KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_dff83bede85f.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 158557 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:	dff83bede85f33f1229e21cabc1b159f8b11230c9b4b6d2e46432d7094c7a917
SHA-1:	cb60dc8be2fe05517280d77bbe3415979f339840
MD5:	68151cd3c5175750d58735083f381838
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	5.26
.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
`31.77.228.62:80`	network

Indicators of Compromise (9)

URLs (1)

- `http://31.77.228.62/`

IPv4 addresses (2)

- `111.111.111.111`
- `31.77.228.62`

Domains (6)

- `zaa.co`
- `31.77.228.62`
- `assets.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
10.0.2.255:138		udp
224.0.0.252:5355		udp
224.0.0.251:5353		udp
31.77.228.62:80		tcp
255.255.255.255:67		udp
10.0.2.255:137		udp

TLS Handshake Failures (cert-pinning) (50)

```
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
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)
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. [conn] pid 0: udp 224.0.0.252:5355
11. [conn] pid 0: tcp 10.0.2.3:80

12. [conn] pid 0: tcp 31.77.228.62:80
13. [conn] pid 0: tcp 10.0.2.3:80
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: tcp 10.0.2.3:443
18. [conn] pid 0: udp 10.0.2.3:53
19. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
lsass.exe
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
csrss.exe
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=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=gpu-process --gpu-preferences=SAA
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
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
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=utility --utility-sub-type=edge_s
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
taskhostw.exe - taskhostw.exe SyncFromCloud
wlrmdr.exe
SppExtComObj.E
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
fontdrvhost.ex - "fontdrvhost.exe"

...and 20 more