Task: Malware Analysis

Name: Purva Pawaskar

Intern Id:259

Malware Analysis Report

Malware Tool: W32.HfsAdware.8054

Hash value: 812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c

1.Summary Section

What it means:

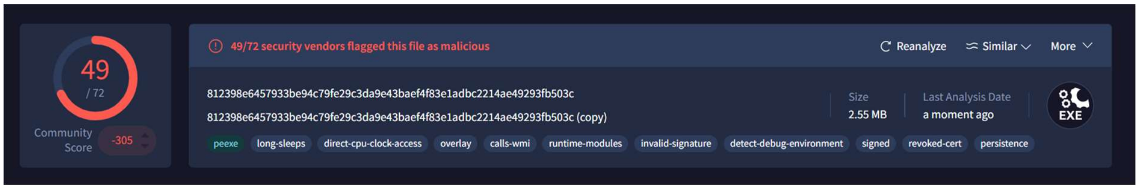
This gives an overview of the file, including risk level, file name, and total number of engines that detected it as malicious.

Summary

The submitted file was analyzed using VirusTotal. Based on the analysis, it is flagged as malicious by multiple antivirus engines.

- File Size: (2.55 MB)
- First Submission Date: (2015-09-01 14:47:28 UTC)
- Last Analysis Date: (2025-08-03 13:49:56 UTC)

Detection Ratio: (49/72 engines marked it malicious) This clearly indicates the file poses a potential security risk.



49/72 security vendors flagged this file as malicious

812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c (copy)

Size: 2.55 MB

Last Analysis Date: a moment ago

Community Score: -305

2. Detection Section

What it means:

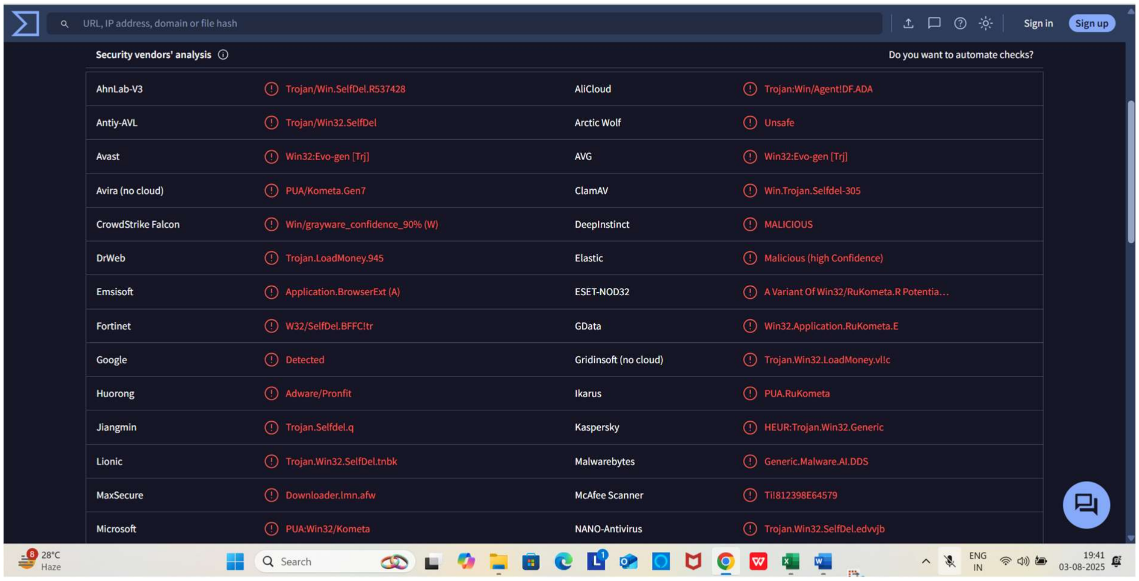
Shows how many antivirus engines marked this file as a trojan, Selfdel-305, or other threats, along with their naming.

Detection

This section contains detailed results from various antivirus engines. Many engines such as DrWeb, GData, MaxSecure, and others have flagged the file as:

- Trojan.Selfdel-305
- LoadMoney.945
- Application.RuKometa.E
- Downloader.lmn.afw

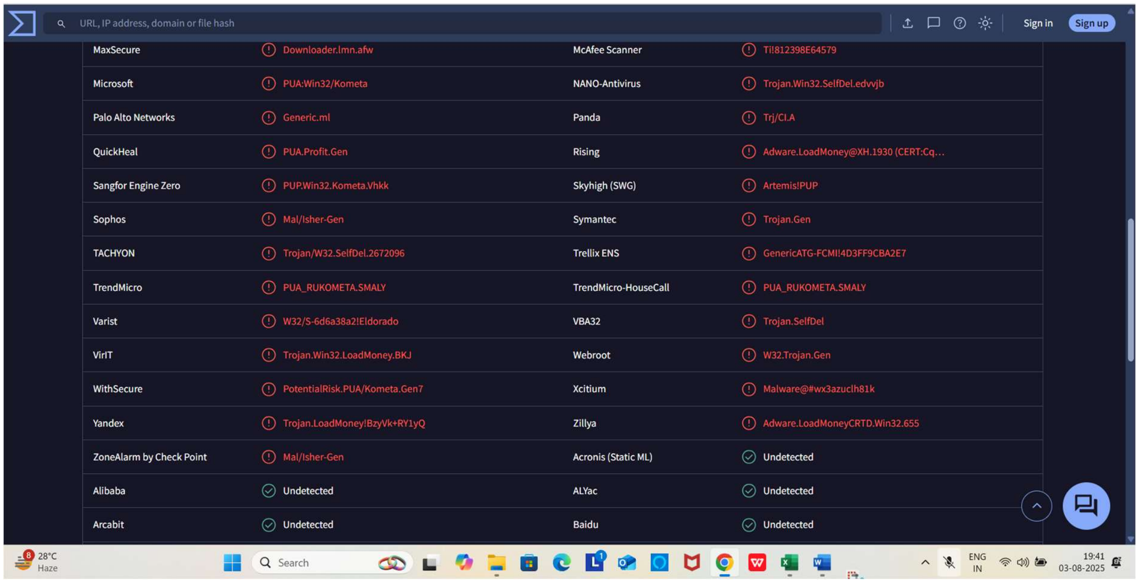
These classifications point toward malware behaviour including data theft, unauthorized system access, and ransomware delivery.



Security vendors' analysis ⓘ

Do you want to automate checks?

AhnLab-V3	! Trojan/Win.SelfDel.R537428	AliCloud	! Trojan:Win/Agent!DF.ADA
Antiy-AVL	! Trojan/Win32.SelfDel	Arctic Wolf	! Unsafe
Avast	! Win32:Evo-gen [Trj]	AVG	! Win32:Evo-gen [Trj]
Avira (no cloud)	! PUA/Kometa.Gen7	ClamAV	! Win.Trojan.Selfdel-305
CrowdStrike Falcon	! Win/grayware_confidence_90% (W)	DeepInstinct	! MALICIOUS
DrWeb	! Trojan.LoadMoney.945	Elastic	! Malicious (high Confidence)
Emsisoft	! Application.BrowserExt (A)	ESET-NOD32	! A Variant Of Win32/RuKometa.R Potentia...
Fortinet	! W32/SelfDel.BFFC!tr	GData	! Win32.Application.RuKometa.E
Google	! Detected	Gridinsoft (no cloud)	! Trojan.Win32.LoadMoney.vl!c
Huorong	! Adware/Pronfit	Ikarus	! PUA.RuKometa
Jiangmin	! Trojan.Selfdel.q	Kaspersky	! HEUR:Trojan.Win32.Generic
Lionic	! Trojan.Win32.SelfDel.tnbk	Malwarebytes	! Generic.Malware.AI.DDS
MaxSecure	! Downloader.lmn.afw	McAfee Scanner	! Ti!812398E64579
Microsoft	! PUA:Win32/Kometa	NANO-Antivirus	! Trojan.Win32.SelfDel.edvvjb



MaxSecure	! Downloader.lmn.afw	McAfee Scanner	! Ti!812398E64579
Microsoft	! PUA:Win32/Kometa	NANO-Antivirus	! Trojan.Win32.SelfDel.edvvjb
Palo Alto Networks	! Generic.ml	Panda	! Trj/CI.A
QuickHeal	! PUA.Profit.Gen	Rising	! Adware.LoadMoney@XH.1930 (CERT:Cq...
Sangfor Engine Zero	! PUP.Win32.Kometa.Vhkk	Skyhigh (SWG)	! Artemis!PUP
Sophos	! Mal/Isher-Gen	Symantec	! Trojan.Gen
TACHYON	! Trojan/W32.SelfDel.2672096	Trellix ENS	! GenericATG-FCMI!4D3FF9CBA2E7
TrendMicro	! PUA_RUKOMETA.SMALY	TrendMicro-HouseCall	! PUA_RUKOMETA.SMALY
Varist	! W32/S-6d6a38a2!Eldorado	VBA32	! Trojan.SelfDel
VirIT	! Trojan.Win32.LoadMoney.BKJ	Webroot	! W32.Trojan.Gen
WithSecure	! PotentialRisk.PUA/Kometa.Gen7	Xcitium	! Malware@#wx3azuclh81k
Yandex	! Trojan.LoadMoney!BzyVk+RY1yQ	Zillya	! Adware.LoadMoneyCRTD.Win32.655
ZoneAlarm by Check Point	! Mal/Isher-Gen	Acronis (Static ML)	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Arcabit	✓ Undetected	Baidu	✓ Undetected

3. Details Section

What it means:

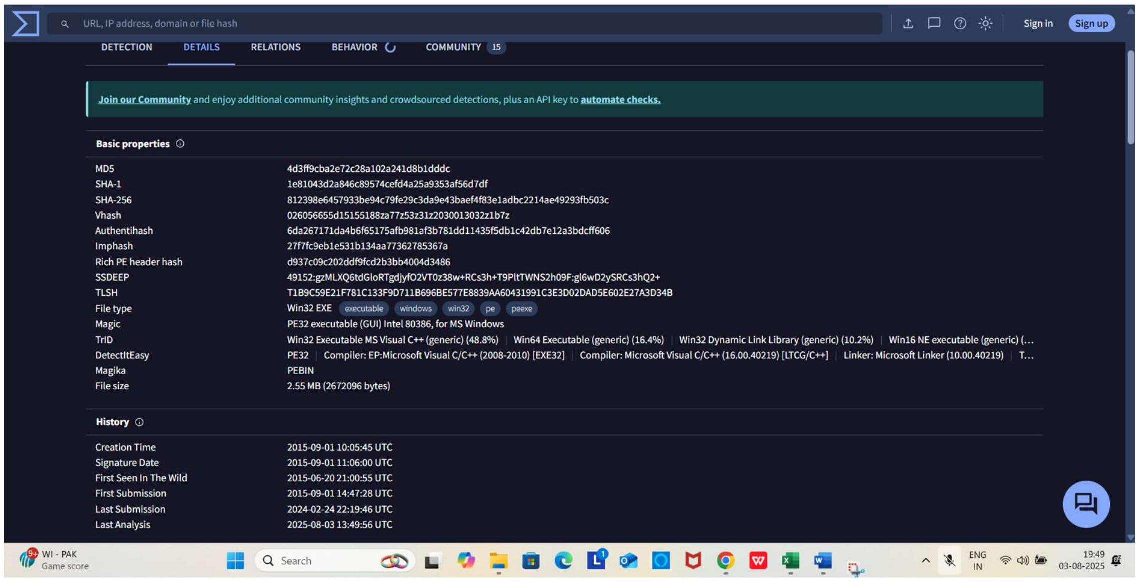
Gives file details like hash values, file size, and creation timestamps.

