KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e2f09c867cb0.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- Decrypted C2 recovered (14 HTTPS request(s)) - TLS-MITM at the hypervisor
- 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:	e2f09c867cb0194c3d7de3c01c9895a14c53d1dd7442a8965248b3ada1b7b945
SHA-1:	180d2faf10b8d284ea6cf41acf848ed8039f687d
MD5:	322d8fe630c940a272603e54f3ac5b46
Size:	1,474,800 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	0x13AEE8	7.88
.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)

```
.b#j
^g(X
YRich
.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$8H
sssss
I*Ai
sssss
|$ f
|$ fA
|l7ss
D$8H
D$(H
\$ A
"r?L
```

\$`H

t$hH

|$pH

sssss|l7ss

r4E3

... and 150 more

Malware Config

C2 / Network (7)

Endpoint	Source
api.msn.com	decrypted_c2
assets.msn.com	decrypted_c2
displaycatalog.mp.microsoft.com	decrypted_c2
fs.microsoft.com	decrypted_c2
realniggacheats.cc	decrypted_c2
slscr.update.microsoft.com	decrypted_c2
www.bing.com	decrypted_c2

Indicators of Compromise (60)

URLs (13)

- 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://www.microsoft.com0
- http://www.quovadis.bm0
- https://aware-cr1.com/api/beacon
- https://aware-cr1.com:443/api/beacon
- https://dev.epicgames.com/commun
- https://dev.epicgames.com/community/api/user_profiles/profile.json?hash_id=roAjr
- https://ocsp.quovadisoffshore.com0
- https://steamcommunity.com/
- https://steamcommunity.com:443/profiles/76561198652917381

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 (31)

`telegram.me`
`dev.epicgames.com`
`steamcommunity.com`
`api.msn.com`
`assets.msn.com`
`www.bing.com`
`realniggacheats.cc`
`aware-cr1.com`
`config.edge.skype.com`
`edge-consumer-static.azureedge.net`
`crl.comodo.net`
`www.microsoft.com0`
`www.quovadis.bm0`
`ocsp.quovadisoffshore.com0`
`abdev.epicgames.com`
`access.nextlsoft.com`
`amcommunity.com`
`ate.com`
`epicgames.com`
`ipv6-literal.net`
`izenpe.com`
`munity.com`
`ndowsupdate.com`
`soft.com`
`ssl.com`
`stugwarepanelv2.com`
`supdate.com`
`t.josteamcommunity.com`
`tedsteamcommunity.com`
`update.com`
...and 1 more

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
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

Decrypted C2 (TLS-MITM) (14)

```
HEAD /fs/windows/config.json  [status=501 sni=fs.microsoft.com]
GET /SLS/%7B855E8A7C-ECB4-4CA3-B045-1DFA50104289%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
GET /SLS/%7B855E8A7C-ECB4-4CA3-B045-1DFA50104289%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
HEAD /fs/windows/config.json  [status=501 sni=fs.microsoft.com]
GET /SLS/%7B855E8A7C-ECB4-4CA3-B045-1DFA50104289%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
GET /SLS/%7B855E8A7C-ECB4-4CA3-B045-1DFA50104289%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /v7.0/products/lookup?fieldsTemplate=InstallAgent&market=US&languages=en-US,en,neutral&alternateId=PackageFamily
GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.19045.6466/0?CH=812&L=en-US&P=&PT=0x30&WUA=10.0.19041.6
```

Memory-Recovered IOCs (runtime deobfuscation) (53)

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://dev.epicgames.com/commun
[url] https://dev.epicgames.com/community/api/user_profiles/profile.json?hash_id=roAjr
[url] https://ocsp.quovadisoffshore.com0
[url] https://steamcommunity.com/
[url] https://steamcommunity.com/profiles/76561198652917381
[url] https://steamcommunity.com:443/profiles/76561198652917381
[url] https://telegram.me/s11yme
[domain] abdev.epicgames.com
[domain] access.nextlsoft.com
[domain] amcommunity.com
[domain] ate.com
[domain] aware-cr1.com
```

[domain] crl.comodo.net
[domain] dev.epicgames.com
[domain] epicgames.com
[domain] ipv6-literal.net
[domain] izenpe.com
[domain] munity.com
[domain] ndowsupdate.com
[domain] ocsp.quovadisoffshore.com0

...and 28 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)
edge.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)
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)
assets.msn.com (tlsstate: deadline exceeded)
www.bing.com (tlsstate: deadline exceeded)
www.bing.com (tlsstate: deadline exceeded)
www.bing.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 224.0.0.252:5355
5. [conn] pid 0: udp 10.0.2.255:137
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: tcp 10.0.2.3:80
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 aware-cr1.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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 10.0.2.3:80
19. [conn] pid 0: udp 10.0.2.3:53
20. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
21. [conn] pid 0: tcp 10.0.2.3:443
22. [conn] pid 0: tcp 10.0.2.3:443

23. [conn] pid 0: tcp 10.0.2.3:80
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
fontdrvhost.ex - "fontdrvhost.exe"
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
winlogon.exe - winlogon.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
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=gpu-process --gpu-preferences=SAA
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
SecurityHealth - "C:\Windows\System32\SecurityHealthSystray.exe"
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=utility --utility-sub-type=entity
wlrmdr.exe - -c -s 0 -f 0 -t Empty -m Empty -a 0 -u Empty
urlhaus_e2f09c - svchost.exe
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 Appinfo
netsh.exe - netsh advfirewall set allprofiles state off

...and 20 more