KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_03a3b3b2a9a5.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 3/10

Threat level: Suspicious

Malicious Activity Summary

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

Hashes

SHA-256:	03a3b3b2a9a5589a715f18c7d9e190d38ec7b55a4f58ecdc9842522060f8f03e
SHA-1:	741a5116e0fc72dcda5e40363130993ccfbefebe
MD5:	cc25118912dc80911f76be64487a3b1d
Size:	1,399,536 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	0x129120	7.91
.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)

```
!Cannot execute in real-mode session       $
06n!Z
Rich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
@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
`224.0.0.252:5355`		`udp`
`10.0.2.3:80`		`tcp`
`10.0.2.3:53`		`udp`
`224.0.0.251:5353`		`udp`
`10.0.2.255:137`		`udp`
`255.255.255.255:67`		`udp`

Behavioral Timeline (57)

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

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

...and 32 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
wininit.exe - wininit.exe
winlogon.exe - winlogon.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
XtuService.exe - C:\Windows\SysWOW64\XtuService.exe
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv bXWSOVrS+k+3WsGXZLgrkA.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
```

...and 20 more