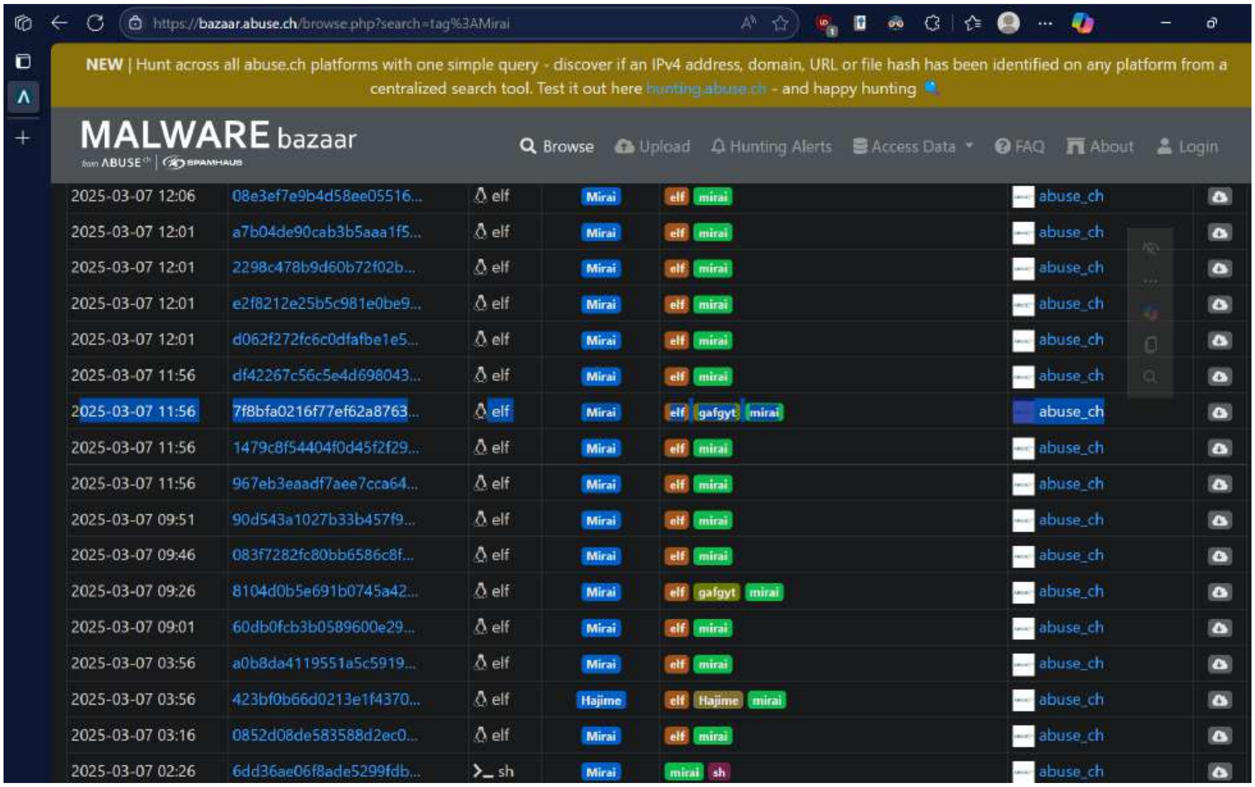
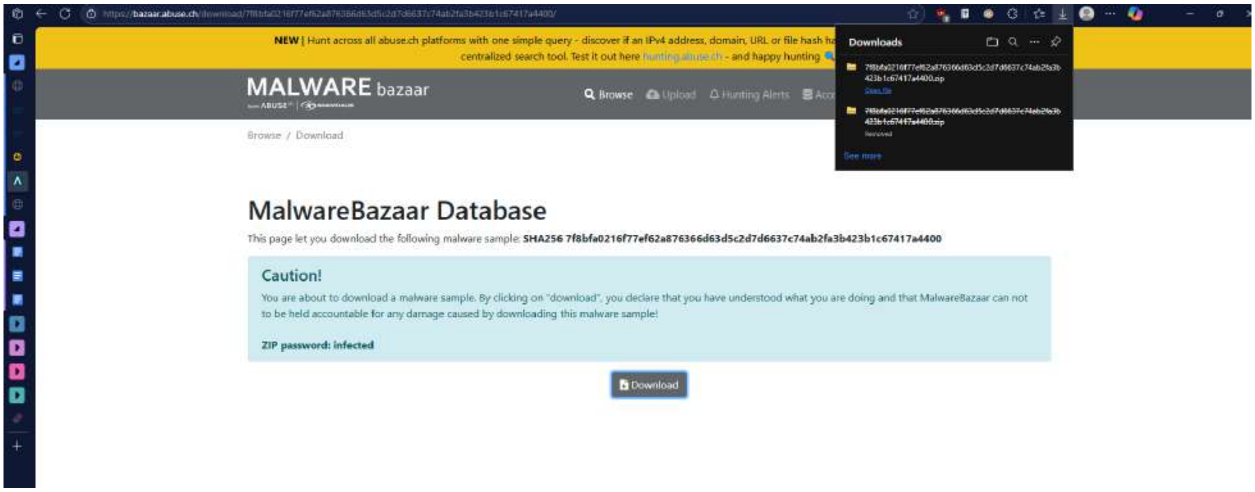
Task-1: Take a screenshot similar to the following screenshot and make sure you highlight the malware you selected



NEW | Hunt across all abuse.ch platforms with one simple query - discover if an IPv4 address, domain, URL or file hash has been identified on any platform from a centralized search tool. Test it out here hunting.abuse.ch - and happy hunting

2025-03-07 12:06	08e3ef7e9b4d58ee05516...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 12:01	a7b04de90cab3b5aaa1f5...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 12:01	2298c478b9d60b72f02b...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 12:01	e2f8212e25b5c981e0be9...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 12:01	d062f272fc6c0dfafbe1e5...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 11:56	df42267c56c5e4d698043...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 11:56	7f8bfa0216f77ef62a8763...	elf	Mirai	elf gafgyt mirai	abuse_ch
2025-03-07 11:56	1479c8f54404f0d45f2f29...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 11:56	967eb3eaadf7aee7cca64...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 09:51	90d543a1027b33b457f9...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 09:46	083f7282fc80bb6586c8f...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 09:26	8104d0b5e691b0745a42...	elf	Mirai	elf gafgyt mirai	abuse_ch
2025-03-07 09:01	60db0fcb3b0589600e29...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 03:56	a0b8da4119551a5c5919...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 03:56	423bf0b66d0213e1f4370...	elf	Hajime	elf Hajime mirai	abuse_ch
2025-03-07 03:16	0852d08de583588d2ec0...	elf	Mirai	elf mirai	abuse_ch
2025-03-07 02:26	6dd36ae06f8ade5299fdb...	>_ sh	Mirai	mirai sh	abuse_ch

Task-2: Take a screenshot showing the downloaded malware sample in your computer


https://bazaar.abuse.ch/download/7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400/
MALWARE bazaar
from ABUSE.ch | SPAMHAUS
Browse
Upload
Hunting Alerts
Acc
Downloads
See more
Download

NEW | Hunt across all abuse.ch platforms with one simple query - discover if an IPv4 address, domain, URL or file hash ha centralized search tool. Test it out here hunting.abuse.ch - and happy hunting

