TASK :- Malware Analysis

Name:- Chandan kumar **Intern Id :- 183**

Malware Analysis Report:- Trojan.Defi.Gen.1

1772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321

📄 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: (531.50 KB)
- First Submission Date: (2017-11-15 15:46:23 UTC)
- Last Analysis Date: (2025-08-02 20:30:51 UTC)
- Detection Ratio: (65/70 engines marked it malicious)

This clearly indicates the file poses a potential security risk.

🛡 2. Detection Section

What it means:

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

- Detection

This section contains detailed results from various antivirus engines. Many engines such as BitDefender, ALYac, Alibaba, and others have flagged the file as:

- Trojan.Fareit
- Ransom.Loki
- CoinMiner
- Dropper:Injector

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

🧬 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.

🔗 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.

Domain	Detections	Created	Registrar
business.bing.com	0 / 94	1996-01-29	MarkMonitor Inc.
c.bing.com	0 / 94	1996-01-29	MarkMonitor Inc.
clients2.googleusercontent.com	1 / 94	2008-11-17	MarkMonitor Inc.
edge-consumer-static.azureedge.net	0 / 94	2014-01-22	MarkMonitor Inc.
edge-mobile-static.azureedge.net	0 / 94	2014-01-22	MarkMonitor Inc.
edgeassetservice.azureedge.net	0 / 94	2014-01-22	MarkMonitor Inc.
firefox.settings.services.mozilla.com	0 / 94	1994-10-18	MarkMonitor Inc.
incoming.telemetry.mozilla.org	0 / 94	1998-01-24	MarkMonitor Inc.
js.monitor.azure.com	0 / 94	1994-10-25	MarkMonitor Inc.
login.live.com	0 / 94	1994-12-28	CSC Corporate Domains, Inc.

IP	Detections	Autonomous System	Country
13.107.253.70	0 / 94	8075	US
13.107.6.158	0 / 94	8068	US
150.171.27.10	0 / 94	8075	US
150.171.28.10	1 / 94	8075	US
172.253.117.132	0 / 94	15169	US
173.254.253.204	0 / 94	36352	US
192.168.0.14	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.101.57.9	0 / 94	8075	NL
20.190.159.138	0 / 94	8075	IE

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2023-07-31	28 / 57	ISO image	DeadlyNightShadeIII.iso

772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321

Sign in | Sign up

Bundled Files (100)

Scanned	Detections	File type	Name
2016-05-22	0 / 57	?	4080
2016-05-21	0 / 57	?	4086
2017-11-15	0 / 60	?	1125
2014-04-30	0 / 52	?	4086
2023-02-24	0 / 59	BMP	DI_MPPLAY.bmp
2023-02-24	0 / 59	BMP	CL_MPBACK.bmp
2025-08-01	0 / 62	ICO	32761
2024-10-17	0 / 62	BMP	BBABORT.bmp
2023-02-24	0 / 59	BMP	EN_MPNEXT.bmp
2023-02-27	0 / 59	?	4082

772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321

Sign in | Sign up

Dropped Files (4)

Scanned	Detections	File type	Name
?	?	file	16a19763520bc5acfa82af2e5e88c3392483d7fc79726e0f774fb6b737a4042f
2025-07-02	0 / 62	Text	PowerPlan.log
?	?	file	9a359c970b0bd60311e1d24cfc72fce42e9697fb9145d3b27dc1380c0787585b
2025-07-02	0 / 60	Text	Null

PE Resource Children (3)

Scanned	Detections	File type	Name
2016-05-22	0 / 57	?	4080
2016-05-21	0 / 57	?	4086
2017-11-15	0 / 60	?	1125

🧠 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.

🔹 Behavior

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 behaviors are typical of malware like **ransomware or infostealers**.

