KVMX

Evidence-First Malware Analysis

Analysis Report: 89de93e69e898d5d.bin

Verdict: MALICIOUS

Verdict: suspicious; 42 anti-VM checks (mixed)

Analysis Overview

Score: 3/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1055.001
- T1056.001
- T1070.004
- T1082
- T1129
- T1134
- T1574.002
- T1622

Hashes

SHA-256:	89de93e69e898d5da92c572f472fc8d0b3b1162eb8d98d4790d2fd6ff849de5b
SHA-1:	4573e72c90d7e6a5f30fb75f460c2573e66f8edb
MD5:	b89ab8277e1e5136f709f9bafa335a06
Size:	1,273,856 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x2AE0
Sections:	7

Name	Virtual Size	Entropy
.text	0x1A0A7	6.49
.rdata	0xCB32	5.24
.data	0x2AE8	1.92

.pdata	0x11D0	5.24
.fptable	0x100	0.0
.rsrc	0x10D4FC	8.0
.reloc	0x658	4.84

Imports

KERNEL32.dll

- CloseHandle
- DuplicateHandle
- GetLastError
- QueryPerformanceCounter
- QueryPerformanceFrequency
- WaitForSingleObject
- CreateMutexW
- Sleep
- GetCurrentProcess
- GetCurrentProcessId

USER32.dll

- MessageBoxW
- GetDoubleClickTime
- GetCaretBlinkTime
- GetSystemMetrics
- wsprintfW
- GetCursorPos
- GetAsyncKeyState
- wsprintfA
- GetWindowRect
- GetDesktopWindow

SHELL32.dll

- SHGetFolderPathW

ADVAPI32.dll

- RegOpenKeyExW
- GetTokenInformation
- OpenProcessToken
- GetUserNameW
- RegCloseKey

COMCTL32.dll

- InitCommonControlsEx

SHLWAPI.dll

- StrCmpIW
- PathFileExistsW

UxTheme.dll

- IsAppThemed
- IsThemeActive

USERENV.dll

- GetUserProfileDirectoryW

ole32.dll

- CoInitializeEx
- CoUninitialize

VERSION.dll

Strings (200 found)

```
!Please run under supported environment    $
kd'Y
"Rich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
RZRZS[@USWATAUAVAWH
D$pL
D$hH
D2,E;
L2$A
fA;|$
D$(@
D$ L
D$`H
D$Pt
D$ H
D$HE3
D$@H
|$8H
T$(H
L$PH
D$ A
|$ L
t$pH
L$PH
L$P3
A_A^A]A\_[]
t$pLc{<L
D$xH
L$PE3
|$xL
D$ H
L9t$x
L$PH
D$ M
L$PL
D$pA
|$pI
D$xH
|$xA
T$xH
L$PL
L$PL
D$pH
|$ A
```

... and 150 more

MITRE ATT&CK (9)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1055.001			static-analyzer
T1056.001			static-analyzer
T1070.004			static-analyzer
T1082			static-analyzer
T1129			static-analyzer
T1134			static-analyzer
T1574.002			static-analyzer
T1622			static-analyzer

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: dropped_exe

Network Connections (6)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:53		udp
10.0.2.255:137		udp
224.0.0.251:5353		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp

Behavioral Timeline (56)

1. [conn] pid 0: udp 255.255.255.255:67
2. [conn] pid 0: udp 224.0.0.251:5353
3. [conn] pid 0: udp 224.0.0.252:5355
4. [conn] pid 0: udp 10.0.2.3:53
5. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
6. [conn] pid 0: tcp 10.0.2.3:80
7. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
8. [conn] pid 0: udp 10.0.2.255:137
9. [conn] pid 0: tcp 10.0.2.3:80
10. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
11. [conn] pid 0: tcp 10.0.2.3:80
12. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
13. [conn] pid 0: tcp 10.0.2.3:80
14. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
15. [conn] pid 0: tcp 10.0.2.3:80
16. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
17. [conn] pid 0: tcp 10.0.2.3:80
18. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
19. [conn] pid 0: udp 10.0.2.3:53

```
20. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
21. [conn] pid 0: tcp 10.0.2.3:80
22. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
25. [conn] pid 0: udp 10.0.2.3:53
```

...and 31 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
smss.exe - \SystemRoot\System32\smss.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
dbInstaller.ex
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
dxgiadaptercac - "C:\Windows\system32\dxgiadaptercache.exe"
```

...and 20 more