7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400.zip
Open file

~~7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400.zip~~
Removed

Browse / Download

MalwareBazaar Database

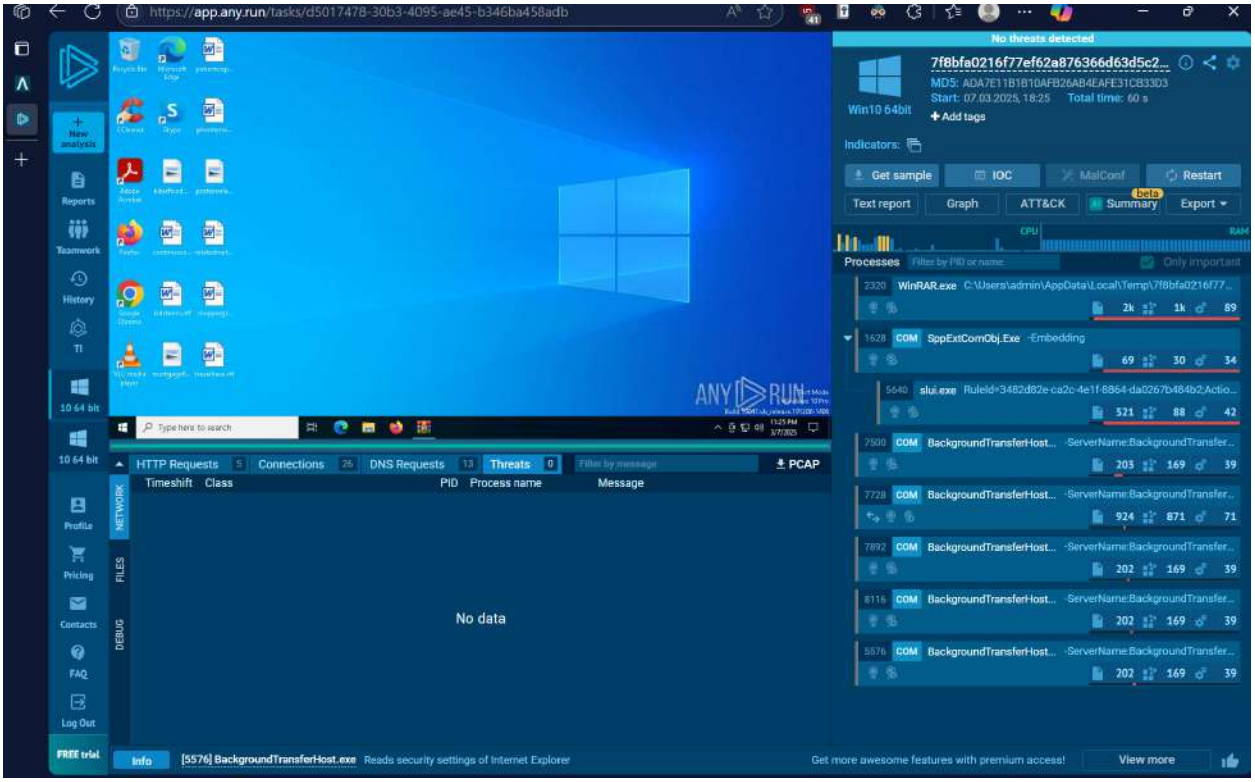
This page let you download the following malware sample: **SHA256 7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400**

Caution!

You are about to download a malware sample. By clicking on "download", you declare that you have understood what you are doing and that MalwareBazaar can not to be held accountable for any damage caused by downloading this malware sample!

ZIP password: infected

Task-6: Go through all the information you find for each category



https://app.any.run/tasks/d5017478-30b3-4095-ae45-b346ba458adb

No threats detected

7f8bfa0216f77ef62a876366d63d5c2...
MD5: ADA7E11B1B10AFB26AB4EAFE31CB33D3
Start: 07.03.2025, 18:25 Total time: 60 s
Win10 64bit

PID	Process	Arguments			
2320	WinRAR.exe	C:\Users\admin\AppData\Local\Temp\7f8bfa0216f77...	2k	1k	89
1628	COM SppExtComObj.Exe	-Embedding	69	30	34
5640	slui.exe	RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Actio...	521	88	42
7500	COM BackgroundTransferHost...	-ServerName:BackgroundTransfer...	203	169	39
7728	COM BackgroundTransferHost...	-ServerName:BackgroundTransfer...	924	871	71
7892	COM BackgroundTransferHost...	-ServerName:BackgroundTransfer...	202	169	39
8116	COM BackgroundTransferHost...	-ServerName:BackgroundTransfer...	202	169	39
5576	COM BackgroundTransferHost...	-ServerName:BackgroundTransfer...	202	169	39

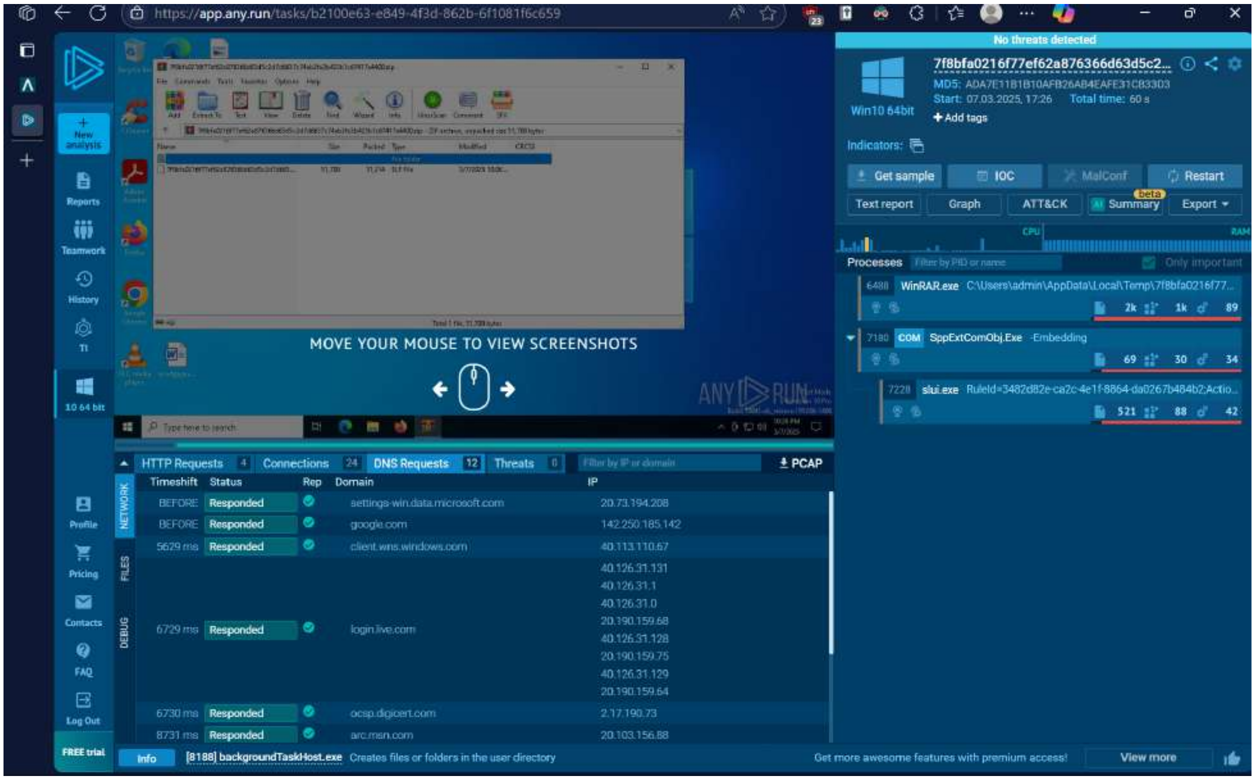
HTTP Requests 5 | Connections 26 | DNS Requests 13 | Threats 0

Timeshift	Class	PID	Process name	Message

No data

Info [5576] BackgroundTransferHost.exe Reads security settings of Internet Explorer

Get more awesome features with premium access!



https://app.any.run/tasks/b2100e63-e849-4f3d-862b-6f1081f6c659

No threats detected

7f8bfa0216f77ef62a876366d63d5c2...
MD5: ADA7E11B1B10AFB26AB4EAFE31CB33D3
Start: 07.03.2025, 17:26 Total time: 60 s
Win10 64bit

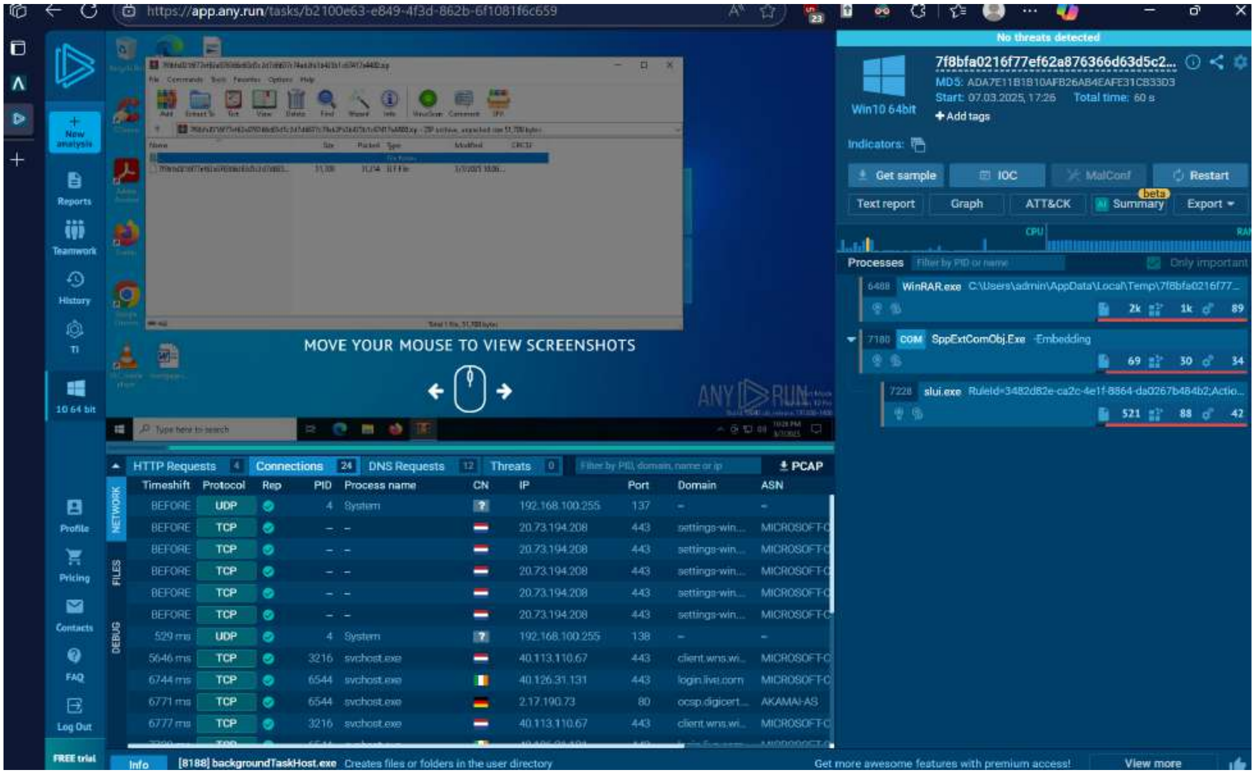
PID	Process	Arguments			
6488	WinRAR.exe	C:\Users\admin\AppData\Local\Temp\7f8bfa0216f77...	2k	1k	89
7180	COM SppExtComObj.Exe	-Embedding	69	30	34
7228	slui.exe	RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Actio...	521	88	42

