KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_3b39762bbe07.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 77 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:	3b39762bbe07ca79b3d8db0e96d5cda84aee772becc387f52abc5d395b4024ea
SHA-1:	3cc8d8374f728f5af4e2c891893c256fdf21c540
MD5:	60f6b6954afed7de062f392a27ec910d
Size:	640,000 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	0x721D0	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)

```
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$8H
|l3s
I*Ai
|l3s
|$ f
|$ fA
|l7ssH
D$8H
D$(H
\$ A
"r?L
\$`H
t$hH
```

`|$pH`

`sssss|ls`

`r4E3`

`TCDA`

`D$`H`

... and 150 more

Malware Config

C2 / Network (4)

Endpoint	Source
`api.msn.com`	decrypted_c2
`assets.msn.com`	decrypted_c2
`config.edge.skype.com`	decrypted_c2
`www.bing.com`	decrypted_c2

Indicators of Compromise (58)

URLs (14)

- `https://telegram.me/s11yme`
- `https://dev.epicgames.com/community/api/user_profiles/profile.json`
- `https://steamcommunity.com/profiles/76561198652917381`
- `http://crl.comodo.net/AAACertificateServices.crl0`
- `http://ctldl.win`
- `http://www.microsoft.com0`
- `http://www.quovadis.bm0`
- `https://aware-cr1.com/api/beacon`
- `https://aware-cr1.com:443/api/beacon`
- `https://dev.epicgames.com/`
- `https://dev.epicgames.com/community/api/user_profiles/profile.json?hash_id=roAjr`
- `https://ocsp.quovadisoffshore.com0`
- `https://telegram.me/`
- `https://telegram.me:443/s11yme`

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 (28)

- `telegram.me`

```
dev.epicgames.com
steamcommunity.com
assets.msn.com
api.msn.com
www.bing.com
config.edge.skype.com
aware-cr1.com
edge-consumer-static.azureedge.net
crl.comodo.net
ctldl.win
www.microsoft.com0
www.quovadis.bm0
ocsp.quovadisoffshore.com0
access.nextlsoft.com
ate.com
epicgames.com
ign.com
ipv6-literal.net
izenpe.com
munity.com
ndowsupdate.com
ssl.com
stugwarepanelv2.com
tedsteamcommunity.com
ty.com
update.com
www.stugwarepanelv2.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

Per-Process ATT&CK Attribution (4)

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

Proces

svchost.exe	3044	191	T1057, T1134
NVDisplay.Cont	1188	466	T1055
msedge.exe	5724	8	T1057
0x144b78000		74	T1057

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
10.0.2.3:53		udp
10.0.2.3:443		tcp
224.0.0.252:5355		udp
10.0.2.255:138		udp
10.0.2.255:137		udp
224.0.0.251:5353		udp
255.255.255.255:67		udp

Memory-Recovered IOCs (runtime deobfuscation) (52)

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

```
[url] http://crl.comodo.net/AAACertificateServices.crl0
[url] http://ctldl.win
[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://dev.epicgames.com/
[url] https://dev.epicgames.com/community/api/user_profiles/profile.json?hash_id=roAjr
[url] https://ocsp.quovadisoffshore.com0
[url] https://steamcommunity.com/profiles/76561198652917381
[url] https://telegram.me/
[url] https://telegram.me/s11yme
[url] https://telegram.me:443/s11yme
[domain] access.nextlsoft.com
[domain] ate.com
[domain] aware-cr1.com
[domain] crl.comodo.net
[domain] ctldl.win
[domain] dev.epicgames.com
[domain] epicgames.com
[domain] ign.com
[domain] ipv6-literal.net
[domain] izenpe.com
[domain] munity.com
[domain] ndowsupdate.com
```

...and 27 more

TLS Handshake Failures (cert-pinning) (50)

```
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)
www.bing.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
www.bing.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)
functional.events.data.microsoft.com  (remote error: tls: unknown certificate)
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 224.0.0.252:5355
8. [conn] pid 0: udp 10.0.2.3:53
9. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
10. [conn] pid 0: tcp 10.0.2.3:80
11. [conn] pid 0: tcp 10.0.2.3:80
12. [conn] pid 0: tcp 10.0.2.3:80
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:443
16. [conn] pid 0: udp 10.0.2.3:53
17. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
18. [conn] pid 0: tcp 10.0.2.3:80
19. [conn] pid 0: tcp 10.0.2.3:80
20. [conn] pid 0: udp 10.0.2.3:53
21. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
22. [conn] pid 0: tcp 10.0.2.3:443
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)

Persistence (1)

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

Spawned Processes (50)

```
System
Registry
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
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
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
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=networ
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
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
taskhostw.exe - taskhostw.exe $(Arg0)
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_s
urlhaus_3b3976 - svchost.exe
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
netsh.exe
schtasks.exe - schtasks.exe /create /tn "WindowsSecurityHealth" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
```

...and 20 more