

Analysis Report: urlhaus_8924a1fca4f3.exe

Verdict: **LIKELY-MALICIOUS**

Verdict: likely-malicious; 104 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

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:	8924a1fca4f30edf90d7bc4303d0248d6aa58580386e23d1387dc1e85f4d7162
SHA-1:	1b713072c1679665f1125593f677c15dcec0d8a3
MD5:	2950855d2e770a4bbb4cb5d776487809
Size:	655,952 bytes

Packer Detection

No packer detected.

PE Information

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

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	0x73660	7.99
.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)

k.\$t
&4l)
IRich
.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
|l3s|l3s
I*Ai
|l7ss|l3s|ls
|\$ f
|\$ fA
|l3s
D\$8H
D\$(H
\\$ A
"r?L

\\$`H
t\$hH
|\$pH
|l7ss|l
ssss
... and 150 more

Malware Config

Indicators of Compromise (11)

URLs (3)

https://telegram.me/m1duus
https://www.pinterest.com/m1duus
https://steamcommunity.com/profiles/76561198657426610

Domains (8)

telegram.me
www.pinterest.com
steamcommunity.com
aware-cr1.com
assets.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net

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: malicious-behavior
Threat score: 70/100 (high)

Factors: c2, attack_techniques

Network Connections (8)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
224.0.0.251:5353		udp
10.0.2.255:138		udp

TLS Handshake Failures (cert-pinning) (50)

assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)
assets.msn.com (tlsstate: deadline exceeded)

Behavioral Timeline (100)

- 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 224.0.0.251:5353
- 5. [conn] pid 0: udp 224.0.0.252:5355
- 6. [conn] pid 0: udp 10.0.2.255:137
- 7. [conn] pid 0: udp 10.0.2.3:53
- 8. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
- 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: udp 10.0.2.3:53
- 16. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
- 17. [conn] pid 0: tcp 10.0.2.3:443
- 18. [conn] pid 0: udp 10.0.2.3:53

```
19. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
20. [conn] pid 0: tcp 10.0.2.3:80
21. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
22. [conn] pid 0: tcp 10.0.2.3:80
23. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
24. [conn] pid 0: tcp 10.0.2.3:80
25. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
```

...and 75 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
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=0n SubSystem=
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
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
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SA
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
urlhaus_8924a1 - svchost.exe
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
ipconfig.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
NvDisplay.Cont - "C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContain
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
```

...and 20 more

Report ID: ixgwuxaiM3jFvCo9xKDR5pUXRtQLNck8H5aZoXBUmM8

Generated by KVMX - kvmx.ai