HTTP Requests 4 | Connections 24 | DNS Requests 12 | Threats 0

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	20.73.194.208
BEFORE	Responded	✓	google.com	142.250.185.142
5629 ms	Responded	✓	client.wns.windows.com	40.113.110.67
6729 ms	Responded	✓	login.live.com	40.126.31.131 40.126.31.1 40.126.31.0 20.190.159.68 40.126.31.128 20.190.159.75 40.126.31.129 20.190.159.64
6730 ms	Responded	✓	ocsp.digicert.com	2.17.190.73
8731 ms	Responded	✓	arc.msn.com	20.103.156.88

Info [8188] backgroundTaskHost.exe Creates files or folders in the user directory

Get more awesome features with premium access!



https://app.any.run/tasks/b2100e63-e849-4f3d-862b-6f1081f6c659

No threats detected

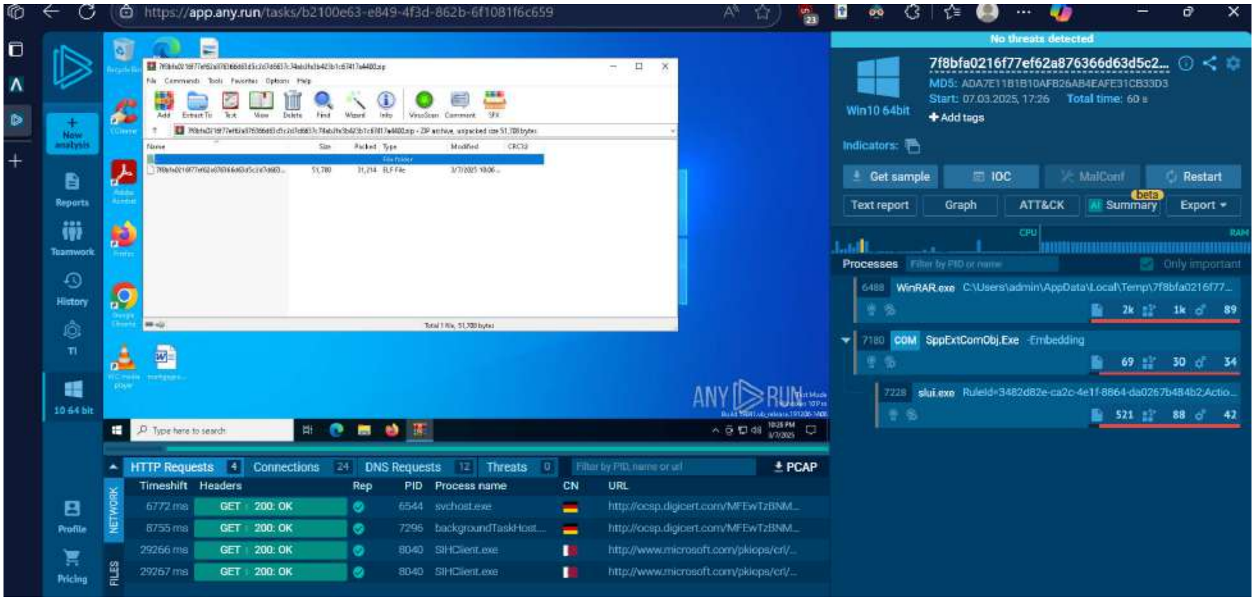
7f8bfa0216f77ef62a876366d63d5c2...
MD5: ADA7E11B1B10AFB26AB4EAFE31CB33D3
Start: 07.03.2025, 17:26 Total time: 60 s
Win10 64bit

Processes					
6488 WinRAR.exe C:\Users\admin\AppData\Local\Temp\7f8bfa0216f77...	2k	1k	89
7180 COM SppExtComObj.Exe -Embedding	69	30	34
7228 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Actio...	521	88	42

HTTP Requests 4 | Connections 24 | DNS Requests 12 | Threats 0

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	–	–
BEFORE	TCP	✓	–	–		20.73.194.208	443	settings-win...	MICROSOFT-C
BEFORE	TCP	✓	–	–		20.73.194.208	443	settings-win...	MICROSOFT-C
BEFORE	TCP	✓	–	–		20.73.194.208	443	settings-win...	MICROSOFT-C
BEFORE	TCP	✓	–	–		20.73.194.208	443	settings-win...	MICROSOFT-C
BEFORE	TCP	✓	–	–		20.73.194.208	443	settings-win...	MICROSOFT-C
529 ms	UDP	✓	4	System	?	192.168.100.255	138	–	–
5646 ms	TCP	✓	3216	svchost.exe		40.113.110.67	443	client.wns.wi...	MICROSOFT-C
6744 ms	TCP	✓	6544	svchost.exe		40.126.31.131	443	login.live.com	MICROSOFT-C
6771 ms	TCP	✓	6544	svchost.exe		2.17.190.73	80	ocsp.digicert...	AKAMAI-AS
6777 ms	TCP	✓	3216	svchost.exe		40.113.110.67	443	client.wns.wi...	MICROSOFT-C

Info [8188] backgroundTaskHost.exe Creates files or folders in the user directory



https://app.any.run/tasks/b2100e63-e849-4f3d-862b-6f1081f6c659

No threats detected

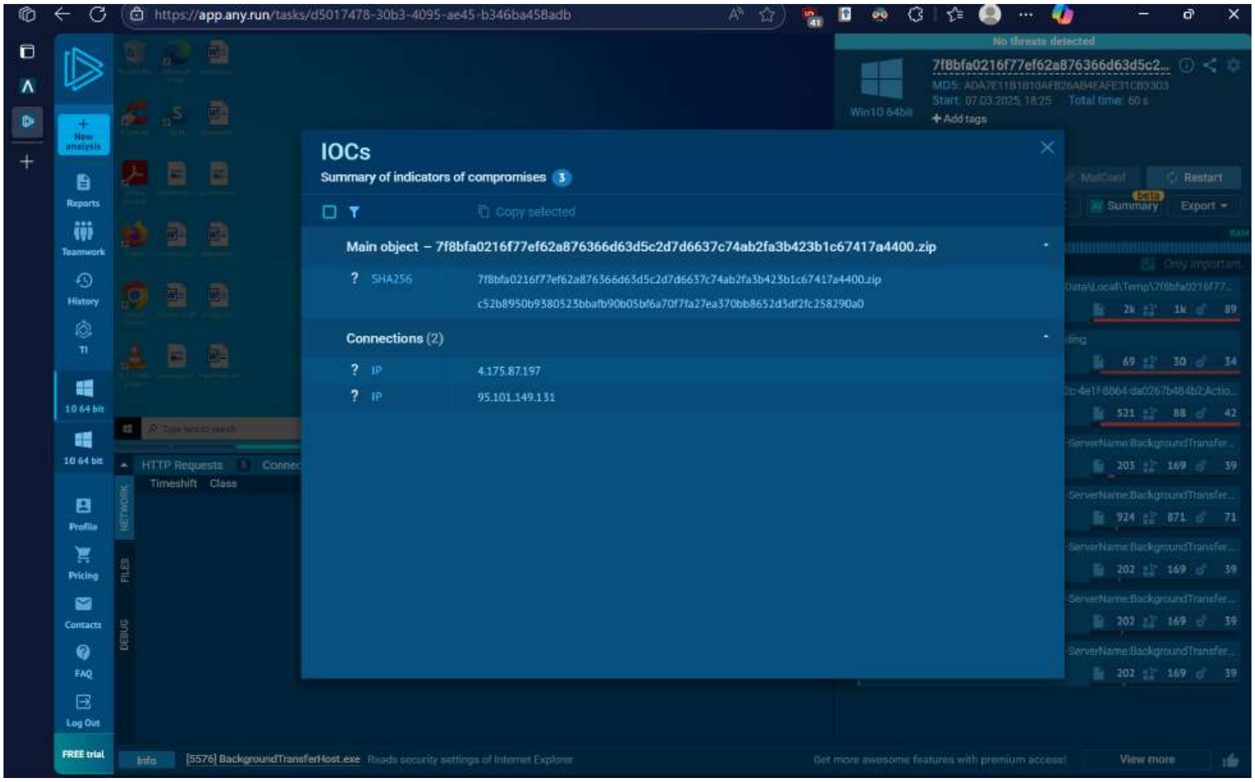
7f8bfa0216f77ef62a876366d63d5c2...
MD5: ADA7E11B1B10AFB26AB4EAFE31CB33D3
Start: 07.03.2025, 17:26 Total time: 60 s
Win10 64bit

