KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_70b4932caeb9.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 80 anti-VM checks (mixed)

Analysis Overview

Score: 5/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- System Information Discovery
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- File and Directory Discovery
- Scheduled Task/Job: Scheduled Task
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	70b4932caeb92c33fbe1a8ad33aa73eb9ee2d7b3e32eab0cc0c7f5e8ec97678a
SHA-1:	2f823cbfa3c1c985b1cb2f322b292d44d190005e
MD5:	e1cc665a64d2023e50a377d5580147af
Size:	880,368 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x76C0

Sections: 7

Name	Virtual Size	Entropy
.text	0x1A1B1	6.55
.rdata	0xCF46	5.1
.data	0x1AEA8	1.94
.pdata	0x14A0	5.12
.fptable	0x100	0.0
.rsrc	0xA9C3C	7.7
.reloc	0x664	4.89

Imports

KERNEL32.dll

- TerminateProcess
- CreateThread
- GetCurrentThreadId
- OpenThread
- FlushInstructionCache
- GetTickCount
- VirtualAlloc
- VirtualProtect
- VirtualFree
- GetModuleHandleA

USER32.dll

- DispatchMessageW
- GetSystemMetrics
- GetCursorPos
- wsprintfA
- MsgWaitForMultipleObjectsEx
- PeekMessageW
- TranslateMessage
- MessageBoxW
- wsprintfW
- GetAsyncKeyState

ADVAPI32.dll

- RegCloseKey
- GetTokenInformation
- OpenProcessToken
- RegQueryInfoKeyW
- RegOpenKeyExW
- GetUserNameW

COMCTL32.dll

- InitCommonControlsEx

SHLWAPI.dll

- PathFileExistsW
- StrCmpIW

UxTheme.dll

- IsAppThemed
- IsThemeActive

USERENV.dll

GetUserProfileDirectoryW

ole32.dll

CoInitializeEx

CoUninitialize

VERSION.dll

GetFileVersionInfoSizeW

Strings (200 found)

```
mgvSg
'-Xy
Rich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
L$ L
SVWATAUAVAWH
D$8ole3
D$<2.dlf
D$@l
D$HH
\$ M
\$LE2
D$`H
D$tH
D$23
d$3L
L$LD
|$03
d$3H
|$1E3
D$`H
D$tH
|$03
 tyD
|$03
|$1H
A_A^A]A\_^[
\$0H
t$8H
sssss
I*Ai
sssss
|l3sH
|$ f
|$ fA
|l7ss
D$8H
D$(H
\$ A
```

"r?L

\$`H

t$hH

|$pH

|l7ss|ls

... and 150 more

Malware Config

C2 / Network (6)

Endpoint	Source
api.msn.com	decrypted_c2
assets.msn.com	decrypted_c2
config.edge.skype.com	decrypted_c2
fs.microsoft.com	decrypted_c2
settings-win.data.microsoft.com	decrypted_c2
www.bing.com	decrypted_c2

Indicators of Compromise (4)

Domains (4)

- api.msn.com
- assets.msn.com
- www.bing.com
- config.edge.skype.com

MITRE ATT&CK (16)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1055	Process Injection	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1057	Process Discovery	Discovery	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1083	File and Directory Discovery		pt_trace
T1053.005	Scheduled Task/Job: Scheduled Ta	Persistence	behavioral_inference
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (2)

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

			Proces
urlhaus_70b493	4548	686	T1083, T1055
svchost.exe	748	536	T1083

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 50/100 (medium)

Factors: evasion, attack_techniques

Network Connections (5)

Destination	Domain	Proto
255.255.255.255:67		udp
224.0.0.251:5353		udp
224.0.0.252:5355		udp
169.254.255.255:137		udp
169.254.255.255:138		udp

Behavioral Timeline (41)

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 169.254.255.255:137
5. [conn] pid 0: udp 169.254.255.255:138
6. [file]: write /ProgramData/Intel/Intel Extreme Tuning Utility/Logs/XtuCore.20260823-09423683.log
7. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Deployment.srd-shm
8. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Deployment.srd-wal
9. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd
10. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd-shm
11. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd-wal
12. [file]: write /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat
13. [file]: write /ProgramData/Microsoft/Windows/wfp/wfpdiag.etl
14. [file]: write /ProgramData/NVIDIA/DisplaySessionContainer1.log
15. [file]: write /ProgramData/NVIDIA/DisplaySessionContainer1.log_backup1
16. [file]: write /ProgramData/NVIDIA/NVDisplay.ContainerLocalSystem.log
17. [file]: write /ProgramData/NVIDIA/NVDisplay.ContainerLocalSystem.log_backup1
18. [file]: write /ProgramData/NVIDIA/NVDisplayContainerWatchdog.log
19. [file]: write /ProgramData/NVIDIA/NVDisplayContainerWatchdog.log_backup1
20. [file]: write /ProgramData/NVIDIA/NvcDispCorePlugin.log
21. [file]: write /ProgramData/NVIDIA/NvcDispCorePlugin.log_backup1
22. [file]: write /ProgramData/NVIDIA Corporation/Drs/nvdrsdb1.bin
23. [file]: write /ProgramData/NVIDIA Corporation/Drs/nvdrssel.bin
24. [file]: write /ProgramData/NVIDIA Corporation/GameSessionTelemetry/telemetryPlugin.log
25. [file]: write /ProgramData/NVIDIA Corporation/GameSessionTelemetry/telemetryPlugin.log_backup

...and 16 more events

Packet capture: available (full PCAP)

Persistence (1)

[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat

Spawned Processes (50)

System

svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM

```
Registry
fontdrvhost.ex - "fontdrvhost.exe"
winlogon.exe - winlogon.exe
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
wininit.exe - wininit.exe
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
taskhostw.exe - taskhostw.exe SyncFromCloud
urlhaus_70b493 - svchost.exe
msedge.exe
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SAA
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
netsh.exe - netsh  advfirewall set allprofiles state off
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
dwm.exe - "dwm.exe"
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv 1AQ2AlB9/kyEMF2yg0Iw7A.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
```

...and 20 more