Details

This section provides metadata of the file:

- SHA-256 Hash: Unique identifier of the file
- File Size: (e.g., 120 KB)
- File Type: (e.g., Windows PE Executable)
- Compilation Timestamp: Shows when the file was compiled, helpful to identify fake timestamps.

Hashes help in identifying and matching the file across databases and threat intel platforms



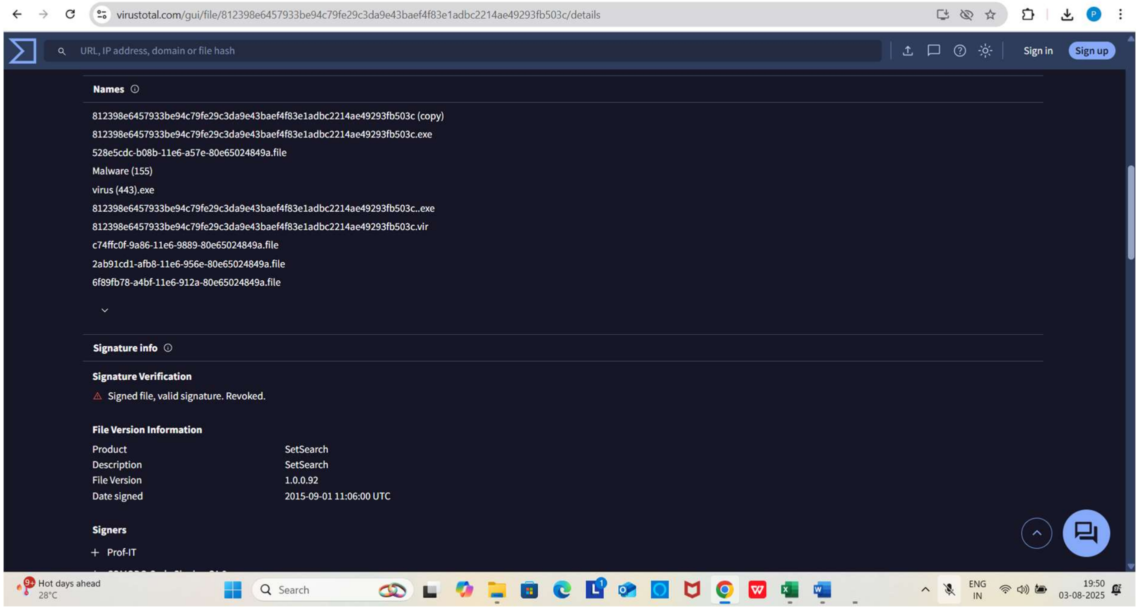
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	4d3ff9cba2e72c28a102a241d8b1dddc
SHA-1	1e81043d2a846c89574cefd4a25a9353af56d7df
SHA-256	812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
Vhash	026056655d15155188za77z53z31z2030013032z1b7z
Authentihash	6da267171da4b6f65175afb981af3b781dd11435f5db1c42db7e12a3bdcff606
Imphash	27f7fc9eb1e531b134aa77362785367a
Rich PE header hash	d937c09c202ddf9fcd2b3bb4004d3486
SSDEEP	49152:gzMLXQ6tdGloRTgdjyfO2VT0z38w+RCs3h+T9PltTWNS2h09F:gl6wD2ySRCs3hQ2+
TLSH	T1B9C59E21F781C133F9D711B696BE577E8839AA60431991C3E3D02DAD5E602E27A3D34B
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (48.8%) | Win64 Executable (generic) (16.4%) | Win32 Dynamic Link Library (generic) (10.2%) | Win16 NE executable (generic) (...
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (16.00.40219) [LTCG/C++] | Linker: Microsoft Linker (10.00.40219) | T...
Magika	PEBIN
File size	2.55 MB (2672096 bytes)

History

Creation Time	2015-09-01 10:05:45 UTC
Signature Date	2015-09-01 11:06:00 UTC
First Seen In The Wild	2015-06-20 21:00:55 UTC
First Submission	2015-09-01 14:47:28 UTC
Last Submission	2024-02-24 22:19:46 UTC
Last Analysis	2025-08-03 13:49:56 UTC



virustotal.com/gui/file/812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c/details

Names

812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c (copy)
812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c.exe
528e5cdc-b08b-11e6-a57e-80e65024849a.file
Malware (155)
virus (443).exe
812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c..exe
812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c.vir
c74ffc0f-9a86-11e6-9889-80e65024849a.file
2ab91cd1-afb8-11e6-956e-80e65024849a.file
6f89fb78-a4bf-11e6-912a-80e65024849a.file

Signature info

Signature Verification

⚠ Signed file, valid signature. Revoked.

File Version Information

Product	SetSearch
Description	SetSearch
File Version	1.0.0.92
Date signed	2015-09-01 11:06:00 UTC

Signers

+ Prof-IT

4.Relations Section

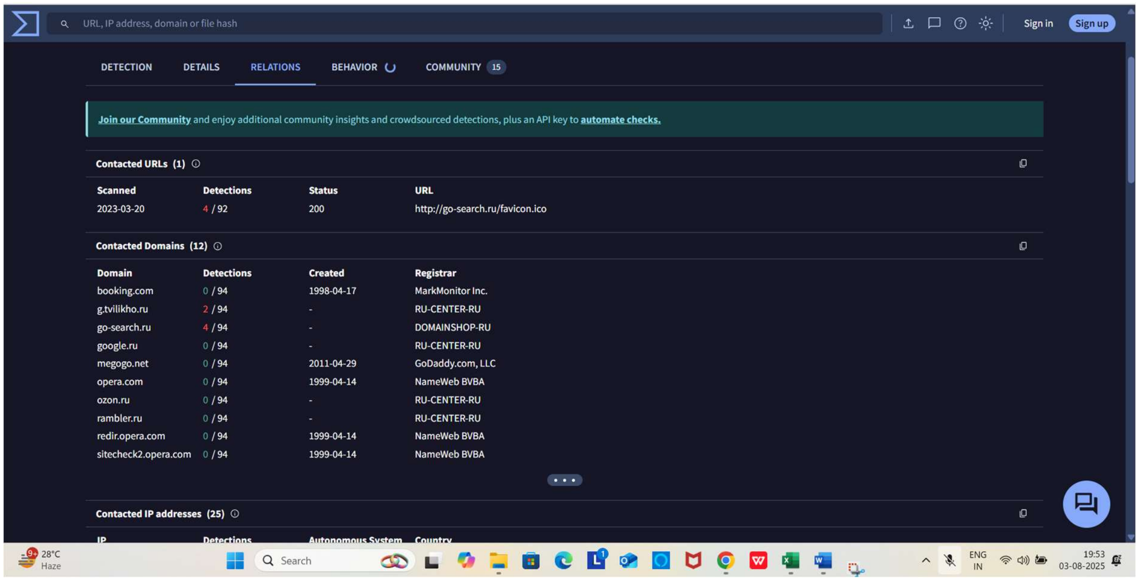
What it means:

This shows other files, domains, or URLs related to this file, often used to spread or communicate with malicious servers.

Relations

VirusTotal shows this file has connections with multiple URLs and IPs, possibly used for C2 (Command and Control) communication or spreading other malware.

The relations indicate this file is part of a larger malware infrastructure.



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted URLs (1)

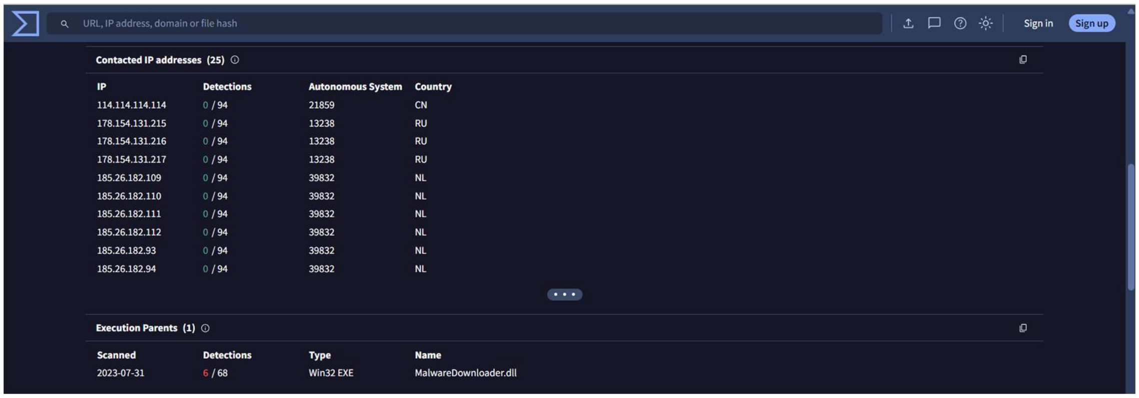
Scanned	Detections	Status	URL
2023-03-20	4 / 92	200	http://go-search.ru/favicon.ico

Contacted Domains (12)

Domain	Detections	Created	Registrar
booking.com	0 / 94	1998-04-17	MarkMonitor Inc.
g.tvilikho.ru	2 / 94	-	RU-CENTER-RU
go-search.ru	4 / 94	-	DOMAINSHOP-RU
google.ru	0 / 94	-	RU-CENTER-RU
megogo.net	0 / 94	2011-04-29	GoDaddy.com, LLC
opera.com	0 / 94	1999-04-14	NameWeb BVBA
ozon.ru	0 / 94	-	RU-CENTER-RU
rambler.ru	0 / 94	-	RU-CENTER-RU
redir.opera.com	0 / 94	1999-04-14	NameWeb BVBA
sitecheck2.opera.com	0 / 94	1999-04-14	NameWeb BVBA

Contacted IP addresses (25)