6488 WinRAR.exe C:\Users\admin\AppData\Local\Temp\7f8bfa0216f77... 2k 1k 89
7180 COM SppExtComObj.Exe -Embedding 69 30 34
7228 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Actio... 521 88 42

HTTP Requests 4 | Connections 24 | DNS Requests 12 | Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL
6772 ms	GET 200: OK	✓	6544	svchost.exe		http://ocsp.digicert.com/MFEwTzBNM...
8755 ms	GET 200: OK	✓	7296	backgroundTaskHost...		http://ocsp.digicert.com/MFEwTzBNM...
29266 ms	GET 200: OK	✓	8040	SIHClient.exe		http://www.microsoft.com/pkiops/crl/...
29267 ms	GET 200: OK	✓	8040	SIHClient.exe		http://www.microsoft.com/pkiops/crl/...

Task-7: Explore information found in the IOC, Text Report, Graph, and ATT&CK tabs



https://app.any.run/tasks/d5017478-30b3-4095-ae45-b346ba458adb

No threats detected

7f8bfa0216f77ef62a876366d63d5c2...
MD5: ADA7E11B1810AFB26AB4EAFE31CB33D3
Start: 07.03.2025, 18:25 Total time: 60 s

IOCs

Summary of indicators of compromises 3

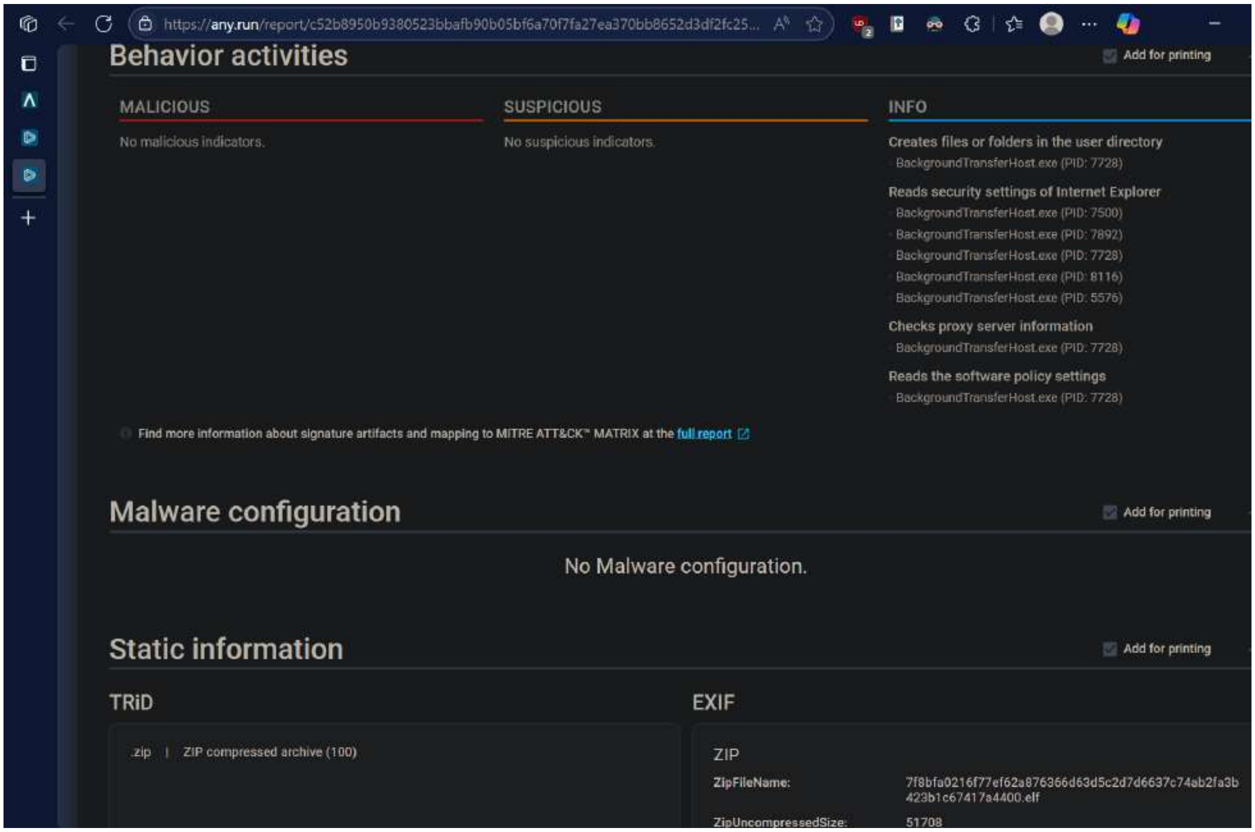
Main object – 7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400.zip

? SHA256 7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400.zip
c52b8950b9380523bbafb90b05bf6a70f7fa27ea370bb8652d3df2fc258290a0

Connections (2)

? IP 4.175.87.197
? IP 95.101.149.131

[5576] BackgroundTransferHost.exe Reads security settings of Internet Explorer



https://any.run/report/c52b8950b9380523bbafb90b05bf6a70f7fa27ea370bb8652d3df2fc25...

Behavior activities

☑ Add for printing

MALICIOUS

No malicious indicators.

SUSPICIOUS

No suspicious indicators.

INFO

Creates files or folders in the user directory
- BackgroundTransferHost.exe (PID: 7728)

Reads security settings of Internet Explorer
- BackgroundTransferHost.exe (PID: 7500)
- BackgroundTransferHost.exe (PID: 7892)
- BackgroundTransferHost.exe (PID: 7728)
- BackgroundTransferHost.exe (PID: 8116)
- BackgroundTransferHost.exe (PID: 5576)

Checks proxy server information
- BackgroundTransferHost.exe (PID: 7728)

Reads the software policy settings
- BackgroundTransferHost.exe (PID: 7728)

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

Malware configuration

☑ Add for printing

No Malware configuration.

Static information

☑ Add for printing

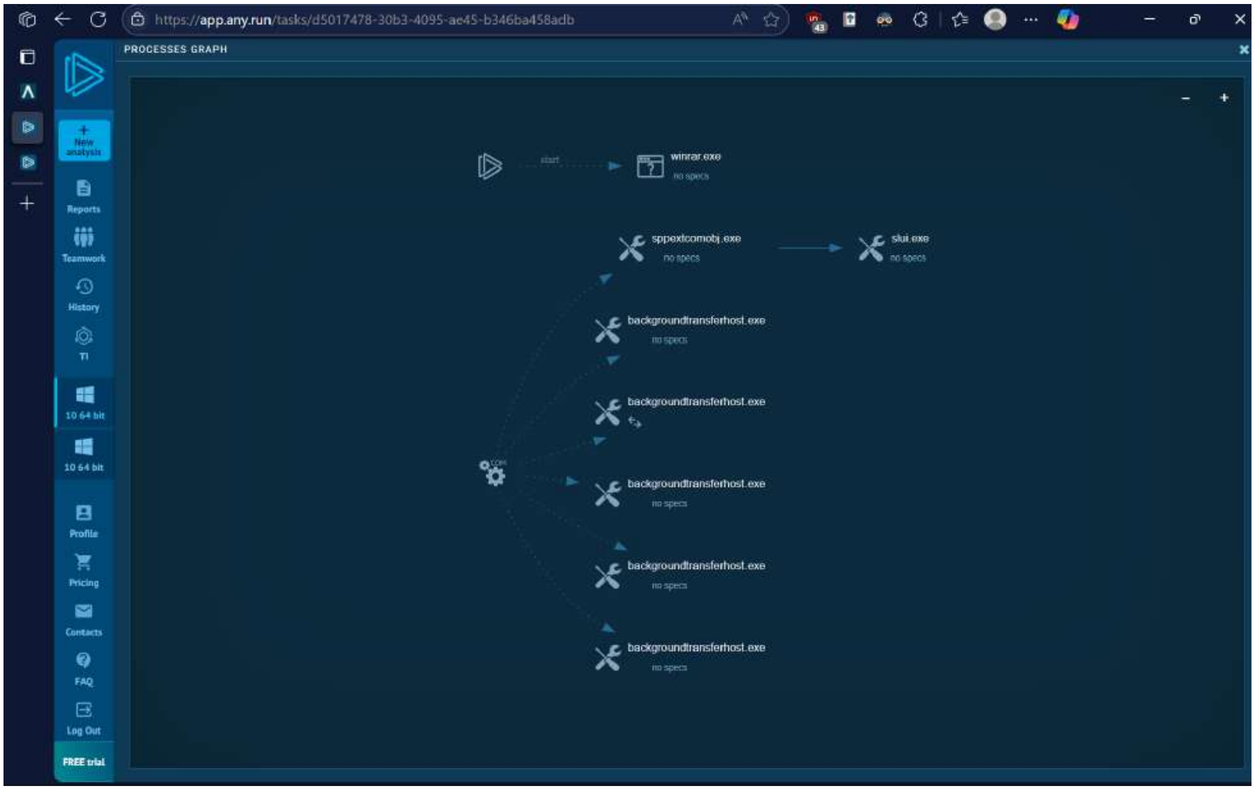
TRiD

.zip | ZIP compressed archive (100)

