KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_f3414f6a3bd7.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 127 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- 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

Hashes

SHA-256:	f3414f6a3bd78e26a859f4301c98ef9094bc43508968331ba1265b711cdbe030
SHA-1:	6ff940ed7095ac5ba2074537032020d00aed67b9
MD5:	faf24936b7e05072e24445e3f0194716
Size:	783,088 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	0x9203C	7.62
.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)

```
#DEL
G@MYv\
hRich
.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$8H
ssss
I*Ai
|ls|l
ssss|l3sH
|$ f
|$ fA
|l3s
D$8H
D$(H
\$ A
"r?L
\$`H
t$hH
```

`|$pH`

`|l7ss|l`

... and 150 more

Malware Config

Indicators of Compromise (9)

URLs (2)

`https://t.me/x0xprs`

`https://steamcommunity.com/profiles/76561198664897346`

Domains (7)

`t.me`

`steamcommunity.com`

`aware-cr1.com`

`api.msn.com`

`assets.msn.com`

`www.bing.com`

`arc.msn.com`

MITRE ATT&CK (13)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			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

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`

224.0.0.252:5355		udp
10.0.2.255:138		udp
255.255.255.255:67		udp
10.0.2.255:137		udp
224.0.0.251:5353		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)
www.bing.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)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
```

Behavioral Timeline (100)

```
 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 224.0.0.252:5355
 6. [conn] pid 0: udp 224.0.0.252:5355
 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. [conn] pid 0: udp 10.0.2.3:53
11. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
12. [conn] pid 0: tcp 10.0.2.3:443
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:80
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: tcp 10.0.2.3:443
19. [conn] pid 0: tcp 10.0.2.3:80
20. [conn] pid 0: tcp 10.0.2.3:80
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:443
24. [conn] pid 0: tcp 10.0.2.3:80
25. [conn] pid 0: tcp 10.0.2.3:80
```

...and 75 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
conhost.exe
urlhaus_f3414f - svchost.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
taskhostw.exe
schtasks.exe
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
SIHClient.exe - C:\Windows\System32\sihclient.exe  /cv SC10HE00jk2bHNIpsUwWtQ.0.2
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
urlhaus_f3414f - "C:\Users\Public\Downloads\urlhaus_f3414f6a3bd7.exe"
SecurityHealth - "C:\Windows\System32\SecurityHealthSystray.exe"
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=networ
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
```

...and 20 more