KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_9355412abe08.exe

Verdict: SUSPICIOUS

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

Analysis Overview

Score: 3/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- Indicator Removal: File Deletion
- Native API
- Modify Registry
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Process Discovery

Hashes

SHA-256:	9355412abe08d3781913f925945e2b93713961b95df327b0f153c29dd3483f0d
SHA-1:	1a03566116122f267b9eae418701679774934f22
MD5:	dda06dac764df47dfca1fa34900042a4
Size:	626,600 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x369F
Sections:	5

Name	Virtual Size	Entropy
.text	0x6711	6.45
.rdata	0x1358	5.1
.data	0x1FB78	4.12

.ndata	0x2C000	0.0
.rsrc	0x7E50	5.28

Imports

ADVAPI32.dll

- RegEnumValueW
- RegEnumKeyW
- RegQueryValueExW
- RegSetValueExW
- RegCloseKey
- RegDeleteValueW
- RegDeleteKeyW
- AdjustTokenPrivileges
- LookupPrivilegeValueW
- OpenProcessToken

SHELL32.dll

- SHGetPathFromIDListW
- SHBrowseForFolderW
- SHGetFileInfoW
- SHFileOperationW
- ShellExecuteExW

ole32.dll

- CoCreateInstance
- OleUninitialize
- OleInitialize
- IIDFromString
- CoTaskMemFree

COMCTL32.dll

- ImageList_Destroy
- ImageList_AddMasked
- ImageList_Create

USER32.dll

- MessageBoxIndirectW
- GetDlgItemTextW
- SetDlgItemTextW
- CreatePopupMenu
- AppendMenuW
- TrackPopupMenu
- OpenClipboard
- EmptyClipboard
- SetClipboardData
- CloseClipboard

GDI32.dll

- GetDeviceCaps
- SetBkColor
- SelectObject
- DeleteObject
- CreateBrushIndirect
- CreateFontIndirectW
- SetBkMode
- SetTextColor

KERNEL32.dll

RemoveDirectoryW
lstrcmpiA
GetTempFileNameW
CreateProcessW
CreateDirectoryW
CreateThread
GlobalLock
GlobalUnlock
GetDiskFreeSpaceW
WideCharToMultiByte

Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.ndata
.rsrc
 s495
taj\V
>FFf;
v'f9
ur9]
uOVh
tDH;
jHjZV
t99]
PSWV
WQSPV
QWPV
SQWPV
8u+j!
t"9]
t#SSS
PjdQ
vX95h
SVW3
Instuj
softua
NulluX
u]9u
t!VU
_^][
UVWj _3
D$4P
L$bf-S
j Zf;
AAf9
t$j"^
f91u
u6Vh
```

```
f9l$
[t$h
D$ Pj(
D$(Ph
D$,UPU
Vj%UUU
WSWh
f9=P/B
tWf="
WPWj0
```
... and 150 more

MITRE ATT&CK (9)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1115	Clipboard Data	Collection	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1057	Process Discovery		pt_trace

Per-Process ATT&CK Attribution (3)

Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).

			Proces
LogonUI.exe	1044	504	T1057
NVDisplay.Cont	1300	1595	T1055, T1083
svchost.exe	764	58	T1057

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

Destination	Domain	Proto
10.0.2.3:53		udp
10.0.2.3:80		tcp
224.0.0.251:5353		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		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 10.0.2.255:137
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
7. [conn] pid 0: tcp 10.0.2.3:80
8. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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 32 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv j43ugGoHREK3o03rpBpGXA.0
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
sppsvc.exe - C:\Windows\system32\sppsvc.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
smss.exe - \SystemRoot\System32\smss.exe 000000c4 00000084
```

```
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b18855 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
```

...and 20 more