EXIF

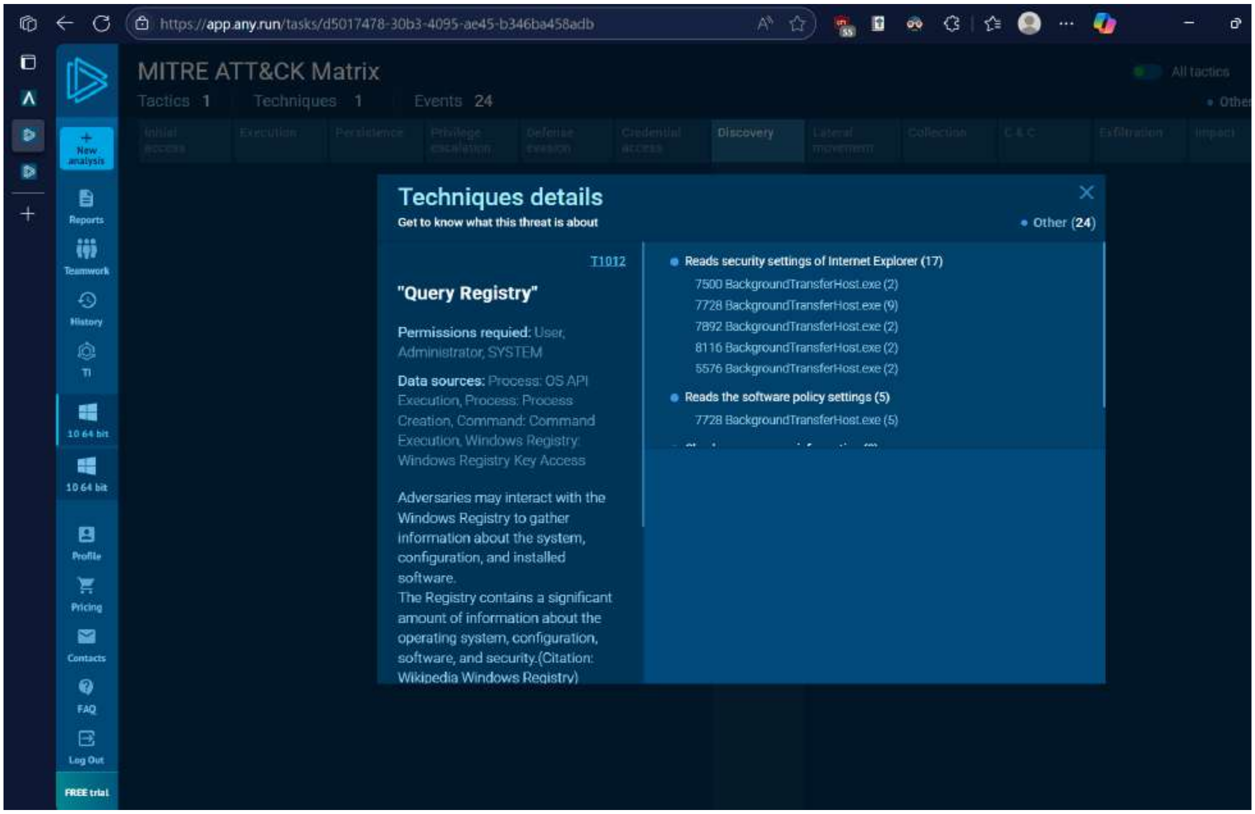
ZIP

ZipFileName:	7f8bfa0216f77ef62a876366d63d5c2d7d6637c74ab2fa3b423b1c67417a4400.elf
ZipUncompressedSize:	51708



https://app.any.run/tasks/d5017478-30b3-4095-ae45-b346ba458adb

PROCESSES GRAPH



Techniques details

Get to know what this threat is about

Other (24)

T1012

"Query Registry"

Permissions requied: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

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)

- Reads security settings of Internet Explorer (17)
  - 7500 BackgroundTransferHost.exe (2)
  - 7728 BackgroundTransferHost.exe (9)
  - 7892 BackgroundTransferHost.exe (2)
  - 8116 BackgroundTransferHost.exe (2)
  - 5576 BackgroundTransferHost.exe (2)
- Reads the software policy settings (5)
  - 7728 BackgroundTransferHost.exe (5)

Task-8: briefly explain the main characteristics of the malware sample

- It probably didn’t work because I couldn’t open it properly, but I believe it would try to connect to other devices to target and send packets to attempt a DDoS.

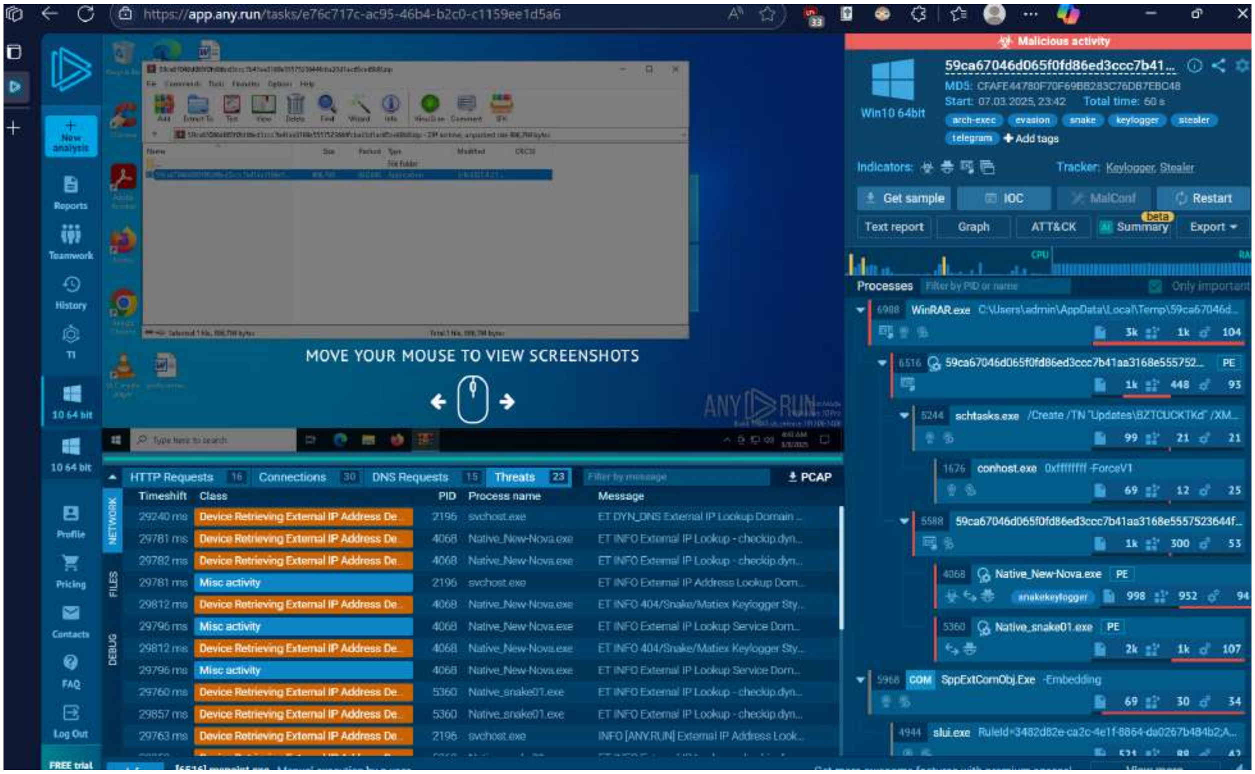
Task-9: Based on your analysis, explain the main characteristics of this malware sample

- Once extracted, it starts a malware named Native_snake01.exe that harvests all web browser credentials and personal data. It also checks to see if an antivirus program is running and device info.