IP	Detections	Autonomous System	Country

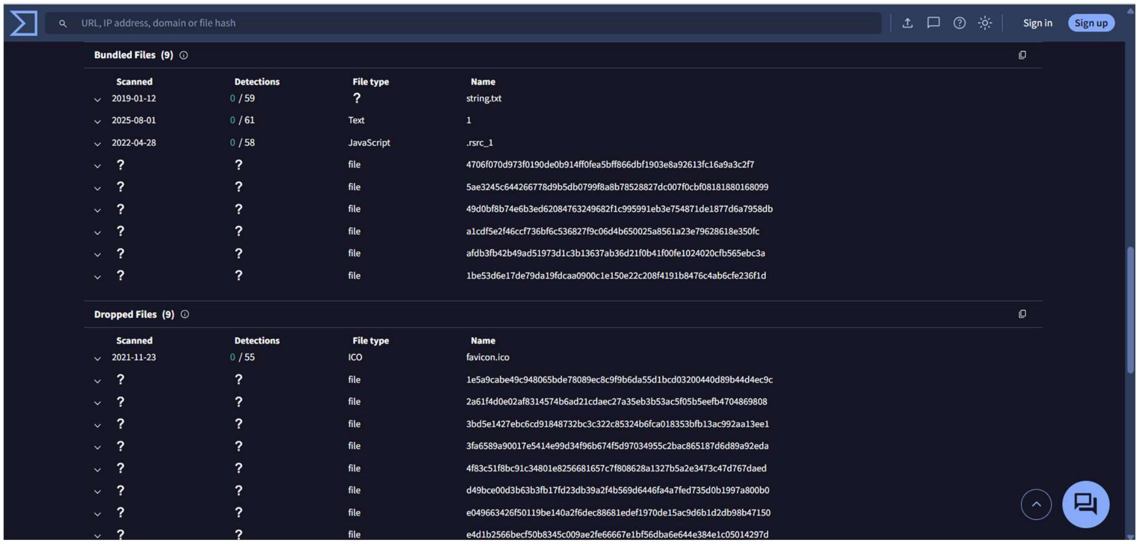


Contacted IP addresses (25)

IP	Detections	Autonomous System	Country
114.114.114.114	0 / 94	21859	CN
178.154.131.215	0 / 94	13238	RU
178.154.131.216	0 / 94	13238	RU
178.154.131.217	0 / 94	13238	RU
185.26.182.109	0 / 94	39832	NL
185.26.182.110	0 / 94	39832	NL
185.26.182.111	0 / 94	39832	NL
185.26.182.112	0 / 94	39832	NL
185.26.182.93	0 / 94	39832	NL
185.26.182.94	0 / 94	39832	NL

Execution Parents (1)

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll

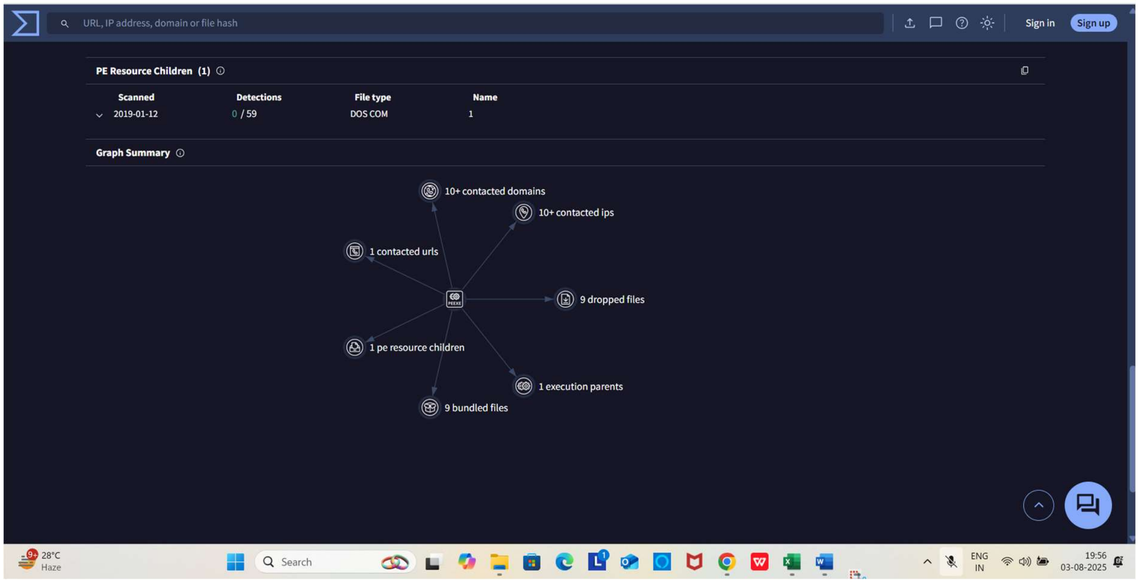


Bundled Files (9)

Scanned	Detections	File type	Name
2019-01-12	0 / 59	?	string.txt
2025-08-01	0 / 61	Text	1
2022-04-28	0 / 58	JavaScript	.rsrc_1
?	?	file	4706f070d973f0190de0b914ff0fea5bff866dbf1903e8a92613fc16a9a3c2f7
?	?	file	5ae3245c644266778d9b5db0799f8a8b78528827dc007f0cbf08181880168099
?	?	file	49d0bf8b74e6b3ed62084763249682f1c995991eb3e754871de1877d6a7958db
?	?	file	a1cdf5e2f46ccf736bf6c536827f9c06d4b650025a8561a23e79628618e350fc
?	?	file	afdb3fb42b49ad51973d1c3b13637ab36d21f0b41f00fe1024020cfb565ebc3a
?	?	file	1be53d6e17de79da19fdcaa0900c1e150e22c208f4191b8476c4ab6cfe236f1d

Dropped Files (9)

Scanned	Detections	File type	Name
2021-11-23	0 / 55	ICO	favicon.ico
?	?	file	1e5a9cabe49c948065bde78089ec8c9f9b6da55d1bcd03200440d89b44d4ec9c
?	?	file	2a61f4d0e02af8314574b6ad21cdaec27a35eb3b53ac5f05b5eefb4704869808
?	?	file	3bd5e1427ebc6cd91848732bc3c322c85324b6fca018353bfb13ac992aa13ee1
?	?	file	3fa6589a90017e5414e99d34f96b674f5d97034955c2bac865187d6d89a92eda
?	?	file	4f83c51f8bc91c34801e8256681657c7f808628a1327b5a2e3473c47d767daed
?	?	file	d49bce00d3b63b3fb17fd23db39a2f4b569d6446fa4a7fed735d0b1997a800b0
?	?	file	e049663426f50119be140a2f6dec88681edef1970de15ac9d6b1d2db98b47150
?	?	file	e4d1b2566becf50b8345c009ae2fe66667e1bf56dba6e644e384e1c05014297d



PE Resource Children (1)

Scanned	Detections	File type	Name
2019-01-12	0 / 59	DOS COM	1

Graph Summary

5.Behavior Section

What it means:

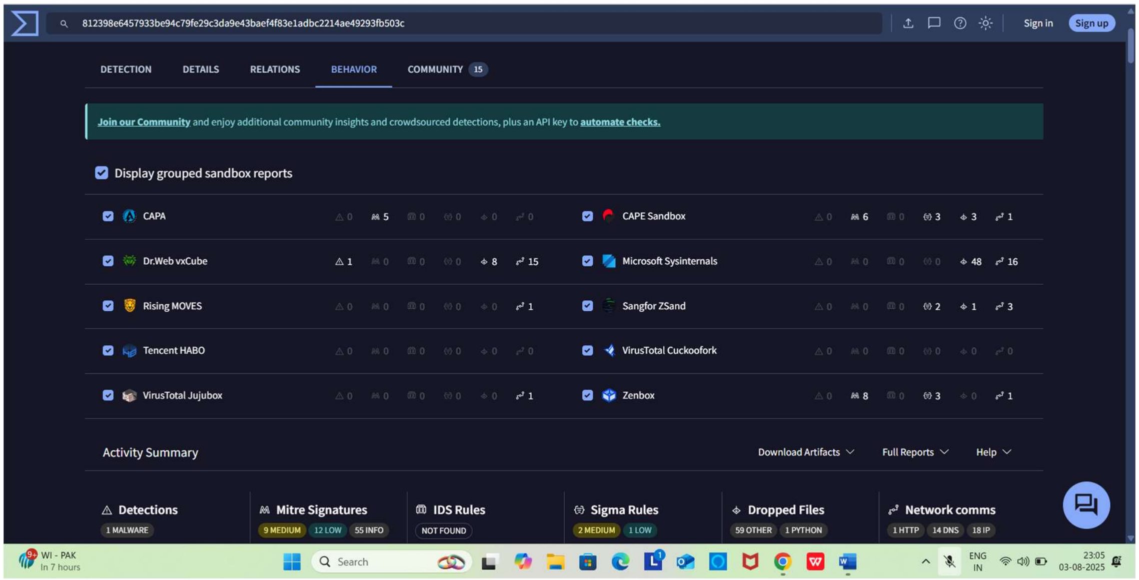
Simulated sandbox environments (like Windows) show what the file does when executed, such as modifying registry, connecting to internet, or downloading files.

Behaviour

Based on dynamic analysis, the file performs several suspicious activities:

- Attempts to connect to external IPs
- Modifies system settings or registry
- Executes multiple processes

These behaviours are typical of malware like ransomware or infostealers.