Malware Behavior Catalog Tree

- Anti-Behavioral Analysis OB0001
- Anti-Static Analysis OB0002
- Collection OB0003
- Credential Access OB0005
- Defense Evasion OB0006
- Discovery OB0007
- Impact OB0008
- Execution OB0009
- Persistence OB0012
- Privilege Escalation OB0013
- File System OC0001
- Memory OC0002
- Process OC0003
- Data OC0004
- Communication OC0006
- Operating System OC0008

Capabilities

- Collection
- Host-Interaction
- Compiler
- Anti-Analysis
- Data-Manipulation
- Executable
- Linking

Network Communication

DNS Resolutions

- business.bing.com
- c.bing.com
- clients2.googleusercontent.com
- edge-consumer-static.azureedge.net
- edge-mobile-static.azureedge.net

IP Traffic

- TCP 13.107.253.70:443 (edge-mobile-static.azureedge.net)
- TCP 13.107.6.158:443 (business.bing.com)
- TCP 44.241.83.71:443 (mscom.demdex.net)
- TCP 150.171.27.10:443 (c.bing.com)
- TCP 172.253.117.132:443 (clients2.googleusercontent.com)
- 173.254.253.204:1122
- TCP 20.99.133.109:443
- TCP 192.229.211.108:80
- UDP 192.168.0.14:137
- TCP 23.55.140.42:80 (www.microsoft.com)
- TCP 173.254.253.204:1122
- TCP 65.9.83.77:443 (firefox.settings.services.mozilla.com)

Files Opened

- C:\Program Files (x86)\Microsoft\Edge\Application\msedge.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\
- C:\ProgramData\Microsoft\Network\Downloader

Files Dropped

+ edb.chk
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\Crashpad
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\Crashpad\attachments
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\Crashpad\metadata
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\Crashpad\reports
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\uninstall.cmd
- C:\Program Files (x86)\Google\GoogleUpdater\140.0.7273.0\updater.exe
- C:\Program Files\Google2480_961645614
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER1558.tmp

Registry actions

Registry Keys Opened

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\Attributes
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace\DelegateFolders
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUriCacheSize
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon

Registry Keys Set

Gemini Summary

+ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W32Time\Config\LastKnownGoodTime
+ <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run\BC_Client
+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\BC_Client
+ HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent\LastPingSentAt

Process and service actions

Processes Created

- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=executable.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0
- "C:\Users\<USER>\Desktop\executable.exe"
- C:\Windows\System32\RuntimeBroker.exe -Embedding
- C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
- C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost
- 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

Activity Summary

Download Artifacts | Full Reports | Help

Shell Commands

"C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://go.microsoft.com/fwlink/?prd=11324&pver=4.5&sbp=AppLaunch2&plcid=0x409&o1=SHIM_NOVERSION_FOUND&version=(null)&processName=executable.exe&platform=0009&osver=6&isServer=0&shimver=4.0.30319.0

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\<USER>\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\<USER>\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=122.0.6261.129 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.92 --initial-client-data=0x32c,0x330,0x334,0x328,0x33c,0x7ffe369b5fd8,0x7ffe369b5fe4,0x7ffe369b5ff0

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2080 --field-trial-handle=2084,i,2824973399164824329,7129459874879380768,262144 --variations-seed-version /prefetch:2

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2420 --field-trial-handle=2084,i,2824973399164824329,7129459874879380768,262144 --variations-seed-version /prefetch:3

"C:\Users\<USER>\Desktop\executable.exe"

"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe" -ServerName:InputApp.AppX9jnwykgrccxc8by3hsrsh07r423xzvav.mca

"C:\Windows\system32\BackgroundTaskHost.exe" -ServerName:BackgroundTaskHost.WebAccountProvider

