

Jonathan Roeseler

Task 1

authenticated. [Read here for more info](#)

MALWARE bazaar

Search: mirai

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-09-30 23:04	a94ca2fc16dbda883af9...	elf	Mirai	elf mirai upx-dec	abuse_ch	
2025-09-30 23:03	401d4390f5c88c606a17...	elf	Mirai	elf mirai UPX	abuse_ch	
2025-09-30 22:46	1e3a3f6ba08cf180698b...	elf	Mirai	elf mirai	abuse_ch	
2025-09-30 22:41	5ef88603f2b5de8dd35f...	elf	Mirai	elf mirai	abuse_ch	
2025-09-30 22:40	d3367e6bc6c0607e869...	elf	Mirai	elf mirai	abuse_ch	

Task 2

MalwareBazaar | SHA256: [a94ca2fc16dbda883af9a26c90a9e73a72245e778038a0bce85bab41f4860acf](#)

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please [Read here for more info](#)

MALWARE bazaar

Intelligence 11 | IOCs | YARA 4 | File information | Comments | Actions

Mirai Vendor detections: 11

SHA256 hash:	a94ca2fc16dbda883af9a26c90a9e73a72245e778038a0bce85bab41f4860acf
SHA3-384 hash:	3df3afafbf9a3048a846325c9b3823eac8583dddcf1c5455bec0715233f3654133e7a538eaf658f6ac19300853c623f
SHA1 hash:	aa66e6bb4bb58813a89857918d661d1190847797
MD5 hash:	d1336cafbd8080b9b0d24707c39167b
humanhash:	ceiling-utah-tennessee-video
File name:	Space.arm
Download:	download sample
Signature	Mirai Alert

Task 6

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
8741 ms	GET 200 OK	✓	1864	svchost.exe	oosp.digicert.com	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgU...	471 b binary
12842 ms	GET 200 OK	✓	1268	svchost.exe	crf.microsoft.com	http://crf.microsoft.com/pki/crl/products/MicRooCerAut2011_2...	825 b binary
12851 ms	GET 200 OK	✓	1268	svchost.exe	www.microsoft.com	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-...	814 b binary
28174 ms	GET 200 OK	✓	6812	SIHClient.exe	www.microsoft.com	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Pro...	419 b binary
28177 ms	GET 200 OK	✓	6812	SIHClient.exe	www.microsoft.com	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Up...	407 b binary
29170 ms	GET 200 OK	✓	6812	SIHClient.exe	www.microsoft.com	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20...	813 b binary
29181 ms	GET 200 OK	✓	6812	SIHClient.exe	crf.microsoft.com	http://crf.microsoft.com/pki/crl/products/MicRooCerAut_2010-	824 b binary

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	TCP	✓	5944	MoUsocoreWorker.exe	settings-win.data.microsoft.com	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-A...	No Data
BEFORE	UDP	✓	4	System	192.168.100.255	192.168.100.255	137	-	-	↑ 1 Kb ↓ -
BEFORE	TCP	✓	1268	svchost.exe	settings-win.data.microsoft.com	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-A...	No Data
BEFORE	TCP	✓	3852	RUXIMICS.exe	settings-win.data.microsoft.com	40.127.240.158	443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-A...	No Data
2572 ms	UDP	✓	4	System	192.168.100.255	192.168.100.255	138	-	-	↑ 2 Kb ↓ -
8717 ms	TCP	✓	1864	svchost.exe	login.live.com	40.126.32.72	443	login.live.com	MICROSOFT-CORP-MSN-A...	↑ 172 Kb ↓ 23 Kb
8738 ms	TCP	✓	1864	svchost.exe	ocsp.digicert.com	2.17.190.73	80	ocsp.digicert.com	AKAMAI-AS	↑ 236 b ↓ 725 b

BEFORE	Responded	✓	settings-win.data.microsoft.com	40.127.240.158
BEFORE	Responded	✓	google.com	172.217.16.206
				40.126.32.72
				40.126.32.140
				20.190.160.20
8708 ms	Responded	✓	login.live.com	20.190.160.132
				20.190.160.128
				20.190.160.3

Timeshift	Class	PID	Process name	Message
12781 ms	Unknown Traffic	-	-	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Task 7

File name: a94ca2fc16bdba883af9a26c90a9e73a72245e778038a0bce85bab41f4860acf.elf
 Full analysis: <https://app.any.run/tasks/7afb81d-6ccc-49fd-822d-95f718196398>
 Verdict: **No threats detected**
 Analysis date: September 30, 2025 at 22:11:11
 OS: Ubuntu 22.04.2
 MIME: application/x-executable
 File info: ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
 MDS: D1336CAFBD808089B0D24707C39167B
 SHA1: AA66E6BB4BB58813A89857918D661D1190847797
 SHA256: A94CA2FC16DBDA883AF9A26C90A9E73A72245E778038A0BCE85BAB41F4860ACF
 SSDEEP: 768:CTTWoAFkDYQZ+MGJ96W04wocouhGrjaLc/Aw3PQOiccc+VfvdK7NIWY8DyJh0cq:CTRAF0YQZK54JaMIO7ffdoWS1E1

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

No malicious indicators.