812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
Sign in
Sign up
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 15

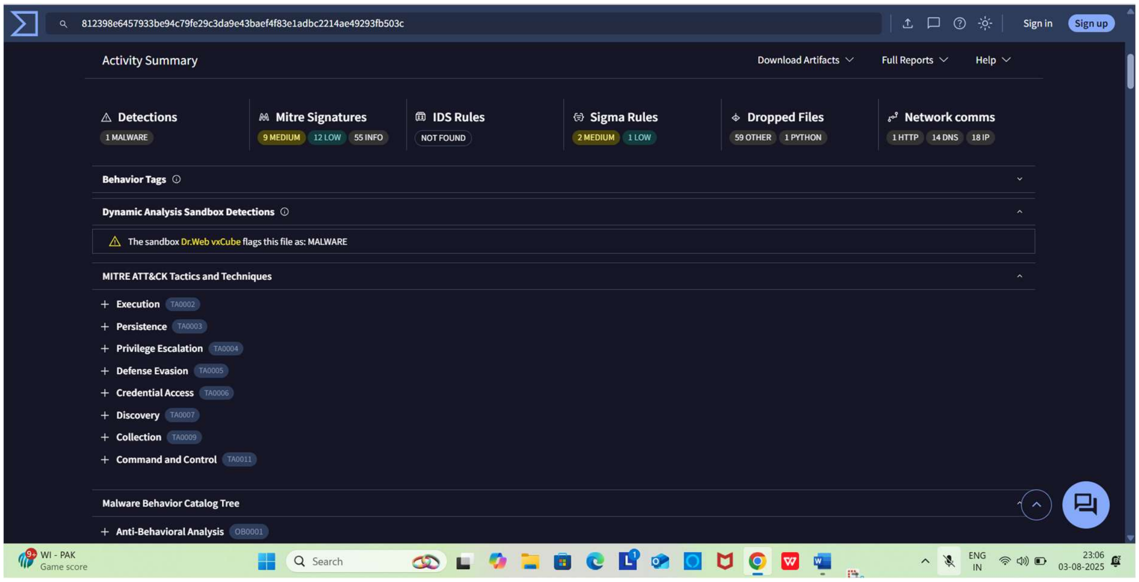
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

☑ Display grouped sandbox reports

☑ CAPA	△ 0	5	0	0	0	0
☑ Dr.Web vxCube	△ 1	0	0	0	8	15
☑ Rising MOVES	△ 0	0	0	0	0	1
☑ Tencent HABO	△ 0	0	0	0	0	0
☑ VirusTotal Jujubox	△ 0	0	0	0	0	1
☑ CAPE Sandbox	△ 0	6	0	3	3	1
☑ Microsoft Sysinternals	△ 0	0	0	0	48	16
☑ Sangfor ZSand	△ 0	0	0	2	1	3
☑ VirusTotal Cuckoofork	△ 0	0	0	0	0	0
☑ Zenbox	△ 0	8	0	3	0	1

Activity Summary

Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
1 MALWARE	9 MEDIUM 12 LOW 55 INFO	NOT FOUND	2 MEDIUM 1 LOW	59 OTHER 1 PYTHON	1 HTTP 14 DNS 18 IP



Activity Summary

Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
1 MALWARE	9 MEDIUM 12 LOW 55 INFO	NOT FOUND	2 MEDIUM 1 LOW	59 OTHER 1 PYTHON	1 HTTP 14 DNS 18 IP

Behavior Tags ⓘ

Dynamic Analysis Sandbox Detections ⓘ

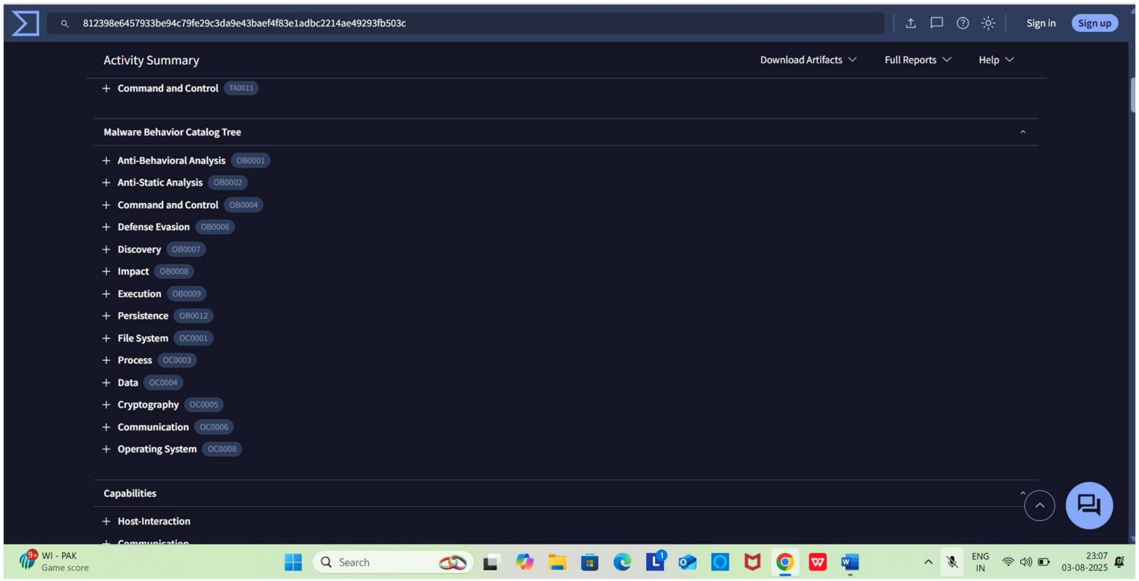
⚠ The sandbox Dr.Web vxCube flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- + Collection TA0009
- + Command and Control TA0011

Malware Behavior Catalog Tree

- + Anti-Behavioral Analysis OB0001



Activity Summary

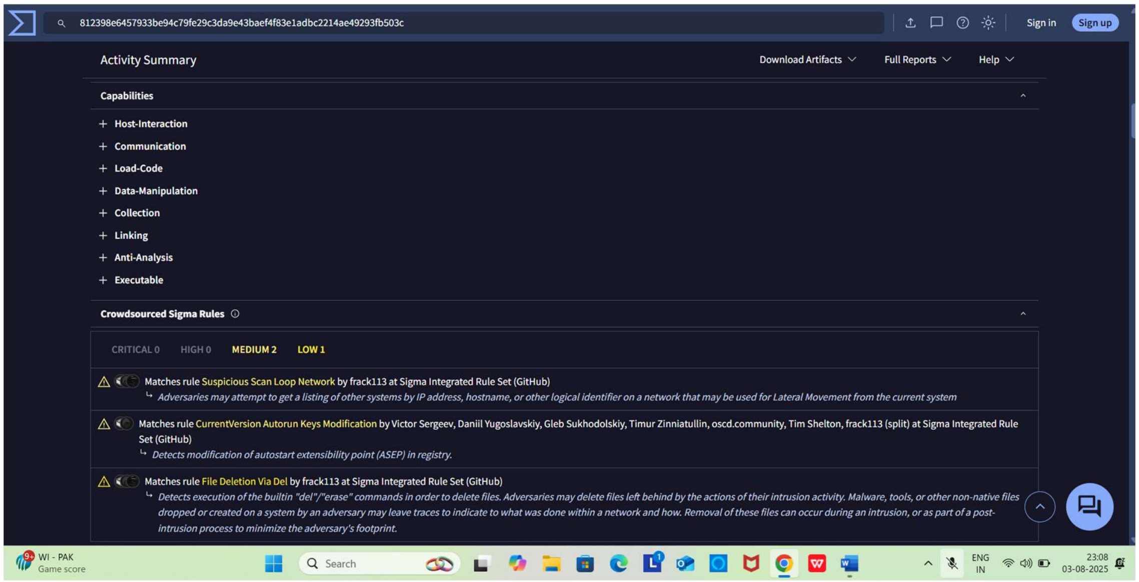
- + Command and Control TA0011

Malware Behavior Catalog Tree

- + Anti-Behavioral Analysis OB0001
- + Anti-Static Analysis OB0002
- + Command and Control OB0004
- + Defense Evasion OB0006
- + Discovery OB0007
- + Impact OB0008
- + Execution OB0009
- + Persistence OB0012
- + File System OC0001
- + Process OC0003
- + Data OC0004
- + Cryptography OC0005
- + Communication OC0006
- + Operating System OC0008

Capabilities

- + Host-Interaction
- + Communication



Activity Summary

Capabilities

- + Host-Interaction
- + Communication
- + Load-Code
- + Data-Manipulation
- + Collection
- + Linking
- + Anti-Analysis
- + Executable

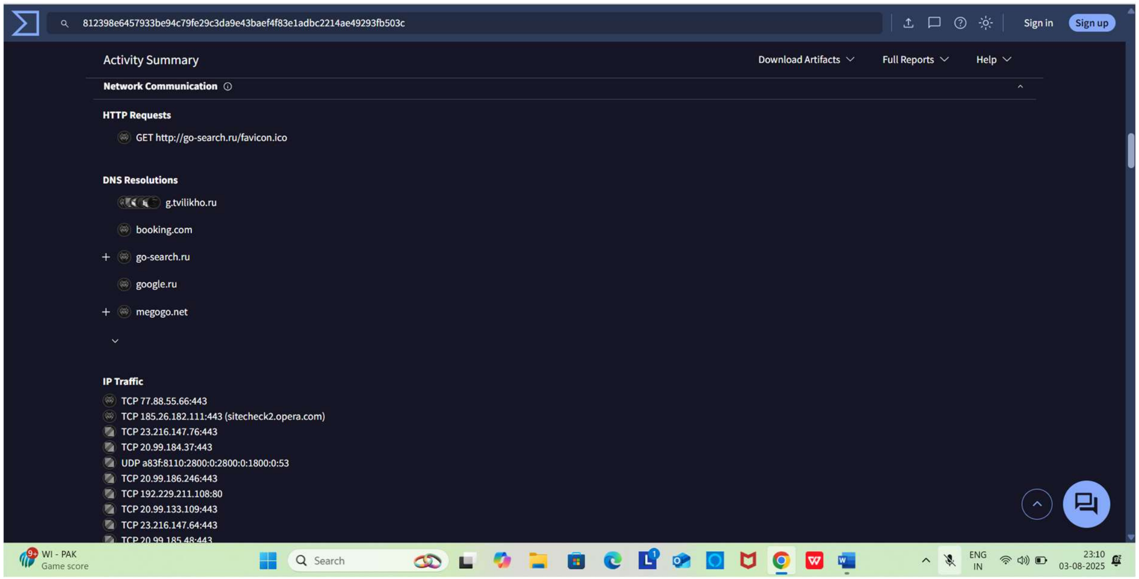
Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 0 MEDIUM 2 LOW 1

⚠ Matches rule Suspicious Scan Loop Network by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system*

⚠ Matches rule CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split) at Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

⚠ Matches rule File Deletion Via Del by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Detects execution of the builtin "del"/"erase" commands in order to delete files. Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.*