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

- The keylogger tries to gain all credentials to steal your information, while Mirai tries to input your information to attack other devices wirelessly.

Task 9 Cont:



https://app.any.run/tasks/e76c717c-ac95-46b4-b2c0-c1159ee1d5a6

HTTP Requests 16 | Connections 30 | DNS Requests 15 | Threats 23

Timeshift	Class	PID	Process name	Message
29240 ms	Device Retrieving External IP Address De...	2196	svchost.exe	ET DYN_DNS External IP Lookup Domain ...
29781 ms	Device Retrieving External IP Address De...	4068	Native_New-Nova.exe	ET INFO External IP Lookup - checkip.dyn...
29782 ms	Device Retrieving External IP Address De...	4068	Native_New-Nova.exe	ET INFO External IP Lookup - checkip.dyn...
29781 ms	Misc activity	2196	svchost.exe	ET INFO External IP Address Lookup Dom...
29812 ms	Device Retrieving External IP Address De...	4068	Native_New-Nova.exe	ET INFO 404/Snake/Matiex Keylogger Sty...
29796 ms	Misc activity	4068	Native_New-Nova.exe	ET INFO External IP Lookup Service Dom...
29812 ms	Device Retrieving External IP Address De...	4068	Native_New-Nova.exe	ET INFO 404/Snake/Matiex Keylogger Sty...
29796 ms	Misc activity	4068	Native_New-Nova.exe	ET INFO External IP Lookup Service Dom...
29760 ms	Device Retrieving External IP Address De...	5360	Native_snake01.exe	ET INFO External IP Lookup - checkip.dyn...
29857 ms	Device Retrieving External IP Address De...	5360	Native_snake01.exe	ET INFO External IP Lookup - checkip.dyn...
29763 ms	Device Retrieving External IP Address De...	2196	svchost.exe	INFO [ANY.RUN] External IP Address Look...

[6516] ...

Malicious activity

59ca67046d065f0fd86ed3ccc7b41...

Win10 64bit

MD5: CFAFE44780F70F69BB283C76DB7EBC48

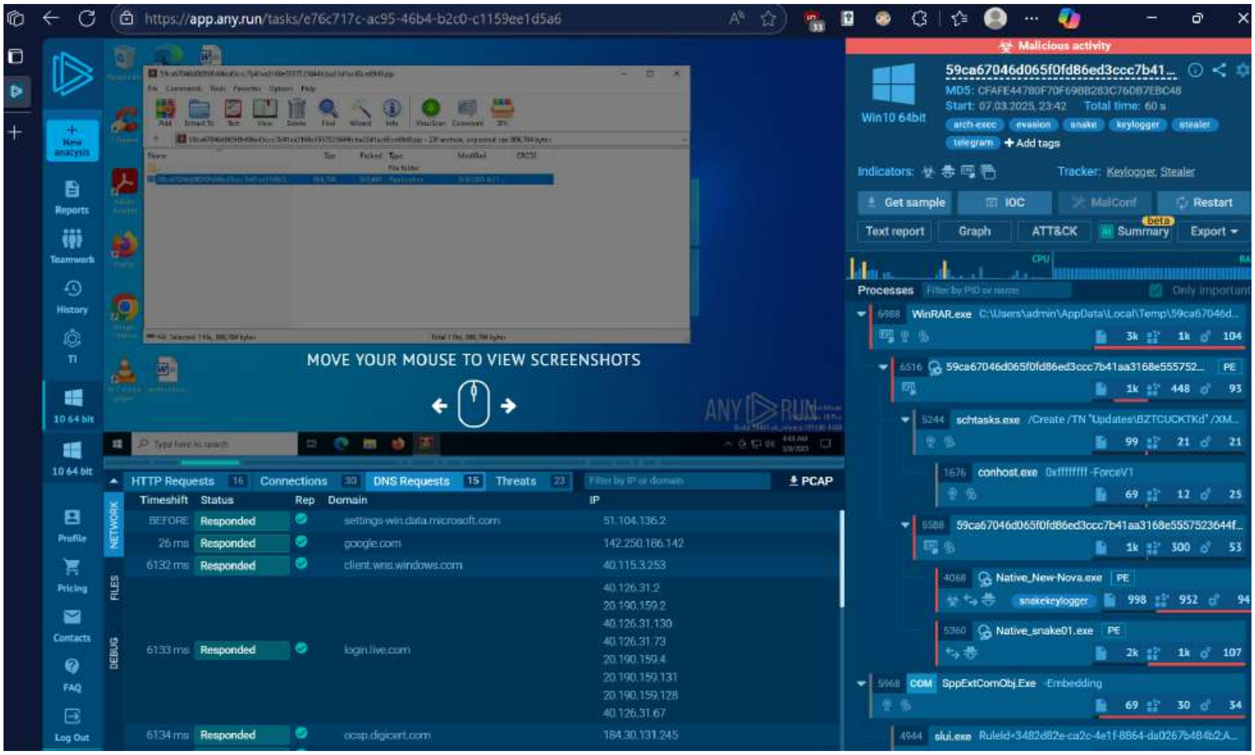
Start: 07.03.2025, 23:42 Total time: 60 s

arch-exec evasion snake keylogger stealer telegram + Add tags

Indicators: Tracker: Keylogger, Stealer

Processes

```
6988 WinRAR.exe C:\Users\admin\AppData\Local\Temp\59ca67046d...          3k  1k  104
  6516 59ca67046d065f0fd86ed3ccc7b41aa3168e555752... PE                  1k  448  93
    5244 schtasks.exe /Create /TN "Updates\BZTCUCKTKd" /XM...            99  21  21
      1676 conhost.exe 0xffffffff -ForceV1                               69  12  25
    5588 59ca67046d065f0fd86ed3ccc7b41aa3168e5557523644f...             1k  300  53
      4068 Native_New-Nova.exe PE  snakekeylogger                       998  952  94
      5360 Native_snake01.exe PE                                         2k  1k  107
5968 COM SppExtComObj.Exe -Embedding                                     69  30  34
  4944 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;A...
```



https://app.any.run/tasks/e76c717c-ac95-46b4-b2c0-c1159ee1d5a6

HTTP Requests 16 | Connections 30 | DNS Requests 15 | Threats 23

Timeshift	Status	Rep	Domain	IP
BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2
26 ms	Responded	✓	google.com	142.250.186.142
6132 ms	Responded	✓	client.wns.windows.com	40.115.3.253
6133 ms	Responded	✓	login.live.com	40.126.31.2 20.190.159.2 40.126.31.130 40.126.31.73 20.190.159.4 20.190.159.131 20.190.159.128 40.126.31.67
6134 ms	Responded	✓	ocsp.digicert.com	184.30.131.245

Malicious activity

59ca67046d065f0fd86ed3ccc7b41...

Win10 64bit

MD5: CFAFE44780F70F69BB283C76DB7EBC48

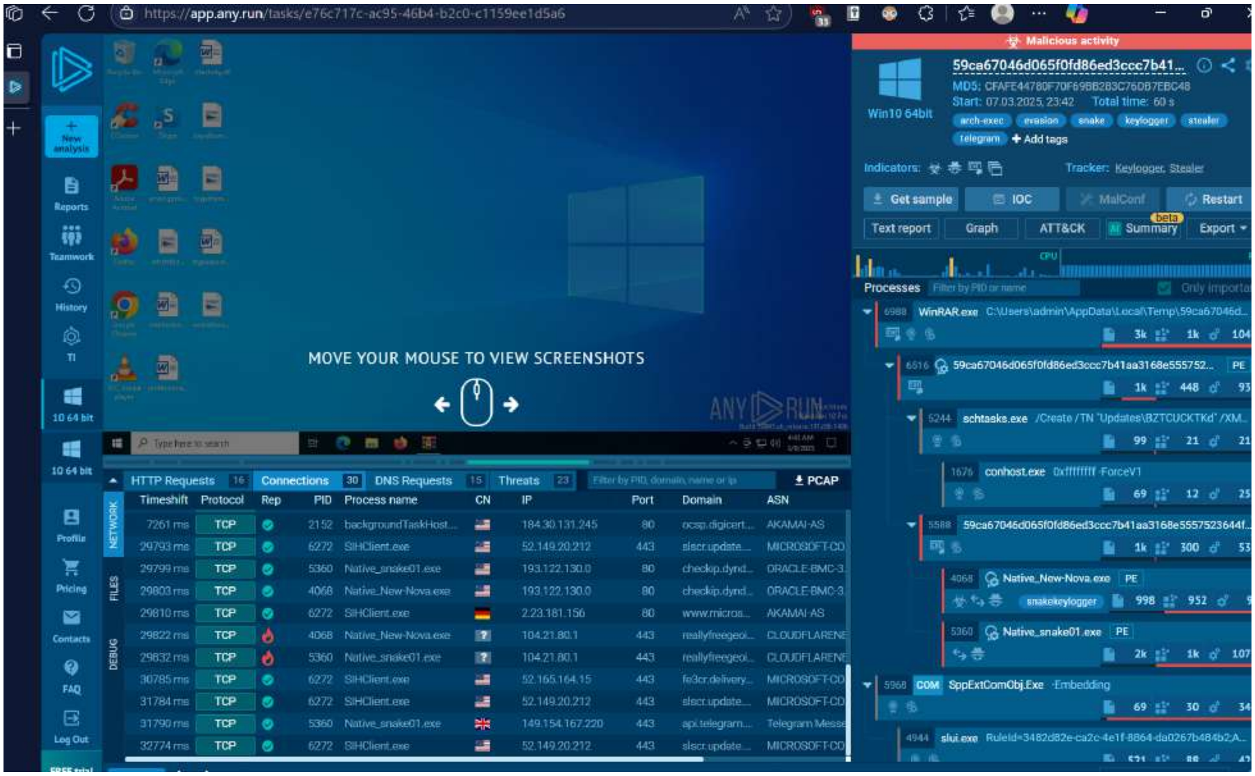
Start: 07.03.2025, 23:42 Total time: 60 s

