KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_d490ac7dc085.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
- Obfuscated Files or Information
- 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:	d490ac7dc0854bea4728b0a4497727fdf74a8b1a4a9dc10d040c71b1814586bd
SHA-1:	ff3e5cedae56fe0e1b14778cf794423eaaba0b9c
MD5:	a5b8225d8a618c9e702ef6bf81668cba
Size:	647,168 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x1EED0
Sections:	5

Name	Virtual Size	Entropy
.text	0x5922A	6.69
.rdata	0x142CE	5.45
.data	0x3C7E4	5.34

.fptable	0x80	0.0
.reloc	0x47F8	6.74

Imports

KERNEL32.dll

- LoadLibraryA
- GetProcAddress
- GetCurrentProcess
- HeapSize
- QueryPerformanceCounter
- QueryPerformanceFrequency
- GetSystemTimePreciseAsFileTime
- Sleep
- GetCurrentThreadId
- WideCharToMultiByte

Strings (200 found)

```
!This program cannot be run in DOS mode.
1Rich=
.text
`.rdata
@.data
.fptable
.reloc
t&VW
v$VQPS
3WQPS
VQPS
+QPW
_^[]
RQVSQ
_^[]
Wh<vF
_^[]
QSVW
YY_[^
YY[kE
WjdRP
SWVRP
YY_^
6SVQRQ
_^[]
t,VS
SVWQ
6PVQ
v@Ph@B
YY_^
VWu)
F(^[
4OVW
t(VW
```

U8V3
st+}
=WRQP
>_^[]
SVWj
_^[]
wJ9G
^_[]
wP;G
rhRj
VQPS
YYQf
uIh=1
uZhx
X4uJ
uIh=1
... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
193.148.56.206:80	network

Indicators of Compromise (9)

URLs (1)

http://193.148.56.206/

IPv4 addresses (2)

111.111.111.111
193.148.56.206

Domains (6)

zaa.co
193.148.56.206
assets.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net

MITRE ATT&CK (9)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
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
193.148.56.206:80		tcp
224.0.0.251:5353		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
10.0.2.255:138		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)
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 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. [conn] pid 0: tcp 10.0.2.3:80

12. [conn] pid 0: tcp 193.148.56.206:80
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 (4)

System
Registry
smss.exe - \SystemRoot\System32\smss.exe
autochk.exe - \??\C:\Windows\system32\autochk.exe *