KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_ab5229913dad.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 76 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

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
- Scheduled Task/Job: Scheduled Task
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	ab5229913dad931d670af38f1038c84f0ce60a7c18407aad655f04863339b9a4
SHA-1:	d52888a0f9bfa8f02fd81393c20db89dd5f89c6d
MD5:	56b130aa5a2bf088c4f5768b1e6e3cd7
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	0xA9C44	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)

```
x>ER
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$8H
ssss
I*Ai
sssss
|$ f
|$ fA
|l3s
D$8H
D$(H
\$ A
"r?L
\$`H
```

`t$hH`

`|$pH`

`|ls@SH`

`sssss|ls@SH`

`r4E3`

... 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 (10)

URLs (3)

`https://aware-cr1.com/`

`https://aware-cr1.com/api/beacon`

`https://aware-cr1.com:443/api/beacon`

Domains (7)

`api.msn.com`

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

`aware-cr1.com`

`ipv6-literal.net`

`l.aware-cr1.com`

MITRE ATT&CK (15)

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	

T1053.005	Scheduled Task/Job: Scheduled Ta	Persistence	behavioral_inference
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 69/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (5)

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

Memory-Recovered IOCs (runtime deobfuscation) (6)

Decoded from guest memory at the hypervisor - recovered from obfuscation static analysis cannot unpack.

```
[url] https://aware-cr1.com/
[url] https://aware-cr1.com/api/beacon
[url] https://aware-cr1.com:443/api/beacon
[domain] aware-cr1.com
[domain] ipv6-literal.net
[domain] l.aware-cr1.com
```

Behavioral Timeline (38)

1. [conn] pid 0: udp 224.0.0.251:5353
2. [conn] pid 0: udp 224.0.0.252:5355
3. [conn] pid 0: udp 255.255.255.255:67
4. [conn] pid 0: udp 169.254.255.255:137
5. [conn] pid 0: udp 169.254.255.255:138
6. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Deployment.srd-shm
7. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Deployment.srd-wal
8. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd
9. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd-shm
10. [file]: write /ProgramData/Microsoft/Windows/AppRepository/StateRepository-Machine.srd-wal
11. [file]: write /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat
12. [file]: write /ProgramData/Microsoft/Windows/wfp/wfpdiag.etl
13. [file]: write /ProgramData/NVIDIA/DisplaySessionContainer1.log
14. [file]: write /ProgramData/NVIDIA/DisplaySessionContainer1.log_backup1
15. [file]: write /ProgramData/NVIDIA/NVDisplay.ContainerLocalSystem.log
16. [file]: write /ProgramData/NVIDIA/NVDisplay.ContainerLocalSystem.log_backup1
17. [file]: write /ProgramData/NVIDIA/NVDisplayContainerWatchdog.log
18. [file]: write /ProgramData/NVIDIA/NVDisplayContainerWatchdog.log_backup1
19. [file]: write /ProgramData/NVIDIA/NvcDispCorePlugin.log
20. [file]: write /ProgramData/NVIDIA/NvcDispCorePlugin.log_backup1
21. [file]: write /ProgramData/NVIDIA Corporation/Drs/nvdrsdb1.bin
22. [file]: write /ProgramData/NVIDIA Corporation/Drs/nvdrssel.bin
23. [file]: write /ProgramData/NVIDIA Corporation/GameSessionTelemetry/telemetryPlugin.log
24. [file]: write /ProgramData/NVIDIA Corporation/GameSessionTelemetry/telemetryPlugin.log_backup
25. [file]: write /ProgramData/NVIDIA Corporation/NvProfileUpdaterPlugin/NvProfileUpdaterPlugin_1.log

...and 13 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
Registry
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
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
urlhaus_ab5229 - svchost.exe
msedge.exe
urlhaus_ab5229 - "C:\Users\Public\Downloads\urlhaus_ab5229913dad.exe"
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv UJ+hSRo6t064PKP903e/7A.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
```

...and 20 more