KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_a1e17215620c.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1027.002
- T1497.001
- T1105
- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Application Layer Protocol: Web Protocols
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	a1e17215620c5d6344e4708cade11bcc22581d5a023d053d6622c6b9801c8717
SHA-1:	35ee6d522ca63517c9d758ab5420782c48a77650
MD5:	82bdb4f9e0d54ae25436306c472a1839
Size:	8,437,632 bytes

Packer Detection

Packer:	Unknown packer (high entropy in .rdata)
Confidence:	medium

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x75400
Sections:	9

Name	Virtual Size	Entropy
.text	0x153B51	6.3

.rdata	0x64A3E8	7.58
.data	0x6CF48	4.8
.pdata	0x5CC4	5.26
.xdata	0xB4	1.78
.idata	0x53E	3.98
.reloc	0x4D0C	5.41
.symtab	0x23E70	5.14
.rsrc	0x1A358	7.98

Imports

kernel32.dll

- WriteFile
- WriteConsoleW
- WerSetFlags
- WerGetFlags
- WaitForMultipleObjects
- WaitForSingleObject
- VirtualQuery
- VirtualFree
- VirtualAlloc
- TlsAlloc

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rdata
@.data
.pdata
@.xdata
@.idata
.reloc
B.symtab
B.rsrc
 Go build ID: "bTbITfQBrVkhlxECSntm/QOuXAf8tYBAzvN4MXVeG/zx7Kuymr6F8-QArw5Uy6/_PuvaxhobqInEDeYCfbY"
|$XL
T$xH
T$`L
L$hE
t$OL
d$pH
L$pf
|$hL
\$EH9
L$pH
|$hH
t$xH9
t$XH9
|$`L
\$;H9
L$PH
```

T$xH
D$PH
L$xH9
|$`I
wDH)
|$ @
t$(D
t$(D
l$ M9,$u
M9,$u
v,UH
D$ H
D$ H
8cpu.u
D$PH
t$pH
L$HH
\$`H)
\$ M
\$XH
onuzH
ofu]F
fuQH
... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
135.181.127.244:80	network

Indicators of Compromise (5)

IPv4 addresses (1)

135.181.127.244

Domains (4)

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

MITRE ATT&CK (10)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1105			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	

T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1071.001	Application Layer Protocol: Web	Command and Control	behavioral_inference
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 40/100 (medium)

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
10.0.2.255:138		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
135.181.127.244:80		tcp
224.0.0.251:5353		udp

TLS Handshake Failures (cert-pinning) (50)

```
www.bing.com  (tlsstate: deadline exceeded)
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)
edge.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)
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 255.255.255.255:67
2. [conn] pid 0: udp 10.0.2.255:137
3. [conn] pid 0: udp 224.0.0.251:5353
4. [conn] pid 0: udp 224.0.0.252:5355
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3

7. [conn] pid 0: tcp 10.0.2.3:80
8. [conn] pid 0: tcp 10.0.2.3:80
9. [conn] pid 0: tcp 10.0.2.3:80
10. [conn] pid 0: tcp 135.181.127.244:80
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: tcp 10.0.2.3:443
15. [conn] pid 0: udp 10.0.2.3:53
16. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: tcp 10.0.2.3:80
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 netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
smss.exe - \SystemRoot\System32\smss.exe
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
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
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
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=crashpad-handler "--user-data-dir
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" --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=gpu-process --gpu-preferences=SAA
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
netsh.exe - netsh advfirewall set allprofiles state off
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
fontdrvhost.ex - "fontdrvhost.exe"

```
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
```

...and 20 more