KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_efda1352c4eb.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 40 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:	efda1352c4eb91fe768535abef056dacdbebc990db714eb8d62ee7fe08bc60a3
SHA-1:	34d837905dcfa4ddee75dad4f114d4f25851c9fb
MD5:	801cd7dd136454f99d15c31bb782c75d
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	7.89
.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)

```
XHx2Z
]rRich
.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$8H
|l3s|ls|lsDi
I*Ai
ssss|ls
|$ f
|$ fA
|l3s|lsH
D$8H
D$(H
\$ A
"r?L
\$`H
```

t$hH

|$pH

|ls@SH

sssss|ls

r4E3

... and 150 more

Malware Config

Indicators of Compromise (121)

URLs (50)

https://telegram.me/s11yme

https://dev.epicgames.com/community/api/user_profiles/profile.json

https://steamcommunity.com/profiles/76561198652917381

http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?

http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0

http://cert.startcom.org/intermediate.pdf0

http://cert.startcom.org/policy.pdf0

http://cert.startcom.org/policy.pdf05

http://cert.startcom.org/sfsca-crl.crl0+

http://certificates.starfieldtech.com/repository/1604

http://crl.comodo.net/AAACertificateServices.crl0

http://crl.d-trust.net/crl/d-trust_br_root_ca_1_2020.crl0y

http://crl.d-trust.net/crl/d-trust_ev_root_ca_1_2020.crl0y

http://crl.startcom.org/sfsca-crl.crl0

http://ctldl.win

http://ocsp.accv.es0

http://ocsp.suscerte.gob.ve0@

http://www.accv.e

http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0

http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0

http://www.accv.es/legislacion_c.htm0U

http://www.ancert.com/cps0

http://www.anf.es

http://www.cert.fnmt.es/dpcs/0

http://www.certicamara.com/dpc/0Z

http://www.certplus.com/CRL/class3P.crl0

http://www.certplus.com/CRL/class3TS.crl0

http://www.correo.com.uy/correocert/cps.pdf0

http://www.d-trust.net/crl/d-trust_root_class_3_ca_2_2009.crl0

http://www.defence.gov.au/pki0

...and 20 more

IPv4 addresses (21)

1.3.132.0

1.3.36.3

1.9.16.1

1.9.16.2

2.23.42.7

2.23.43.1

2.5.29.1

2.5.29.10

2.5.29.14

2.5.29.15
2.5.29.16
2.5.29.17
2.5.29.18
2.5.29.19
2.5.29.30
2.5.29.31
2.5.29.32
2.5.29.33
2.5.29.35
2.5.29.37
41.3.6.1

Domains (50)

telegram.me
dev.epicgames.com
steamcommunity.com
aware-cr1.com
assets.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net
acraiz.icpbrasil.gov.br
cert.startcom.org
certificates.starfieldtech.com
crl.comodo.net
crl.d-trust.net
crl.startcom.org
ctldl.win
ocsp.accv.es0
ocsp.suscerte.gob.ve0@
www.accv.e
www.accv.es
www.ancert.com
www.anf.es
www.cert.fnmt.es
www.certicamara.com
www.certplus.com
www.correo.com.uy
www.correo.com
www.d-trust.net
www.defence.gov.au
www.e-me.lv
www.e-szigno.hu

...and 20 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

Per-Process ATT&CK Attribution (3)

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

Proces				
NVDisplay.Cont	1144	415	T1055, T1083	
msedge.exe	4324	60	T1083	
urlhaus_efda13	4548	135	T1055	

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

Memory-Recovered IOCs (runtime deobfuscation) (121)

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

```
[url] http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?
[url] http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0
[url] http://cert.startcom.org/intermediate.pdf0
[url] http://cert.startcom.org/policy.pdf0
[url] http://cert.startcom.org/policy.pdf05
[url] http://cert.startcom.org/sfsca-crl.crl0+
[url] http://certificates.starfieldtech.com/repository/1604
[url] http://crl.comodo.net/AAACertificateServices.crl0
[url] http://crl.d-trust.net/crl/d-trust_br_root_ca_1_2020.crl0y
[url] http://crl.d-trust.net/crl/d-trust_ev_root_ca_1_2020.crl0y
[url] http://crl.startcom.org/sfsca-crl.crl0
```

[url] http://ctldl.win
[url] http://ocsp.accv.es0
[url] http://ocsp.suscerte.gob.ve0@
[url] http://www.accv.e
[url] http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0
[url] http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0
[url] http://www.accv.es/legislacion_c.htm0U
[url] http://www.ancert.com/cps0
[url] http://www.anf.es
[url] http://www.cert.fnmt.es/dpcs/0
[url] http://www.certicamara.com/dpc/0Z
[url] http://www.certplus.com/CRL/class3P.crl0
[url] http://www.certplus.com/CRL/class3TS.crl0
[url] http://www.correo.com.uy/correocert/cps.pdf0

...and 96 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)
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)
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 224.0.0.252:5355
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. [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
winlogon.exe - winlogon.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
autochk.exe - \??\C:\Windows\system32\autochk.exe *
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
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
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
urlhaus_efda13 - svchost.exe
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
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=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=utility --utility-sub-type=networ
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
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
identity_helpe - "C:\Program Files (x86)\Microsoft\Edge\Application\146.0.3856.109\identity_helper.exe" --type=utili
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
schtasks.exe - schtasks.exe /create /tn "SecurityHealthService" /xml "C:\Users\MATT~1.JOH\AppData\Local\Temp\~st0000
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start

...and 20 more