arch-exec evasion snake keylogger stealer telegram + Add tags

Indicators: Tracker: Keylogger, Stealer

Processes

```
6988 WinRAR.exe C:\Users\admin\AppData\Local\Temp\59ca67046d...          3k  1k  104
  6516 59ca67046d065f0fd86ed3ccc7b41aa3168e555752... PE                  1k  448  93
    5244 schtasks.exe /Create /TN "Updates\BZTCUCKTKd" /XM...            99  21  21
      1676 conhost.exe 0xffffffff -ForceV1                               69  12  25
    5588 59ca67046d065f0fd86ed3ccc7b41aa3168e5557523644f...             1k  300  53
      4068 Native_New-Nova.exe PE  snakekeylogger                       998  952  94
      5360 Native_snake01.exe PE                                         2k  1k  107
5968 COM SppExtComObj.Exe -Embedding                                     69  30  34
  4944 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;A...
```



https://app.any.run/tasks/e76c717c-ac95-46b4-b2c0-c1159ee1d5a6

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Malicious activity

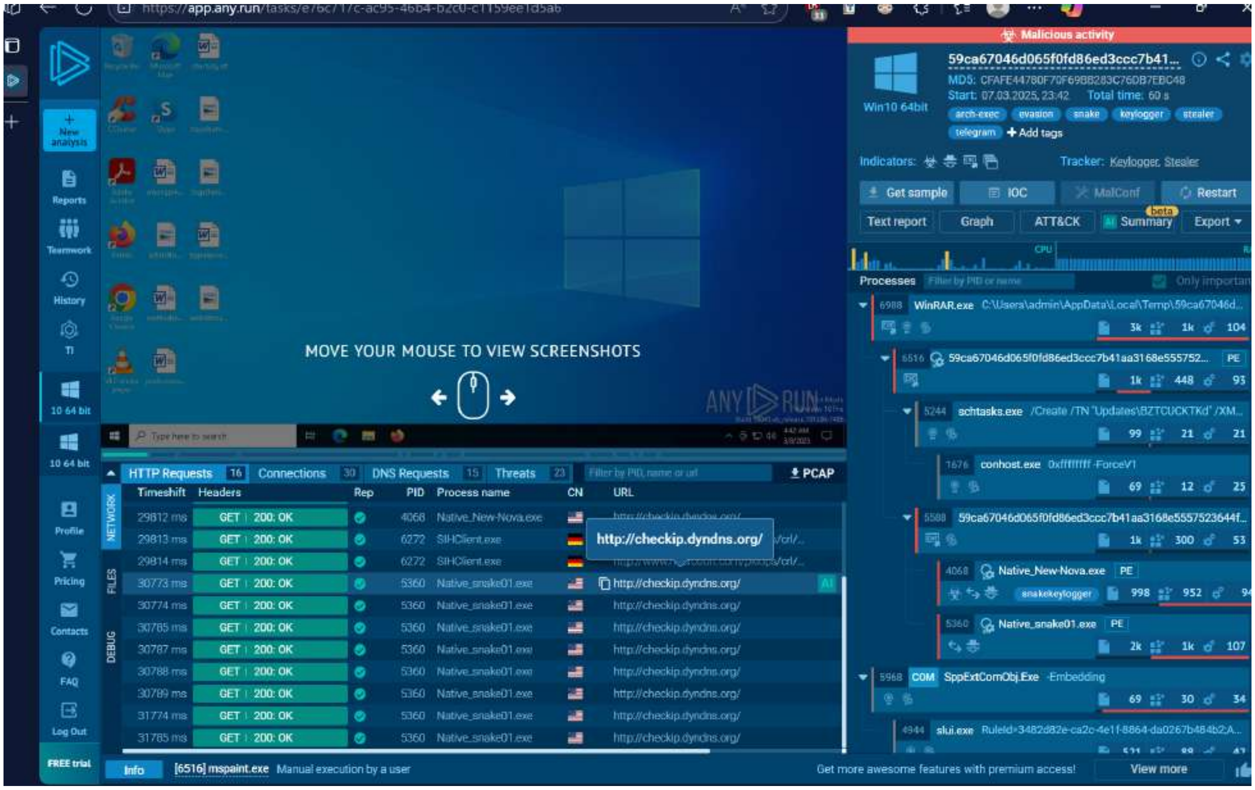
59ca67046d065f0fd86ed3ccc7b41...
MD5: CFAFE44780F70F69B8283C76DB7EBC48
Start: 07.03.2025, 23:42 Total time: 60 s
Win10 64bit
arch-exec evasion snake keylogger stealer telegram + Add tags
Indicators:
Tracker: Keylogger, Stealer

HTTP Requests 16 | Connections 30 | DNS Requests 15 | Threats 23
Filter by PID, domain, name or ip

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
7261 ms	TCP	✓	2152	backgroundTaskHost...		184.30.131.245	80	ocsp.digicert...	AKAMAI-AS
29793 ms	TCP	✓	6272	SIHClient.exe		52.149.20.212	443	slscr.update...	MICROSOFT-CO
29799 ms	TCP	✓	5360	Native_snake01.exe		193.122.130.0	80	checkip.dynd...	ORACLE-BMC-3
29803 ms	TCP	✓	4068	Native_New-Nova.exe		193.122.130.0	80	checkip.dynd...	ORACLE-BMC-3
29810 ms	TCP	✓	6272	SIHClient.exe		2.23.181.156	80	www.micros...	AKAMAI-AS
29822 ms	TCP	🔥	4068	Native_New-Nova.exe	?	104.21.80.1	443	reallyfreegeoi...	CLOUDFLARENE
29832 ms	TCP	🔥	5360	Native_snake01.exe	?	104.21.80.1	443	reallyfreegeoi...	CLOUDFLARENE
30785 ms	TCP	✓	6272	SIHClient.exe		52.165.164.15	443	fe3cr.delivery...	MICROSOFT-CO
31784 ms	TCP	✓	6272	SIHClient.exe		52.149.20.212	443	slscr.update...	MICROSOFT-CO
31790 ms	TCP	✓	5360	Native_snake01.exe		149.154.167.220	443	api.telegram...	Telegram Messe
32774 ms	TCP	✓	6272	SIHClient.exe		52.149.20.212	443	slscr.update...	MICROSOFT-CO

Processes Filter by PID or name Only important

```
6988 WinRAR.exe C:\Users\admin\AppData\Local\Temp\59ca67046d...      3k  1k  104
  6516 59ca67046d065f0fd86ed3ccc7b41aa3168e555752... PE             1k  448  93
    5244 schtasks.exe /Create /TN "Updates\BZTCUCKTKd" /XM...       99  21  21
      1676 conhost.exe 0xffffffff -ForceV1                          69  12  25
    5588 59ca67046d065f0fd86ed3ccc7b41aa3168e5557523644f...         1k  300  53
      4068 Native_New-Nova.exe PE  snakekeylogger                   998  952
      5360 Native_snake01.exe PE                                    2k  1k  107
5968 COM SppExtComObj.Exe -Embedding                                69  30  34
  4944 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;A...
```



https://app.any.run/tasks/e76c717c-ac95-46b4-b2c0-c1159ee1d5a6

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Malicious activity

59ca67046d065f0fd86ed3ccc7b41...
MD5: CFAFE44780F70F69B8283C76DB7EBC48
Start: 07.03.2025, 23:42 Total time: 60 s
Win10 64bit
arch-exec evasion snake keylogger stealer telegram + Add tags
Indicators:
Tracker: Keylogger, Stealer

HTTP Requests 16 | Connections 30 | DNS Requests 15 | Threats 23
Filter by PID, name or url