Activity Summary

Network Communication

HTTP Requests

GET http://go-search.ru/favicon.ico

DNS Resolutions

g.tvilikho.ru

booking.com

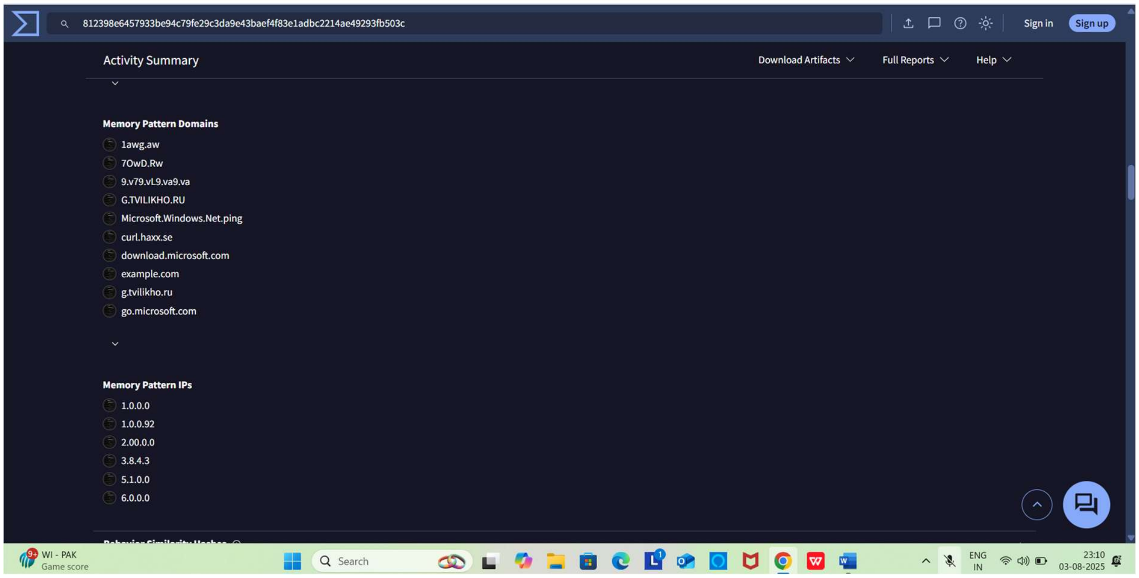
+ go-search.ru

google.ru

+ megogo.net

IP Traffic

```
TCP 77.88.55.66:443
TCP 185.26.182.111:443 (sitecheck2.opera.com)
TCP 23.216.147.76:443
TCP 20.99.184.37:443
UDP a83f:8110:2800:0:2800:0:1800:0:53
TCP 20.99.186.246:443
TCP 192.229.211.108:80
TCP 20.99.133.109:443
TCP 23.216.147.64:443
TCP 20.99.185.48:443
```



Activity Summary

Memory Pattern Domains

1awg.aw

7OwD.Rw

9.v79.vL9.va9.va

G.TVILIKHO.RU

Microsoft.Windows.Net.ping

curl.haxx.se

download.microsoft.com

example.com

g.tvilikho.ru

go.microsoft.com

Memory Pattern IPs

1.0.0.0

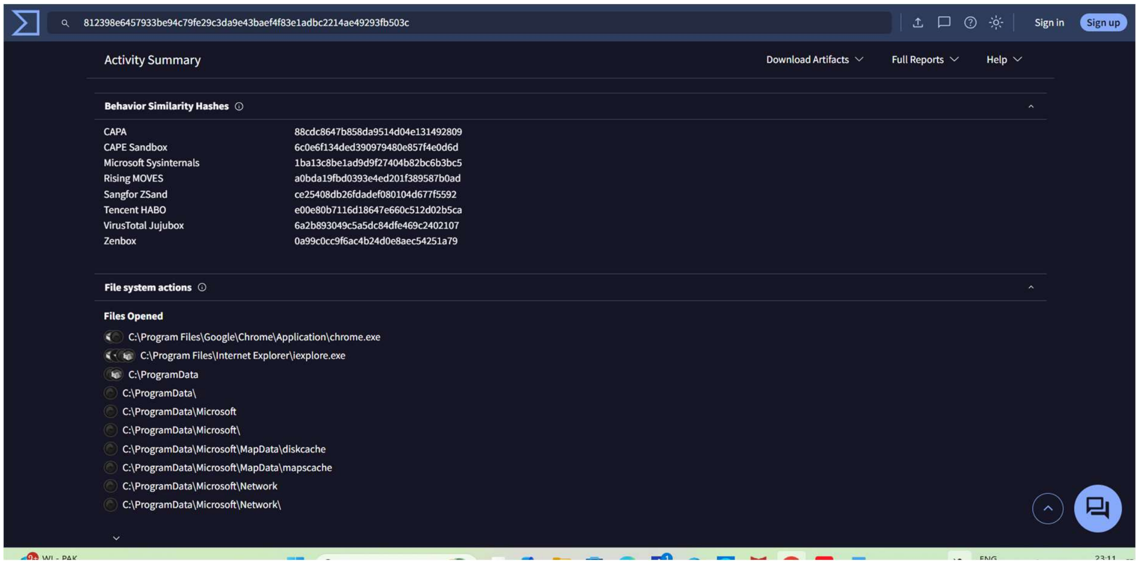
1.0.0.92

2.00.0.0

3.8.4.3

5.1.0.0

6.0.0.0


812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
Sign in
Sign up
Download Artifacts
Full Reports
Help

Activity Summary

Behavior Similarity Hashes

CAPA	88cdc8647b858da9514d04e131492809
CAPE Sandbox	6c0e6f134ded390979480e857f4e0d6d
Microsoft Sysinternals	1ba13c8be1ad9d9f27404b82bc6b3bc5
Rising MOVES	a0bda19fbd0393e4ed201f389587b0ad
Sangfor ZSand	ce25408db26fdadef080104d677f5592
Tencent HABO	e00e80b7116d18647e660c512d02b5ca
VirusTotal Jujubox	6a2b893049c5a5dc84dfe469c2402107
Zenbox	0a99c0cc9f6ac4b24d0e8aec54251a79

File system actions

Files Opened

C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Program Files\Internet Explorer\iexplore.exe

C:\ProgramData

C:\ProgramData\

C:\ProgramData\Microsoft

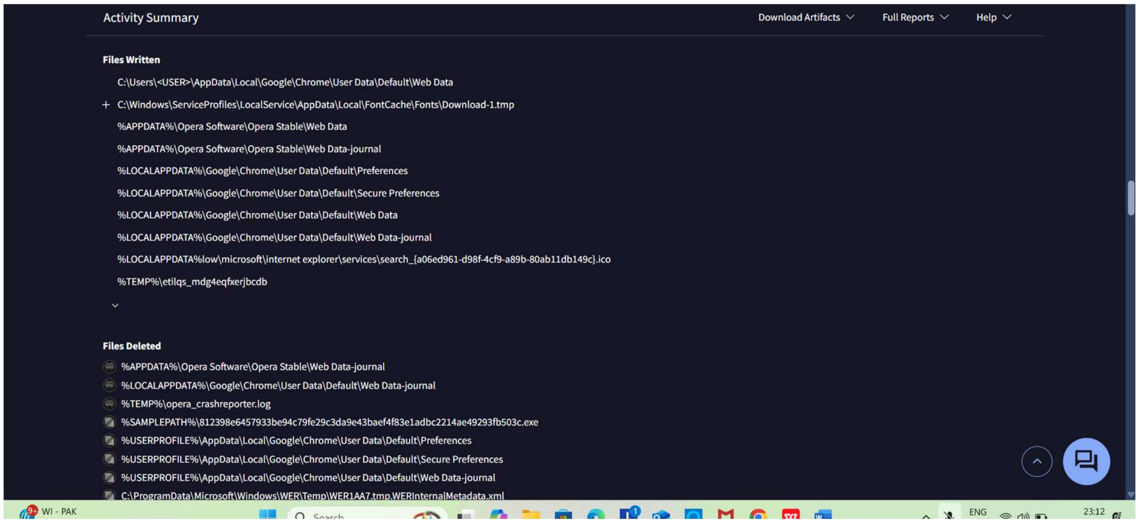
C:\ProgramData\Microsoft\

C:\ProgramData\Microsoft\MapData\diskcache

C:\ProgramData\Microsoft\MapData\mapscache

C:\ProgramData\Microsoft\Network

C:\ProgramData\Microsoft\Network\



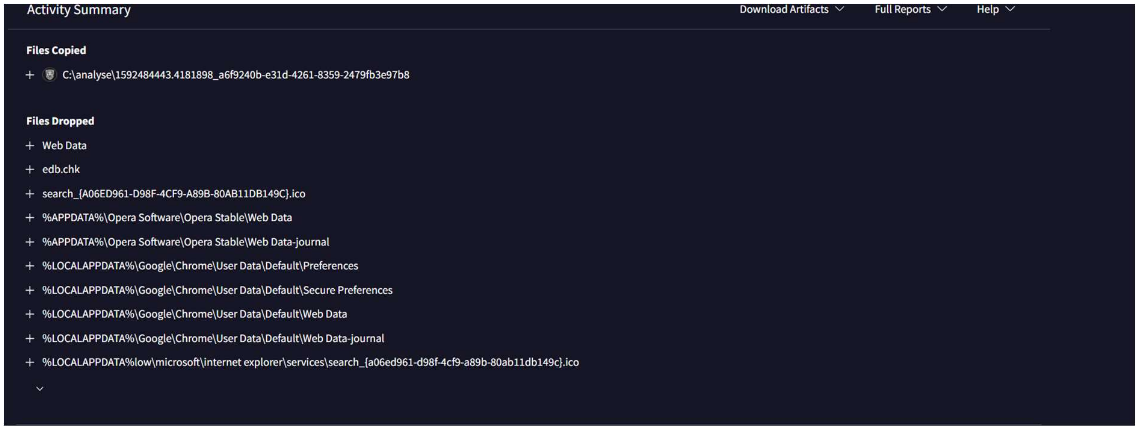
Activity Summary

Files Written

- C:\Users\<USER>\AppData\Local\Google\Chrome\User Data\Default\Web Data
- C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp
- %APPDATA%\Opera Software\Opera Stable\Web Data
- %APPDATA%\Opera Software\Opera Stable\Web Data-journal
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Secure Preferences
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data-journal
- %LOCALAPPDATA%low\microsoft\internet explorer\services\search_{a06ed961-d98f-4cf9-a89b-80ab11db149c}.ico
- %TEMP%\etilqs_mdg4eqfxerjbcdb

Files Deleted

- %APPDATA%\Opera Software\Opera Stable\Web Data-journal
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data-journal
- %TEMP%\opera_crashreporter.log
- %SAMPLEPATH%\812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c.exe
- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Preferences
- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences
- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1AA7.tmp.WERInternalMetadata.xml



