KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_4a997d7569f5.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 197094 anti-VM checks (rdtsc)

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:	4a997d7569f5d3ff1b7435712afac59b83a2b91ed57bd7790b3dfb7212e652e6
SHA-1:	52fa37eaa77680b775c7a40db7b9b9a607cbac77
MD5:	4aac447303f0b8e13c93a3f7f7a6a0f1
Size:	795,136 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	0x1B582	5.27
.data	0x3DC14	5.28
.pdata	0x4038	5.72

.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 (1)

Endpoint	Source
`94.103.88.121:80`	network

Indicators of Compromise (8)

URLs (1)

`http://94.103.88.121/`

IPv4 addresses (2)

`111.111.111.111`

`94.103.88.121`

Domains (5)

`zaa.co`

`94.103.88.121`

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

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
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
94.103.88.121:80		tcp
10.0.2.255:137		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
224.0.0.251:5353		udp
255.255.255.255:67		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)
config.edge.skype.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
config.edge.skype.com  (remote error: tls: unknown certificate)
```

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 224.0.0.252:5355
7. [conn] pid 0: udp 10.0.2.255:137
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. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
12. [conn] pid 0: tcp 10.0.2.3:80
13. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt

14. [conn] pid 0: tcp 10.0.2.3:80
15. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
16. [conn] pid 0: tcp 94.103.88.121:80
17. [http] pid 0: POST http://94.103.88.121/
18. [conn] pid 0: tcp 10.0.2.3:80
19. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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: udp 10.0.2.3:53
25. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3

...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
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
Registry
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
smss.exe - \SystemRoot\System32\smss.exe
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
taskhostw.exe - taskhostw.exe SyncFromCloud
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
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=renderer --pdf-upsell-enabled --v
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=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=utility --utility-sub-type=entity
netsh.exe - netsh advfirewall set allprofiles state off
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
lsass.exe - C:\Windows\system32\lsass.exe

...and 20 more