom ImpersonationLevel (SCRIPT)
- wscript.exe (PID: 6880)

Starts POWERSHELL.EXE for commands execution
- wscript.exe (PID: 6880)

Checks for external IP
- svchost.exe (PID: 2172)
- msiexec.exe (PID: 6292)

INFO

Attempting to use instant messaging service
- svchost.exe (PID: 2172)
- msiexec.exe (PID: 6292)

Creates or changes the value of an item property via Powershell
- wscript.exe (PID: 6880)

The process uses the downloaded file
- wscript.exe (PID: 6880)

Manual execution by a user
- powershell.exe (PID: 5912)

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

This malware sample is a key logger, which records every key pressed on the device. SNAKEKEYLOGGER was detected by Suricata when it was delivered via “msiexec.exe”. wscript.exe used Powershell to run commands. In order to communicate with external servers, both msiexec.exe and svchost.exe attempted to use an instant messaging service.

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

While mirai and VIPKeylogger are both types of malwares, they differ in their objectives. VIPKeyloggers are designed to record the keys pressed on the device in order to steal credentials or other personal data. VIPKeyloggers may also take screenshots of on-screen information. Mirai is designed to turn the infected device into part of a botnet, which then can be used to carry out tasks like DDoS attacks.