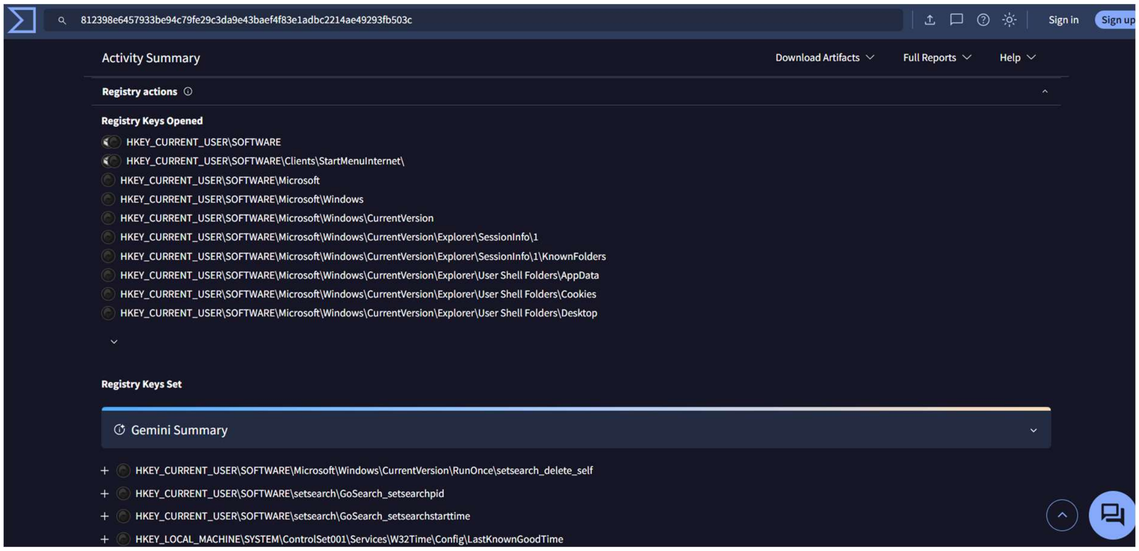
Activity Summary

Files Copied

- C:\analyse\1592484443.4181898_a6f9240b-e31d-4261-8359-2479fb3e97b8

Files Dropped

- Web Data
- edb.chk
- search_{A06ED961-D98F-4CF9-A89B-80AB11DB149C}.ico
- %APPDATA%\Opera Software\Opera Stable\Web Data
- %APPDATA%\Opera Software\Opera Stable\Web Data-journal
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Secure Preferences
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data
- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Web Data-journal
- %LOCALAPPDATA%low\microsoft\internet explorer\services\search_{a06ed961-d98f-4cf9-a89b-80ab11db149c}.ico



812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c

Activity Summary

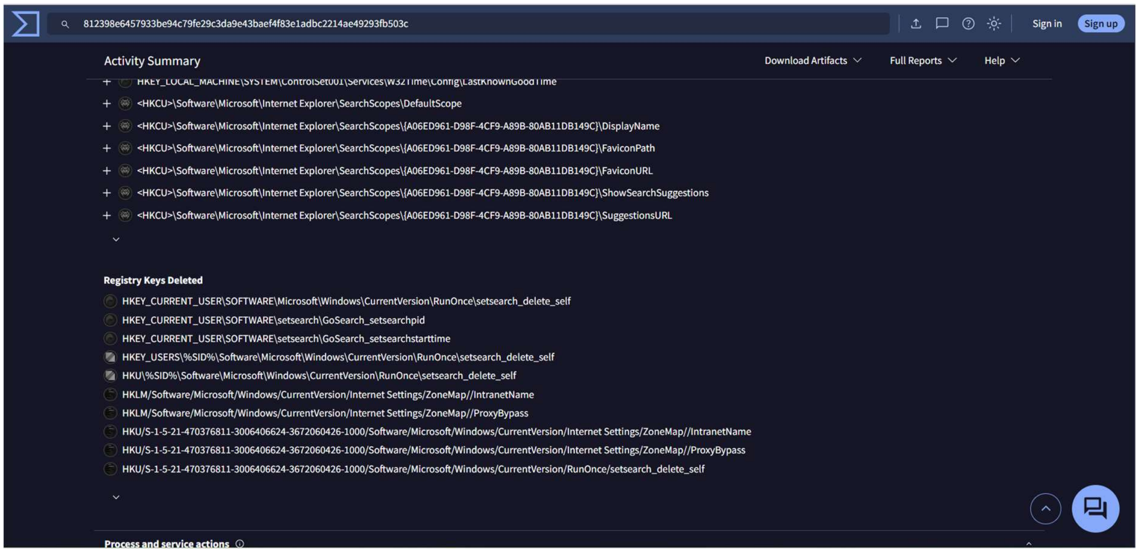
Registry actions

Registry Keys Opened

- HKEY_CURRENT_USER\SOFTWARE
- HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\
- HKEY_CURRENT_USER\SOFTWARE\Microsoft
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Cookies
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop

Registry Keys Set

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\setsearch_delete_self
- HKEY_CURRENT_USER\SOFTWARE\setsearch\GoSearch_setsearchpid
- HKEY_CURRENT_USER\SOFTWARE\setsearch\GoSearch_setsearchstarttime
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\Config\LastKnownGoodTime



812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c

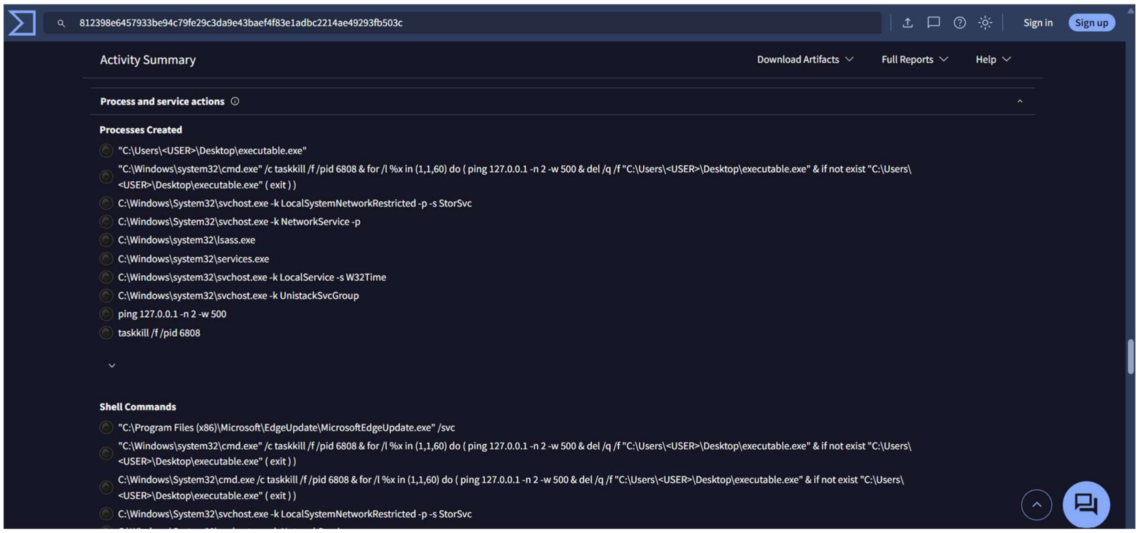
Activity Summary

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\Config\LastKnownGoodTime
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\DefaultScope
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\{A06ED961-D98F-4CF9-A89B-80AB11DB149C}\DisplayName
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\{A06ED961-D98F-4CF9-A89B-80AB11DB149C}\FaviconPath
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\{A06ED961-D98F-4CF9-A89B-80AB11DB149C}\FaviconURL
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\{A06ED961-D98F-4CF9-A89B-80AB11DB149C}\ShowSearchSuggestions
- <HKCU>\Software\Microsoft\Internet Explorer\SearchScopes\{A06ED961-D98F-4CF9-A89B-80AB11DB149C}\SuggestionsURL

Registry Keys Deleted

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\setsearch_delete_self
- HKEY_CURRENT_USER\SOFTWARE\setsearch\GoSearch_setsearchpid
- HKEY_CURRENT_USER\SOFTWARE\setsearch\GoSearch_setsearchstarttime
- HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\RunOnce\setsearch_delete_self
- HKU\%SID%\Software\Microsoft\Windows\CurrentVersion\RunOnce\setsearch_delete_self
- HKLM/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap//IntranetName
- HKLM/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap//ProxyBypass
- HKU/S-1-5-21-470376811-3006406624-3672060426-1000/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap//IntranetName
- HKU/S-1-5-21-470376811-3006406624-3672060426-1000/Software/Microsoft/Windows/CurrentVersion/Internet Settings/ZoneMap//ProxyBypass
- HKU/S-1-5-21-470376811-3006406624-3672060426-1000/Software/Microsoft/Windows/CurrentVersion/RunOnce/setsearch_delete_self

Process and service actions



812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c

Activity Summary

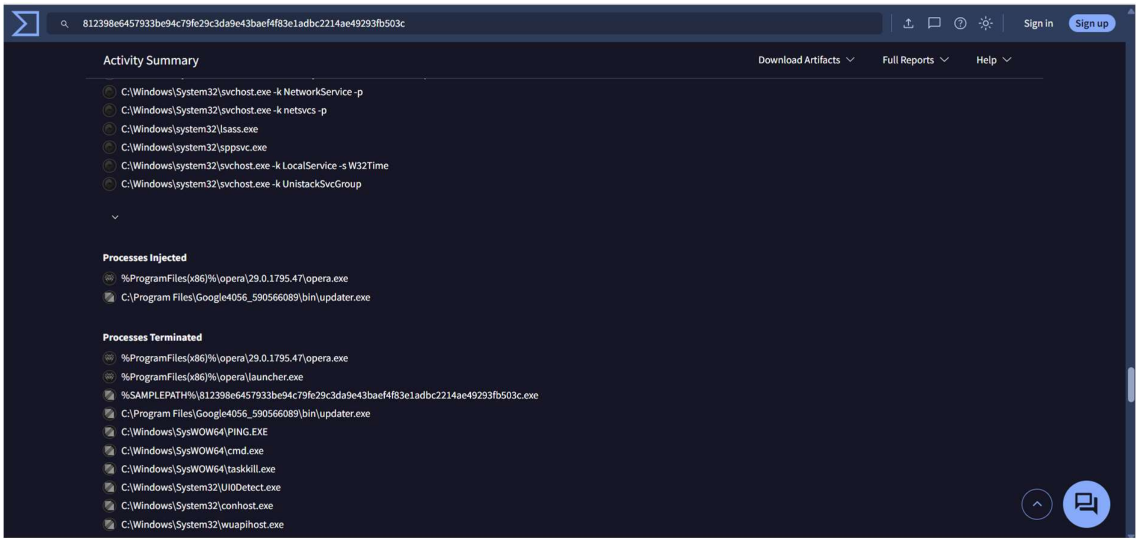
Process and service actions

Processes Created

- "C:\Users\<USER>\Desktop\executable.exe"
- "C:\Windows\system32\cmd.exe" /c taskkill /f /pid 6808 & for /l %x in (1,1,60) do (ping 127.0.0.1 -n 2 -w 500 & del /q /f "C:\Users\<USER>\Desktop\executable.exe" & if not exist "C:\Users\<USER>\Desktop\executable.exe" (exit))
- C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
- C:\Windows\System32\svchost.exe -k NetworkService -p
- C:\Windows\system32\lsass.exe
- C:\Windows\system32\services.exe
- C:\Windows\system32\svchost.exe -k LocalService -s W32Time
- C:\Windows\system32\svchost.exe -k UnistackSvcGroup
- ping 127.0.0.1 -n 2 -w 500
- taskkill /f /pid 6808

