KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_0638be794bcc.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 40 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
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	0638be794bcc72c65d713483753dfd9b67a0af6095c90e0437c4e164a0eb0ec9
SHA-1:	41f3dd216ef75b51167d655993a87edc24a8bbee
MD5:	62cf91d0883273ad51ef19652e8105ab
Size:	797,696 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x48D20
Sections:	6

Name	Virtual Size	Entropy
.text	0x7561C	6.47
.rdata	0x1B62A	5.25
.data	0x3DC14	5.28
.pdata	0x4044	5.76

.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
.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
L$0H
... and 150 more

Malware Config

C2 / Network (5)

Endpoint	Source
api.msn.com	decrypted_c2
assets.msn.com	decrypted_c2
login.live.com	decrypted_c2
www.bing.com	decrypted_c2
80.76.49.106:80	network

Indicators of Compromise (11)

URLs (1)

http://80.76.49.106/

IPv4 addresses (2)

111.111.111.111
80.76.49.106

Domains (8)

zaa.co
de3.de
80.76.49.106
assets.msn.com
api.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net

MITRE ATT&CK (8)

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	
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 (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
10.0.2.3:53		udp
224.0.0.251:5353		udp
10.0.2.255:138		udp
255.255.255.255:67		udp
80.76.49.106:80		tcp
10.0.2.255:137		udp
224.0.0.252:5355		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)
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 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. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
11. [conn] pid 0: tcp 10.0.2.3:80
12. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
13. [conn] pid 0: tcp 10.0.2.3:80
14. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
15. [conn] pid 0: tcp 80.76.49.106:80
16. [http] pid 0: POST http://80.76.49.106/
17. [conn] pid 0: udp 10.0.2.3:53
18. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
19. [conn] pid 0: tcp 10.0.2.3:443
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
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
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv HwDisabZgkWXcVRq7nRwyA.0
MpCmdRun.exe - "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.26020.6-0\MpCmdRun.exe" -IdleTask -TaskName
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
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
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
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=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=renderer --pdf-upsell-enabled --v
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts

svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes

dwm.exe - "dwm.exe"

...and 20 more