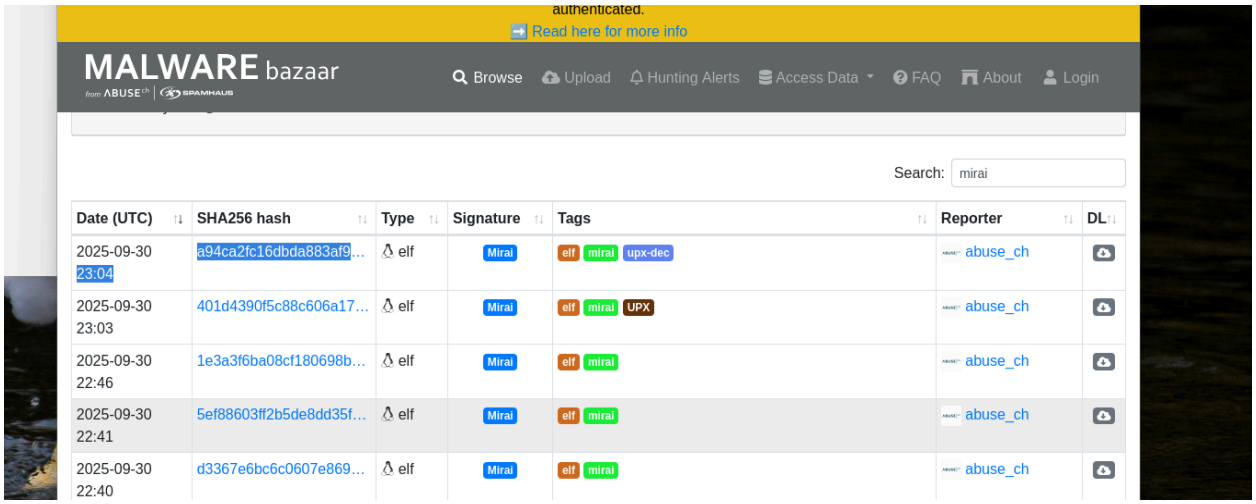
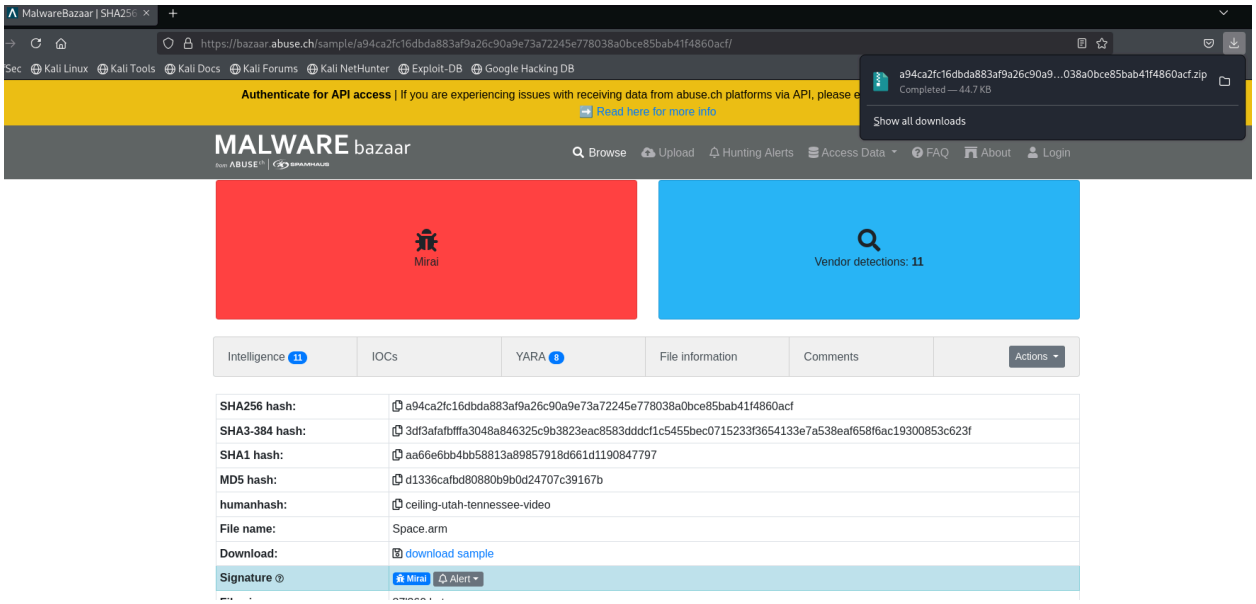
Jonathan Roeseler