Shell Commands

- "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
- "C:\Windows\system32\cmd.exe" /c taskkill /f /pid 6808 & for /l %x in (1,1,60) do (ping 127.0.0.1 -n 2 -w 500 & del /q /f "C:\Users\<USER>\Desktop\executable.exe" & if not exist "C:\Users\<USER>\Desktop\executable.exe" (exit))
- C:\Windows\System32\cmd.exe /c taskkill /f /pid 6808 & for /l %x in (1,1,60) do (ping 127.0.0.1 -n 2 -w 500 & del /q /f "C:\Users\<USER>\Desktop\executable.exe" & if not exist "C:\Users\<USER>\Desktop\executable.exe" (exit))
- C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc



812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c

Activity Summary

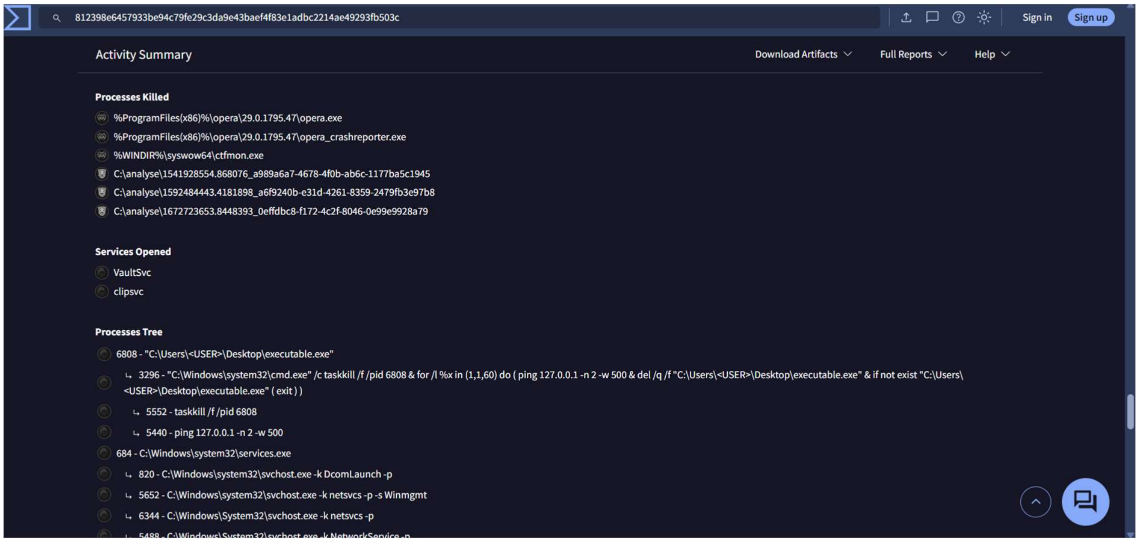
- C:\Windows\System32\svchost.exe -k NetworkService -p
- C:\Windows\System32\svchost.exe -k netsvcs -p
- C:\Windows\system32\lsass.exe
- C:\Windows\system32\sppsvc.exe
- C:\Windows\system32\svchost.exe -k LocalService -s W32Time
- C:\Windows\system32\svchost.exe -k UnistackSvcGroup

Processes Injected

- %ProgramFiles(x86)%\opera\29.0.1795.47\opera.exe
- C:\Program Files\Google4056_590566089\bin\updater.exe

Processes Terminated

- %ProgramFiles(x86)%\opera\29.0.1795.47\opera.exe
- %ProgramFiles(x86)%\opera\launcher.exe
- %SAMPLEPATH%\812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c.exe
- C:\Program Files\Google4056_590566089\bin\updater.exe
- C:\Windows\SysWOW64\PING.EXE
- C:\Windows\SysWOW64\cmd.exe
- C:\Windows\SysWOW64\taskkill.exe
- C:\Windows\System32\UI0Detect.exe
- C:\Windows\System32\conhost.exe
- C:\Windows\System32\wuapihost.exe


812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
Sign in
Sign up
Download Artifacts
Full Reports
Help

Activity Summary

Processes Killed

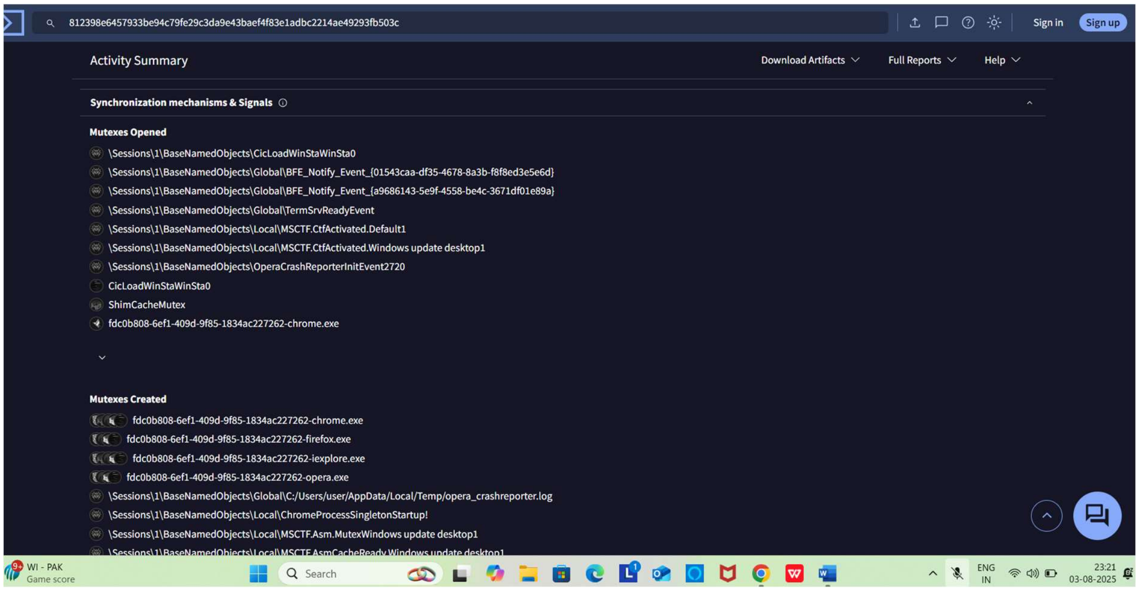
- %ProgramFiles(x86)%\opera\29.0.1795.47\opera.exe
- %ProgramFiles(x86)%\opera\29.0.1795.47\opera_crashreporter.exe
- %WINDIR%\syswow64\ctfmon.exe
- C:\analyse\1541928554.868076_a989a6a7-4678-4f0b-ab6c-1177ba5c1945
- C:\analyse\1592484443.4181898_a6f9240b-e31d-4261-8359-2479fb3e97b8
- C:\analyse\1672723653.8448393_0effdbc8-f172-4c2f-8046-0e99e9928a79

Services Opened

- VaultSvc
- clipsvc

Processes Tree

```
6808 - "C:\Users\<USER>\Desktop\executable.exe"
  ↳ 3296 - "C:\Windows\system32\cmd.exe" /c taskkill /f /pid 6808 & for /l %x in (1,1,60) do ( ping 127.0.0.1 -n 2 -w 500 & del /q /f "C:\Users\<USER>\Desktop\executable.exe" & if not exist "C:\Users\<USER>\Desktop\executable.exe" ( exit ) )
    ↳ 5552 - taskkill /f /pid 6808
    ↳ 5440 - ping 127.0.0.1 -n 2 -w 500
684 - C:\Windows\system32\services.exe
  ↳ 820 - C:\Windows\system32\svchost.exe -k DcomLaunch -p
  ↳ 5652 - C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
  ↳ 6344 - C:\Windows\System32\svchost.exe -k netsvcs -p
  ↳ 5488 - C:\Windows\System32\svchost.exe -k NetworkService -p
```



Activity Summary

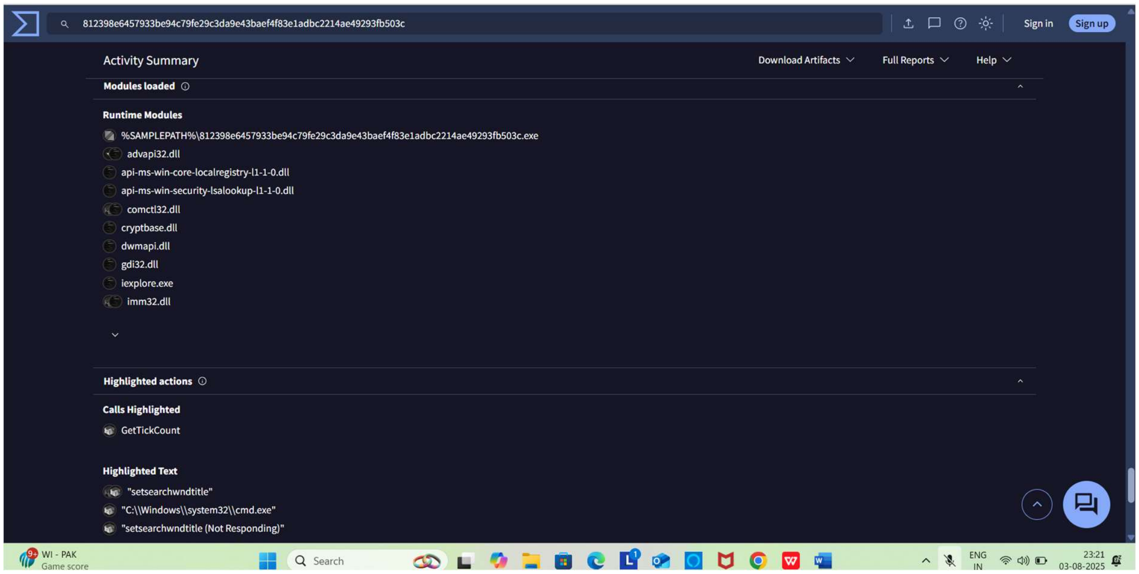
Synchronization mechanisms & Signals

Mutexes Opened

- \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
- \Sessions\1\BaseNamedObjects\Global\BFE_Notify_Event_{01543caa-df35-4678-8a3b-f8f8ed3e5e6d}
- \Sessions\1\BaseNamedObjects\Global\BFE_Notify_Event_{a9686143-5e9f-4558-be4c-3671df01e89a}
- \Sessions\1\BaseNamedObjects\Global\TermSrvReadyEvent
- \Sessions\1\BaseNamedObjects\Local\MSCTF.CtfActivated.Default1
- \Sessions\1\BaseNamedObjects\Local\MSCTF.CtfActivated.Windows update desktop1
- \Sessions\1\BaseNamedObjects\OperaCrashReporterInitEvent2720
- CicLoadWinStaWinSta0
- ShimCacheMutex
- fdc0b808-6ef1-409d-9f85-1834ac227262-chrome.exe

