KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e2affa0d6d98.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 118 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:	e2affa0d6d98ca6cd8dbb05f8db955a71127b37c631a9cea4c967bdc992c93e6
SHA-1:	cbe184ae6fff5254b172b160e127de27dee3409e
MD5:	05c80e5463a628b7c823595f3b1f4bbf
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)

```
}7N*
!oJH
>G*>
F#ty
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$8H
|l7ss
I*Ai
sssss|ls|lsH
|$ f
|$ fA
|l7ss
D$8H
D$(H
\$ A
"r?L
\$`H
```

t$hH

|$pH

... and 150 more

Malware Config

Indicators of Compromise (54)

URLs (14)

- http://t.me/x0xprs
- http://steamcommunity.com/profiles/76561198664897346
- http://crl.comodo.net/AAACertificateServices.crl0
- http://www.microsoft.com0
- http://www.quovadis.bm0
- https://aware-cr1.com/api/beacon
- https://aware-cr1.com:443/api/beacon
- https://ocsp.quovadisoffshore.com0
- https://steamcommunity.c
- https://steamcommunity.com/
- https://steamcommunity.com/profiles/76561198664897346
- https://steamcommunity.com/profiles/765611986648C2
- https://steamcommunity.com:443/profiles/76561198664897346
- https://t.me/x0xprs

IPv4 addresses (16)

- 1.3.132.0
- 1.3.36.3
- 1.9.16.1
- 1.9.16.2
- 2.23.43.1
- 2.5.29.1
- 2.5.29.10
- 2.5.29.14
- 2.5.29.15
- 2.5.29.17
- 2.5.29.19
- 2.5.29.31
- 2.5.29.32
- 2.5.29.35
- 2.5.29.37
- 41.3.6.1

Domains (24)

- t.me
- steamcommunity.com
- aware-cr1.com
- api.msn.com
- assets.msn.com
- www.bing.com
- arc.msn.com
- crl.comodo.net
- www.microsoft.com0
- www.quovadis.bm0
- ocsp.quovadisoffshore.com0

steamcommunity.c
absteamcommunity.com
access.nextlsoft.com
ate.com
ipv6-literal.net
izenpe.com
l.aware-cr1.com
ndowsupdate.com
ssl.com
stugwarepanelv2.com
tedsteamcommunity.com
unity.com
www.stugwarepanelv2.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
224.0.0.251:5353		udp
10.0.2.3:53		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
10.0.2.255:137		udp

Memory-Recovered IOCs (runtime deobfuscation) (48)

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

```
[url] http://crl.comodo.net/AAACertificateServices.crl0
[url] http://www.microsoft.com0
[url] http://www.quovadis.bm0
[url] https://aware-cr1.com/api/beacon
[url] https://aware-cr1.com:443/api/beacon
[url] https://ocsp.quovadisoffshore.com0
[url] https://steamcommunity.c
[url] https://steamcommunity.com/
[url] https://steamcommunity.com/profiles/76561198664897346
[url] https://steamcommunity.com/profiles/765611986648C2
[url] https://steamcommunity.com:443/profiles/76561198664897346
[url] https://t.me/x0xprs
[domain] absteamcommunity.com
[domain] access.nextlsoft.com
[domain] ate.com
[domain] aware-cr1.com
[domain] crl.comodo.net
[domain] ipv6-literal.net
[domain] izenpe.com
[domain] l.aware-cr1.com
[domain] ndowsupdate.com
[domain] ocsp.quovadisoffshore.com0
[domain] ssl.com
[domain] steamcommunity.c
[domain] steamcommunity.com
```

...and 23 more

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)
```

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 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. [conn] pid 0: udp 10.0.2.3:53
9. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
10. [conn] pid 0: tcp 10.0.2.3:443
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:80
14. [conn] pid 0: tcp 10.0.2.3:80
15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: tcp 10.0.2.3:80
19. [conn] pid 0: tcp 10.0.2.3:443
20. [conn] pid 0: tcp 10.0.2.3:80
21. [conn] pid 0: tcp 10.0.2.3:80
22. [conn] pid 0: tcp 10.0.2.3:80
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
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
winlogon.exe - winlogon.exe
smss.exe - \SystemRoot\System32\smss.exe
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
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.RulesEngine.AppXgphnekvm0vv49drvfeh
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
urlhaus_e2affa - svchost.exe
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.IrisService.AppXwt29n3t7x7q6fgyrrbb
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
msedge.exe
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=SAA
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
conhost.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
taskhostw.exe - taskhostw.exe SyncFromCloud
netsh.exe - netsh  advfirewall set allprofiles state off
```

```
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
```

...and 20 more