Task 1

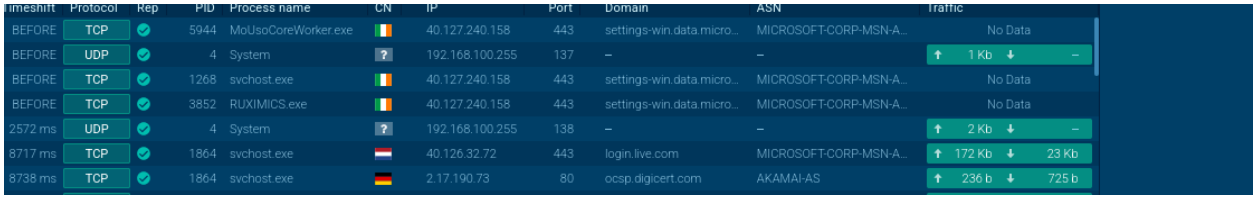


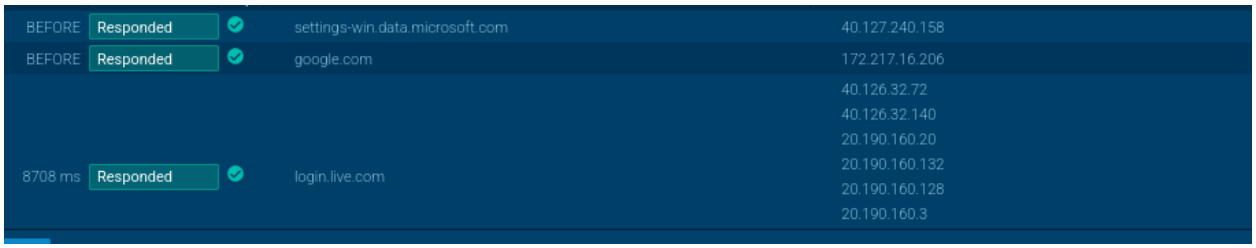
Task 2

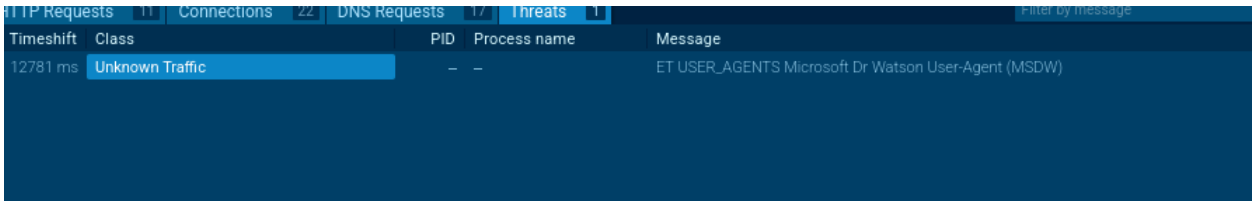


Task 6


HTTP Requests 11
Connections 22
DNS Requests 17
Threats 1
Filter by PID, name or url
PCAP
Timeshift Headers Rep PID Process name CN URL Content
8741 ms GET | 200: OK 1864 svchost.exe http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgU... 471 b binary
12842 ms GET | 200: OK 1268 svchost.exe http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2... 825 b binary
12851 ms GET | 200: OK 1268 svchost.exe http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-... 814 b binary
28174 ms GET | 200: OK 6812 SIHClient.exe http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Pro... 419 b binary
28177 ms GET | 200: OK 6812 SIHClient.exe http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Up... 407 b binary
29170 ms GET | 200: OK 6812 SIHClient.exe http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20... 813 b binary
29181 ms GET | 200: OK 6812 SIHClient.exe http://crl.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 40.127.240.158 443 settings-win.data.micro... MICROSOFT-CORP-MSN-A... No Data
BEFORE UDP 4 System 192.168.100.255 137 – – 1 Kb –
BEFORE TCP 1268 svchost.exe 40.127.240.158 443 settings-win.data.micro... MICROSOFT-CORP-MSN-A... No Data
BEFORE TCP 3852 RUXIMICS.exe 40.127.240.158 443 settings-win.data.micro... MICROSOFT-CORP-MSN-A... No Data
2572 ms UDP 4 System 192.168.100.255 138 – – 2 Kb –
8717 ms TCP 1864 svchost.exe 40.126.32.72 443 login.live.com MICROSOFT-CORP-MSN-A... 172 Kb 23 Kb
8738 ms TCP 1864 svchost.exe 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
8708 ms Responded login.live.com
40.126.32.72
40.126.32.140
20.190.160.20
20.190.160.132
20.190.160.128
20.190.160.3


Connections 22
DNS Requests 17
Threats 1
Timeshift Class PID Process name Message
12781 ms Unknown Traffic – – ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Task 7

File name:	a94ca2fc16dbda883af9a26c90a9e73a72245e778038a0bce85bab41f4860acf.elf
Full analysis:	https://app.any.run/tasks/7afbf81d-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
MD5:	D1336CAFBD80880B9B0D24707C39167B
SHA1:	AA66E6BB4BB58813A89857918D661D1190847797
SHA256:	A94CA2FC16DBDA883AF9A26C90A9E73A72245E778038A0BCE85BAB41F4860ACF
SSDEEP:	768:CTTWoAFkDYQZ+MGJ96WO4wocoulhGrjaLCt/Aw3PQOicc+VfvdK7NiWY8DyJh0cq:CTRAF0YQZK54jaMIO7ffdolWSv1El