Mutexes Created

- fdc0b808-6ef1-409d-9f85-1834ac227262-chrome.exe
- fdc0b808-6ef1-409d-9f85-1834ac227262-firefox.exe
- fdc0b808-6ef1-409d-9f85-1834ac227262-iexplore.exe
- fdc0b808-6ef1-409d-9f85-1834ac227262-opera.exe
- \Sessions\1\BaseNamedObjects\Global\C:/Users/user/AppData/Local/Temp/opera_crashreporter.log
- \Sessions\1\BaseNamedObjects\Local\ChromeProcessSingletonStartup!
- \Sessions\1\BaseNamedObjects\Local\MSCTF.Asm.MutexWindows update desktop1
- \Sessions\1\BaseNamedObjects\Local\MSCTF.AsmCacheReady.Windows update desktop1



Activity Summary

Modules loaded

Runtime Modules

- %SAMPLEPATH%\812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c.exe
- advapi32.dll
- api-ms-win-core-localregistry-l1-1-0.dll
- api-ms-win-security-lsalookup-l1-1-0.dll
- comctl32.dll
- cryptbase.dll
- dwmapi.dll
- gdi32.dll
- iexplore.exe
- imm32.dll

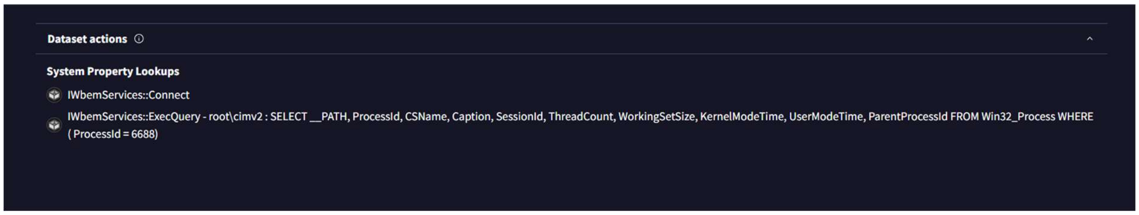
Highlighted actions

Calls Highlighted

- GetTickCount

Highlighted Text

- "setsearchwndtitle"
- "C:\\Windows\\system32\\cmd.exe"
- "setsearchwndtitle (Not Responding)"



Dataset actions

System Property Lookups

- IWbemServices::Connect
- IWbemServices::ExecQuery - root\cimv2 : SELECT __PATH, ProcessId, CSName, Caption, SessionId, ThreadCount, WorkingSetSize, KernelModeTime, UserModeTime, ParentProcessId FROM Win32_Process WHERE (ProcessId = 6688)

6. Community Section

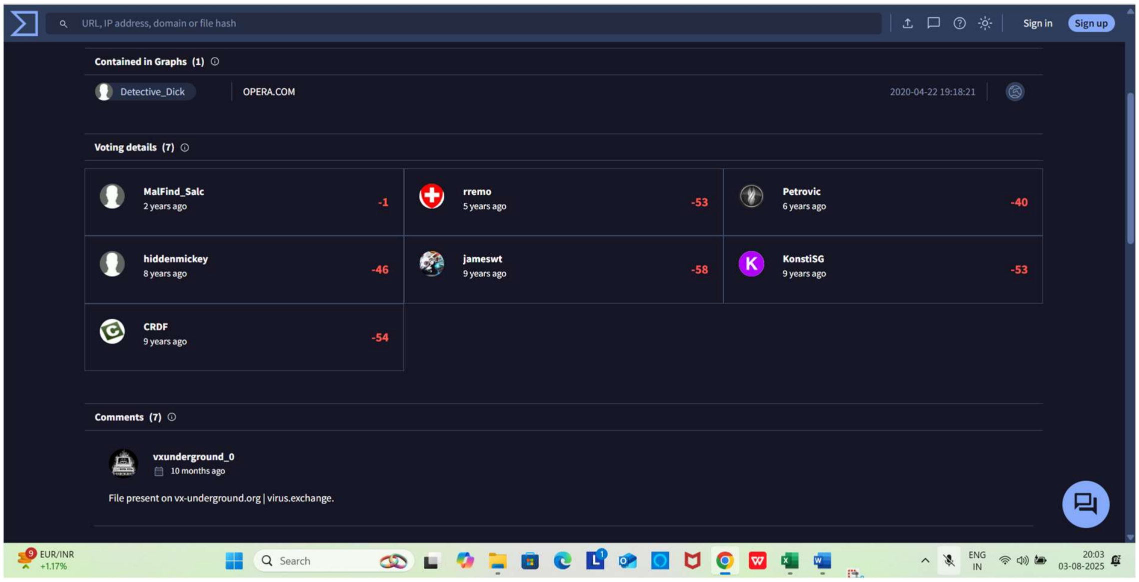
What it means:

Comments and votes by VirusTotal users or researchers on the malicious nature of the file.

Community

Multiple community members have confirmed the file to be malicious. Some have labeled it as part of known malware families.

This public feedback helps validate the automated detection and provides more context about the threat.



Contained in Graphs (1)

Detective_Dick OPERA.COM 2020-04-22 19:18:21

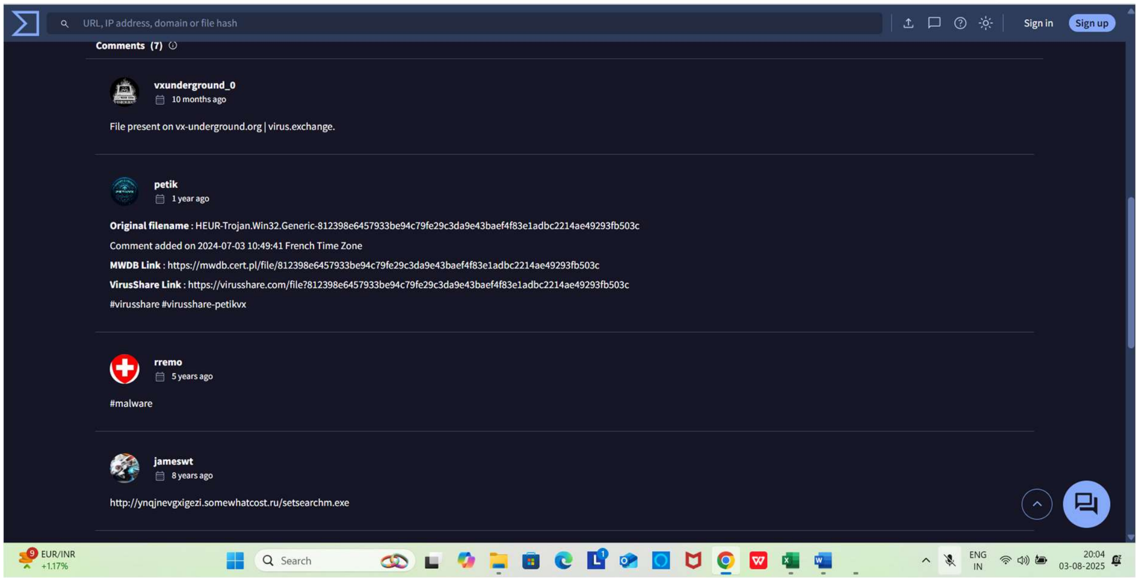
Voting details (7)

MalFind_Salc	2 years ago	-1
rremo	5 years ago	-53
Petrovic	6 years ago	-40
hiddenmickey	8 years ago	-46
jameswt	9 years ago	-58
KonstiSG	9 years ago	-53
CRDF	9 years ago	-54

Comments (7)

vxunderground_0
10 months ago

File present on vx-underground.org | virus.exchange.



Comments (7)

vxunderground_0
10 months ago

File present on vx-underground.org | virus.exchange.

petik
1 year ago

Original filename : HEUR-Trojan.Win32.Generic-812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
Comment added on 2024-07-03 10:49:41 French Time Zone
MWDB Link : https://mwdb.cert.pl/file/812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
VirusShare Link : https://virusshare.com/file?812398e6457933be94c79fe29c3da9e43baef4f83e1adbc2214ae49293fb503c
#virusshare #virusshare-petikvx

rremo
5 years ago

#malware

jameswt
8 years ago

http://ynqjnevgxigezi.somewhatcost.ru/setsearchm.exe

Objective of the Task

The purpose of this task was to analyze a suspicious file associated with W32.HfsAdware.8054 using VirusTotal, a widely used online malware analysis platform. The goal was to understand how this file behaves, how antivirus engines classify it, and what kind of threat it could pose to a system if allowed to run.

Steps I Took

1. I started by taking the hash of the suspicious file and searched for it on VirusTotal.

2. Once found, I carefully reviewed the different sections that VirusTotal provides:
    - Summary: for an overall view of the threat level.
    - Detection: to see how various antivirus engines responded.
    - Details: for technical metadata like file type and compilation time.
    - Relations: to see if the file is linked to any known malicious URLs or IPs.
    - Behaviour: to observe what actions the file might perform when executed.
    - Community: to read public comments from security researchers.
3. I noted down key findings and patterns that stood out.
4. I also documented the results and screenshots to support the report and make the investigation more visual and evidence-based.

What I Found

- The file was detected by multiple antivirus engines as W32.HfsAdware.8054 — a form of adware.
- The detection names suggest that the file:
    - Could be showing unwanted ads to the user.
    - Might change browser settings or redirect traffic.
    - Could potentially download other files or payloads onto the victim's system.
- The behaviour section indicated that the file could create registry entries, attempt persistence, and potentially establish connections to external domains.
- The Relations tab suggested some level of interaction with external URLs or IPs — possibly for ad delivery or remote control.
- Feedback in the Community section confirmed that other users and analysts had flagged this file as malicious or suspicious.

What I Learned

- How to analyze a file without running it — just by using its hash and looking up known intelligence.
- How to interpret antivirus engine results and understand what they tell us about malware types like adware.

- Why metadata like compilation time and file type can help reveal the origin and intent of a malicious file.
- How to use VirusTotal's relations and behaviour features to trace the bigger picture behind a single malware sample.

Why This Matters

- While adware is often considered “less harmful” than ransomware or trojans, it still poses a real threat — from tracking and spying to being used as a delivery method for more dangerous malware.
- This kind of analysis is useful for blue team roles, especially in SOC environments, and helps in threat detection, response, and prevention.
- It also shows the power of open tools like VirusTotal in understanding malware — especially when you don’t have access to a sandbox or reverse engineering tools.

Conclusion

Analysing W32.HfsAdware.8054 gave me hands-on experience with static and cloud-based malware analysis. I learned how to gather threat intelligence using hash-based searching, and how even seemingly low-risk files can behave in suspicious ways. This task strengthened my ability to detect and assess malware, a skill that is incredibly valuable for anyone aiming to work in cybersecurity, threat intelligence, or digital forensics.