KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_3e79cc9aee9a.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 41 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Process Injection: Dynamic-link Library Injection
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- Process Discovery
- Access Token Manipulation
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	3e79cc9aee9a74b4fb131db1222d3649db21edf776e071737a0644e69c62dba6
SHA-1:	0a502d54762b6562de80ce64e549e46c4bacf8cd
MD5:	5e21d4f7b0f651bb8ec310da7c213f25
Size:	795,648 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x48630
Sections:	6

Name	Virtual Size	Entropy
.text	0x74F2C	6.47
.rdata	0x1B602	5.24

.data	0x3DC14	5.28
.pdata	0x4038	5.73
.fptable	0x100	0.0
.reloc	0xDB4	5.4

Imports

KERNEL32.dll

- LoadLibraryA
- GetProcAddress
- GetCurrentProcess
- SetEndOfFile
- QueryPerformanceCounter
- QueryPerformanceFrequency
- GetSystemTimePreciseAsFileTime
- ReleaseSRWLockExclusive
- AcquireSRWLockExclusive
- SleepConditionVariableSRW

Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich
hYtj
.text
`.rdata
@.data
.pdata
@.fptable
.reloc
\$0H
|$ H
|$ H
\$0H
\$0H
@USVWAUAVAWH
w-I;
`A_A^A]_^[]
@USVWATAUAVAWH
w L;
hA_A^A]A\_^[]
 t<H
\$8H
D$8H
D$(H
@SUVWAVH
 A^_^][
\$0H
\$0H
@SUVWAVH
 A^_^][
@SUVWAVAWH
(A_A^_^][
```

```
A'H;
SWATAUAVAW
D$pH
D$xH
T$xH
L$xH
\$xH
D$`H
T$hH
D$ L
L$hL
t$pD
D$`H
T$hH
D$ L
L$hL
T$HD
|$@D
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`135.181.127.244:80`	network

Indicators of Compromise (9)

URLs (1)

`http://135.181.127.244/`

IPv4 addresses (2)

`111.111.111.111`

`135.181.127.244`

Domains (6)

`zaa.co`

`135.181.127.244`

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

MITRE ATT&CK (10)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	

T1057	Process Discovery		pt_trace
T1134	Access Token Manipulation		pt_trace
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
svchost.exe	1004	253	T1057, T1134
svchost.exe	1564	89	T1134
0x156cac000		25	T1057

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 70/100 (high)

Factors: c2, attack_techniques

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
135.181.127.244:80		tcp
224.0.0.251:5353		udp
10.0.2.255:137		udp
10.0.2.255:138		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)
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)
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)

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: tcp 10.0.2.3:80
12. [conn] pid 0: tcp 135.181.127.244:80
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:443
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: udp 10.0.2.3:53
18. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
19. [conn] pid 0: tcp 10.0.2.3:80
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 10.0.2.3:80
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
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
urlhaus_3e79cc
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
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=networ
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
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=renderer --pdf-upsell-enabled --v

```
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
wlrmdr.exe
taskhostw.exe - taskhostw.exe SyncFromCloud
netsh.exe - netsh  advfirewall set allprofiles state off
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_s
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
```

...and 20 more