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)

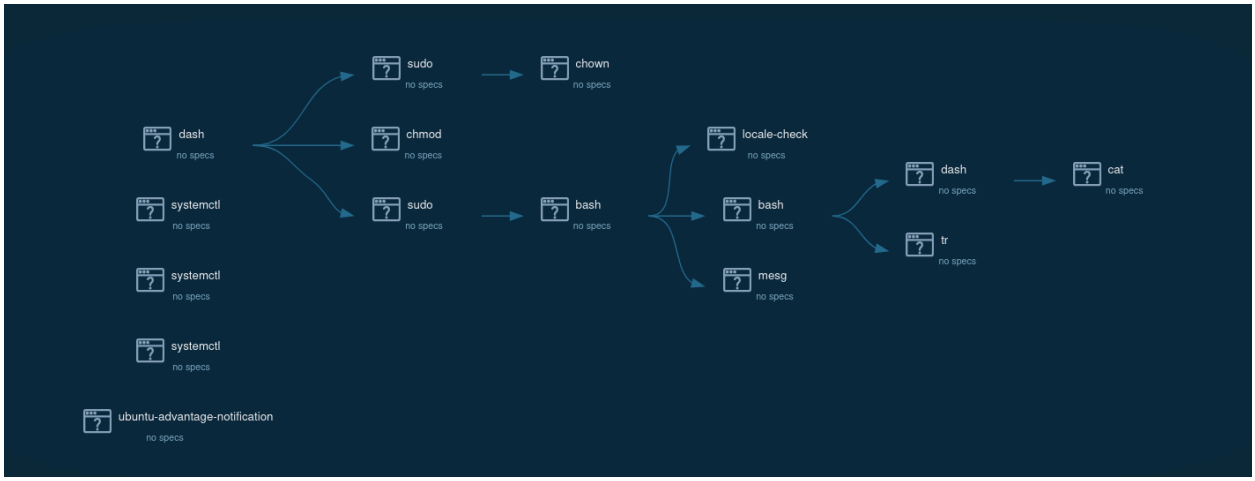
Executes commands using command-line interpreter

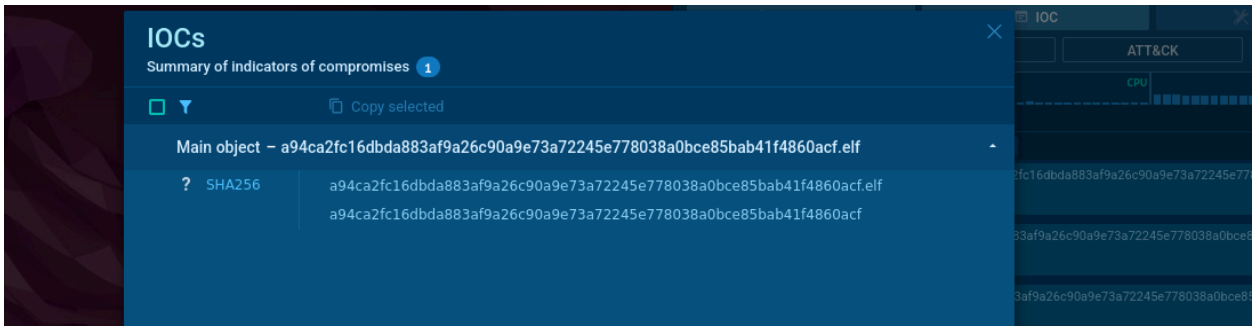
- sudo (PID: 1914)

INFO

No info indicators.

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



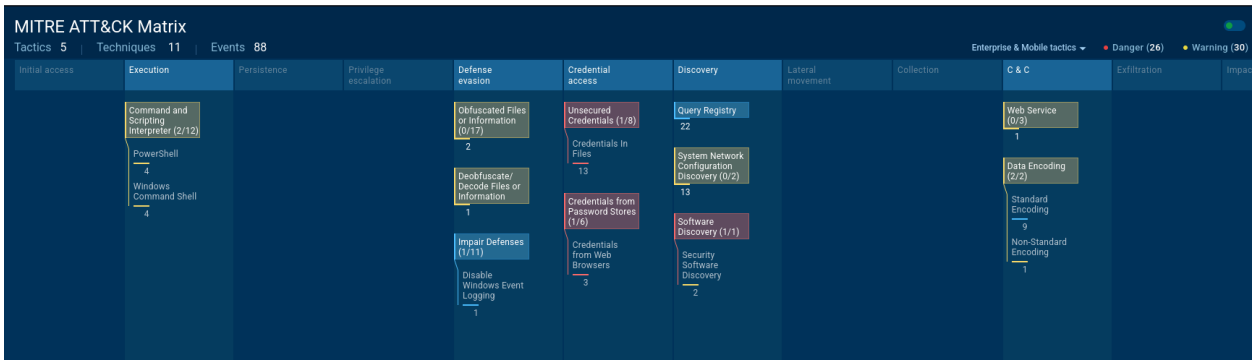


Task 8:

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.