VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Display grouped sandbox reports

CAPA	0	7	0	0	0	0
Microsoft Sysinternals	0	0	0	0	15	3
VirusTotal Jujubox	0	0	0	0	0	0
Zenbox	0	1	0	0	0	0

Activity Summary

Download Artifacts | Full Reports | Help

Detections

NOT FOUND

Mitre Signatures

28 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

15 OTHER

Network comms

3 IP

Behavior Tags

idle

Mitre ATT&CK Tactics and Techniques

Execution TA0002

Command and Scripting Interpreter T1059
- Accept command line arguments

Shared Modules T1129
- Link function at runtime on Windows

Privilege Escalation TA0004

Access Token Manipulation T1134
- Modify access privileges

Defense Evasion TA0005

Obfuscated Files or Information T1027
- Encode data using XOR

Modify Registry T1112
- Delete registry value
- Delete registry key

Access Token Manipulation T1134
- Modify access privileges

File and Directory Permissions Modification T1222
- Set file attributes

Discovery TA0007

Application Window Discovery T1010
- Find graphical window

Query Registry T1012
- Query or enumerate registry key
- Query or enumerate registry value

System Information Discovery T1082
- Query environment variable
- Check OS version
- Get disk size
- Reads software policies
- Sample reads itself and does not show any behavior, likely it performs some host environment checks and compares to an embedded key

File and Directory Discovery T1083
ⓘ Get file system object information
ⓘ Enumerate files on Windows
ⓘ Get file size
ⓘ Get common file path
ⓘ Check if file exists
ⓘ Enumerate files recursively
ⓘ Reads ini files

Security Software Discovery T1518.001
ⓘ May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

Collection TA0009

Clipboard Data T1115
ⓘ Open clipboard

Video Capture T1125
ⓘ Capture webcam image

Impact TA0034

System Shutdown/Reboot T1529
ⓘ Shutdown system

Impact TA0040

System Shutdown/Reboot T1529
ⓘ Shutdown system

Network Communication

IP Traffic
192.229.211.108:80 (TCP)
20.99.133.109:443 (TCP)
a83f:8110:0:0:0:0:0:800:53 (UDP)

Behavior Similarity Hashes ⓘ

CAPA
76c6c8e44cd4f1dbddc0f6c2202c1480

Microsoft Sysinternals
6d50b0036b7cc4b877078c34e5bfe50b

VirusTotal Jujubox
191faad5a09da73eae2a7cc1c593c36b

Zenbox
a859a46bf50c84f856b4b29bd1d7d983

File system actions ⓘ

Files Opened

C:\Windows\system32\UXTHEME.dll

C:\Windows\system32\USERENV.dll

C:\Windows\system32\SETUPAPI.dll

C:\Windows\system32\APPHELP.dll

C:\Windows\system32\PROPSYS.dll

C:\Windows\system32\DWMAPI.dll

C:\Windows\system32\CRYPTBASE.dll

C:\Windows\system32\OLEACC.dll

C:\Windows\system32\OLEACCRC.DLL

C:\Windows\system32\CLBCATQ.dll

Files Written

C:\Users\user\AppData\Local\Microsoft\Windows\Caches

C:\Users\user\AppData\Local\Temp\

C:\Users\user\AppData\Local\Temp\nsh809F.tmp

Files Deleted

C:\ProgramData\Microsoft\Windows\WER\Temp\WER17B9.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1884.tmp.csv

C:\ProgramData\Microsoft\Windows\WER\Temp\WER18B4.tmp.txt

C:\Windows\System32\spp\store\2.0\cache\cache.dat

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A96.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A97.tmp.csv

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AA8.tmp.txt

C:\Users\<USER>\AppData\Local\Temp\nsn99A1.tmp

C:\Users\user\AppData\Local\Temp\nsh809F.tmp

Files Dropped

%USERPROFILE%\AppData\Local\Temp\nshDD6F.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER17B9.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER17B9.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1884.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1884.tmp.csv

C:\ProgramData\Microsoft\Windows\WER\Temp\WER18B4.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER18B4.tmp.txt

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A96.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A96.tmp.WERInternalMetadata.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2A97.tmp

Registry actions

Registry Keys Opened

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma

HKEY_CURRENT_USER\Software\Microsoft\CTF\DirectSwitchHotkeys

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder

Process and service actions

Processes Created

%SAMPLEPATH%\3d63c59fc80b92ba67a8a5b2d3c1effa8ab5f70a224be06287bf359958c370a8.exe

C:\Windows\System32\wuapihost.exe

Shell Commands

"%SAMPLEPATH%\3d63c59fc80b92ba67a8a5b2d3c1effa8ab5f70a224be06287bf359958c370a8.exe"

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

Processes Terminated

C:\Windows\System32\wuapihost.exe

Processes Tree

↳ 1996 - %SAMPLEPATH%\3d63c59fc80b92ba67a8a5b2d3c1effa8ab5f70a224be06287bf359958c370a8.exe

↳ 2828 - C:\Windows\System32\wuapihost.exe

2872 - %WINDIR%\explorer.exe

616 - C:\Windows\System32\svchost.exe

7652 - C:\Users\user\Desktop\software.exe

Modules loaded

Runtime Modules

%SAMPLEPATH%\3d63c59fc80b92ba67a8a5b2d3c1effa8ab5f70a224be06287bf359958c370a8.exe

C:\Windows\system32\UXTHEME.dll

C:\Windows\system32\USERENV.dll

API-MS-Win-Core-LocalRegistry-L1-1-0.dll

advapi32.dll

C:\Windows\system32\SETUPAPI.dll

C:\Windows\system32\APPHELP.dll

propsys.dll

C:\Windows\system32\PROPSYS.dll

C:\Windows\system32\DWMAPI.dll

Highlighted actions

Calls Highlighted

GetTickCount

Highlighted Text

Optional update delivery is not working

NSIS Error

Installer integrity check has failed. Common causes include incomplete download and damaged media. Contact the installer's author to obtain a new copy. More information at: http://nsis.sf.net/NSIS_Er