SUSPICIOUS

Modifies file or directory owner

- sudo (PID: 1907)

Executes commands using command-line interpreter

- sudo (PID: 1914)

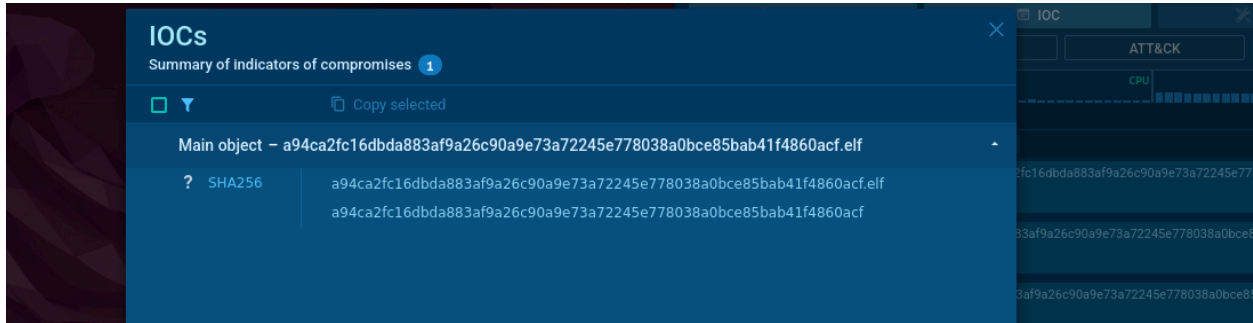
INFO

No info indicators.

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



Tactics	Techniques	Events	Enterprise & Mobile tactics	Danger	Warning	Other					
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Command and Scripting Interpreter (1/12) Unix Shell 2			File and Directory Permissions Modification (1/2) Linux and Mac File and Directory Permissions Modification							

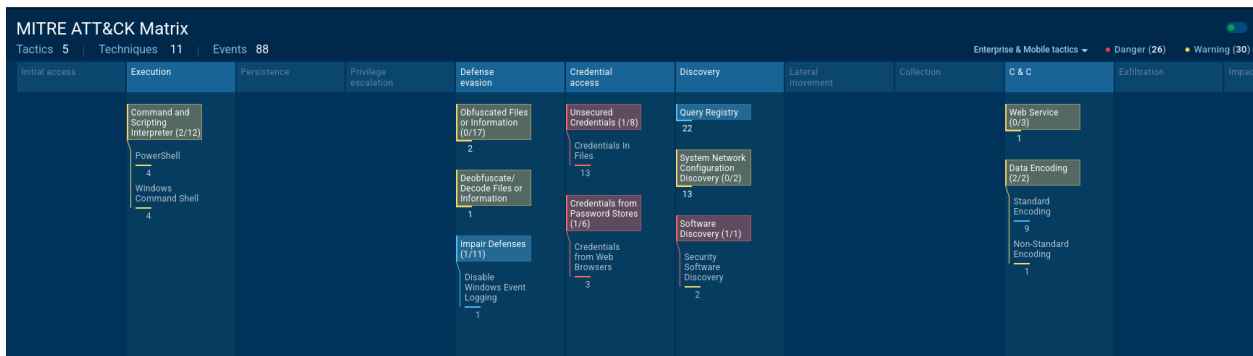


Task 8:

Unfortunately, any.run was not able to detect this malware due to various reasons and/or the malware has some evasion techniques. Ensuring that most of its processes were not actually seen in time. Some examples could be that it detects itself in a sandbox environment or it waits before connecting to externally controlled servers(at least a minute later). Some suspicious events were caught; however, such as running commands using the CLI (execution) and modifying file and directory permissions (Defense evasion).

Task 9:

This malware was easily classified by any.run. It quickly reached out to external servers/IPs and ran multiple processes in PowerShell, easily seen as malicious. It quickly ran a malicious PowerShell script to steal credentials, and it obfuscated some of its payloads.



As you can see below, much of its technique matches MITRE's ATT&CK framework.

Task10:

The Mirai malware is definitely more sophisticated, and it attempts to go under the radar. Mirai is more difficult to detect than the keylogger. As you can see between the two ATT&CK graphs, the keylogger was picked up on much better than the Mirai malware. Furthermore, unlike the Mirai malware, the keylogger was flagged as malicious almost instantly. The keylogger was definitely "loud" as it spawned hundreds of processes and made many system/file changes.