C:\Windows\System32\RuntimeBroker.exe -Embedding

C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc

Processes Terminated

%WINDIR%\syswow64\cmd.exe

%WINDIR%\syswow64\reg.exe

<PATH_SAMPLE.EXE>

<SYSTEM32>\wbem\wmiprvse.exe

C:\Program Files\Google2484_713615054\bin\updater.exe

C:\Windows\System32\UI0Detect.exe

C:\Windows\System32\wuapihost.exe

C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe

Services Opened

VaultSvc

clipsvc

Synchronization mechanisms & Signals

Mutexes Opened

\Sessions\1\BaseNamedObjects\Global\.net clr networking

ShimCacheMutex

Mutexes Created

\Sessions\1\BaseNamedObjects\

\Sessions\1\BaseNamedObjects\Global\.net clr networking

\Sessions\1\BaseNamedObjects\Global\CorDBIPCSetupSyncEvent_2056

\Sessions\1\BaseNamedObjects\c6ffeb26-2059-444f-821b-62ab565762e0

CTF.Asm.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500

CTF.Compart.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500

CTF.LBES.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500

CTF.Layouts.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500

CTF.TMD.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500

CTF.TimListCache.FMPDefaultS-1-5-21-1482476501-1645522239-1417001333-500MUTEX.DefaultS-1-5-21-1482476501-1645522239-1417001333-500

Highlighted actions

Highlighted Text

"C:\\Windows\\system32\\cmd.exe"

🌐 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.

772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321

Comments (4)

vxunderground_0
9 months ago

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

intezer_analyze
4 years ago

#malware #MaliciousPacker
#packed
Full genetic report from Intezer Analyze:
https://analyze.intezer.com/#/files/772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321
#IntezerAnalyze

rremo
5 years ago

#malware

HybridAnalysis
7 years ago

submitname:"19a6ea0f-cca8-11e7-967e-80e65024849a.file.exe.bin"
vxstream-threatscore:100/100
memurl:"Heuristic match: Font.Name"
memip:"7.1.7.96"
source:https://www.hybrid-analysis.com/sample/772d9f798c5e823b84daa0928beb65722bdddf42e8bb18256a50dbaea959c321?environmentId=100

Summary of Work:-

🔍 Objective of the Task:

The objective of this task was to analyze a suspicious file for potential malicious behavior using VirusTotal and understand the threat indicators associated with it. This analysis helps identify the nature of the file, its behavior, and the potential impact it can have if executed.

🛠️ **Steps Taken:**

1. The suspicious file was uploaded to VirusTotal, a widely used malware analysis platform.
2. After upload, all relevant sections like Summary, Detection, Details, Relations, Behavior, and Community were analyzed step by step.
3. Each section was studied to understand how the file is behaving and what security vendors report about it.
4. Screenshots were taken from each section and documented accordingly in this PoC report.

📊 **Findings:**

- The file was flagged by multiple antivirus vendors as Trojan, Dropper, Ransomware (Loki), and Miner.
- The detection names suggest it is capable of:
    - Dropping further malicious files,
    - Encrypting user data (ransomware),
    - Stealing credentials (Fareit),
    - Possibly mining cryptocurrency.

- Behavior analysis showed signs of suspicious or unsafe activity patterns.
- Relationship graph pointed towards connections with other malicious files or URLs.
- Community comments and votes also indicated unsafe and suspicious behavior.

🎓 **What I Learned:**

- How to analyze files using VirusTotal.
- Interpreting results from multiple antivirus engines.
- Understanding the hashes, file relationships, dropper behavior, and AV labels.
- Importance of each section in malware analysis.
- How malware families like Fareit or Loki operate.

🤔 **Why this is important:**

- Such analysis is crucial in real-world Incident Response, Threat Hunting, or Purple Team exercises.
- Helps in building awareness and defending against phishing/malware attacks.
- Shows how open-source intelligence tools like VirusTotal can aid in malware investigation without deep reverse engineering.

✅ **Conclusion:**

This exercise provided hands-on experience in analyzing a malicious file using an industry-standard tool. It enhanced my understanding of how modern threats are

detected and how cybersecurity professionals use platforms like VirusTotal to investigate potential threats. This skill is essential for roles in Threat Intelligence, SOC (Security Operations Center), or Malware Analysis.