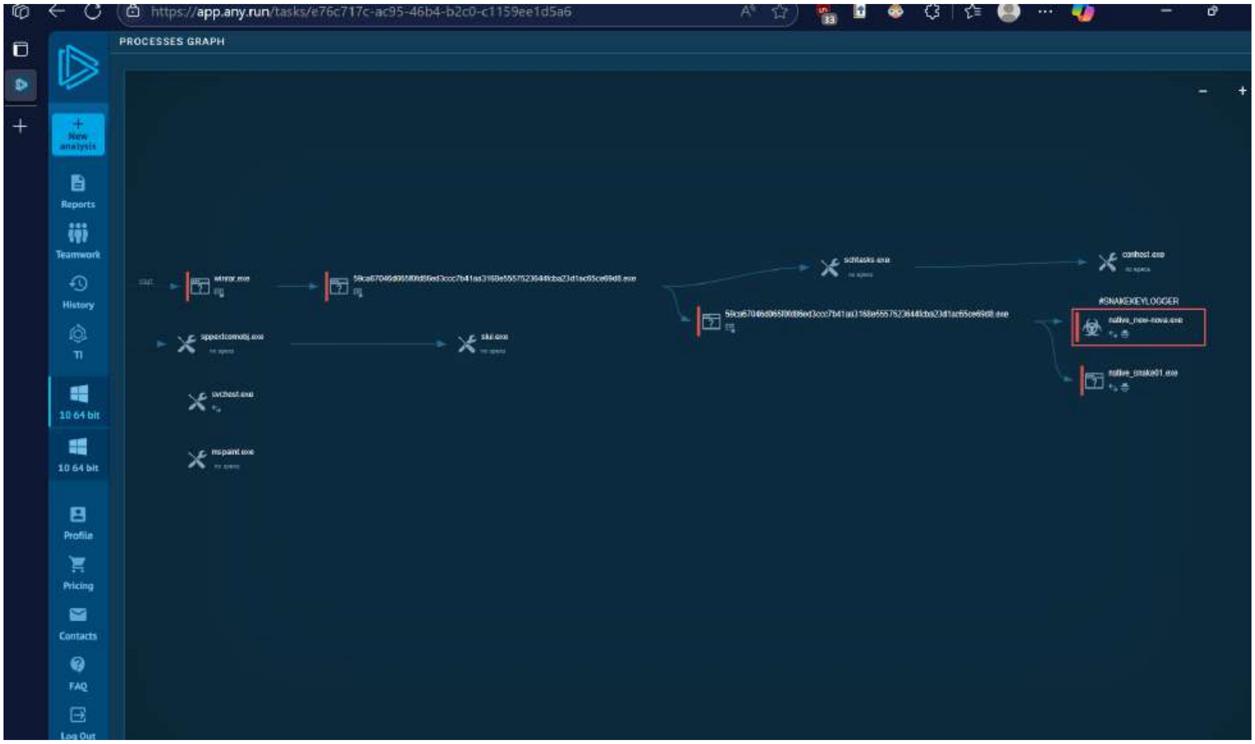
Timeshift	Headers	Rep	PID	Process name	CN	URL
29812 ms	GET 200: OK	✓	4068	Native_New-Nova.exe		http://checkip.dyndns.org/
29813 ms	GET 200: OK	✓	6272	SIHClient.exe		.../crl/...
29814 ms	GET 200: OK	✓	6272	SIHClient.exe		http://www.[illegible]/pkiops/crl/...
30773 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
30774 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
30785 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
30787 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
30788 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
30789 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
31774 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/
31785 ms	GET 200: OK	✓	5360	Native_snake01.exe		http://checkip.dyndns.org/

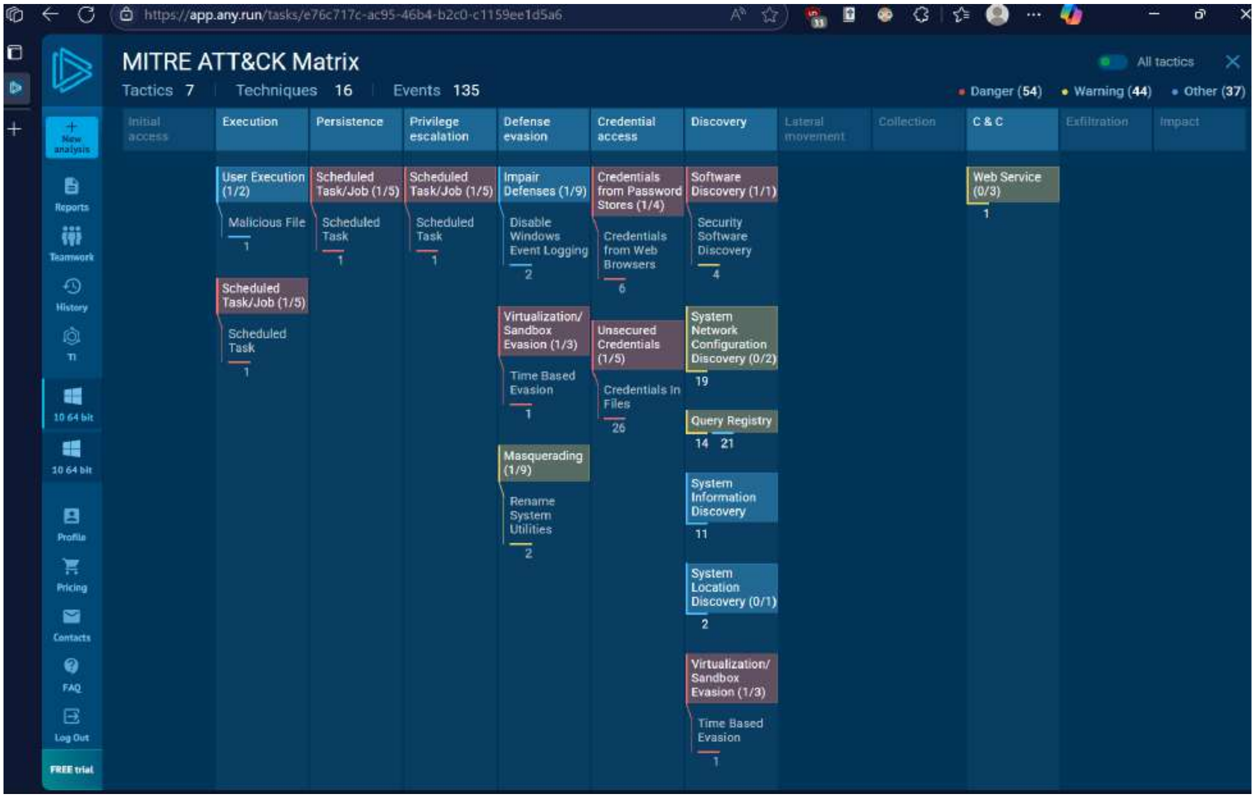
http://checkip.dyndns.org/

Info [6516] mspaint.exe Manual execution by a user

Get more awesome features with premium access! View more

```
6988 WinRAR.exe C:\Users\admin\AppData\Local\Temp\59ca67046d...      3k  1k  104
  6516 59ca67046d065f0fd86ed3ccc7b41aa3168e555752... PE             1k  448  93
    5244 schtasks.exe /Create /TN "Updates\BZTCUCKTKd" /XM...       99  21  21
      1676 conhost.exe 0xffffffff -ForceV1                          69  12  25
    5588 59ca67046d065f0fd86ed3ccc7b41aa3168e5557523644f...         1k  300  53
      4068 Native_New-Nova.exe PE  snakekeylogger                   998  952
      5360 Native_snake01.exe PE                                    2k  1k  107
5968 COM SppExtComObj.Exe -Embedding                                69  30  34
  4944 slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;A...
```





MITRE ATT&CK Matrix

Tactics 7 | Techniques 16 | Events 135

● Danger (54) ● Warning (44) ● Other (37)

Initial access

Execution
- User Execution (1/2)
  - Malicious File — 1
- Scheduled Task/Job (1/5)
  - Scheduled Task — 1

Persistence
- Scheduled Task/Job (1/5)
  - Scheduled Task — 1

Privilege escalation
- Scheduled Task/Job (1/5)
  - Scheduled Task — 1

Defense evasion
- Impair Defenses (1/9)
  - Disable Windows Event Logging — 2
- Virtualization/Sandbox Evasion (1/3)
  - Time Based Evasion — 1
- Masquerading (1/9)
  - Rename System Utilities — 2

Credential access
- Credentials from Password Stores (1/4)
  - Credentials from Web Browsers — 6
- Unsecured Credentials (1/5)
  - Credentials In Files — 26

Discovery
- Software Discovery (1/1)
  - Security Software Discovery — 4
- System Network Configuration Discovery (0/2) — 19
- Query Registry — 14 21
- System Information Discovery — 11
- System Location Discovery (0/1) — 2
- Virtualization/Sandbox Evasion (1/3)
  - Time Based Evasion — 1

Lateral movement

Collection

C & C
- Web Service (0/3) — 1

Exfiltration

Impact