KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_d7aaced4338f.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 77 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Process Injection: Dynamic-link Library Injection
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	d7aaced4338fe732409d552c6ddf9cf3f7776b272d1c0e56b83af8b46438722d
SHA-1:	93ef1574324343108421c056a1319a6a924ea4d8
MD5:	c541eb0729da58fed7d1ccc05f9c0409
Size:	5,735,256 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x66140
Sections:	6

Name	Virtual Size	Entropy
.text	0x1ED238	6.15
.rdata	0x338CE8	4.73
.data	0x39208	5.17
.idata	0x45E	3.9

.reloc	0x12398	6.73
.symtab	0x2ED03	5.16

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
.idata
.reloc
B.symtab
 Go build ID: "ZAUcHocWlI28ZRzTqqPi/_wHMenX5K9nqlRUg3P_k/REI5lxLS0Z_tEat9vNKT/8FgEwJgz7JPogOow4N4u"
l$J9
t$d9
l$`9
D$,9
l$<)
T$@9
L$<9
T$(9
L$h9
;cpu.u
t$4)
?onua
?ofuP
9fuG
>alu
\$(1
L$,1
D$ 9
T$#!
J$9H$
J(9H(u|
J,8H,us
J-8H-uj
J49H4ub
J89H8uZ
J<8H<uQ
```

J=8H=uH
JD9HDu@
JH9HHu8
JL8HLu/
JM8HMu&
HT9JTu
JX9HXu
J\8H\u
J]8H]u
l$<1
T$41
\$89
\$89
t$<)
D$$5
D$$5
... 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
95.135.181.73:80	network

Indicators of Compromise (9)

URLs (1)

http://95.135.181.73/

IPv4 addresses (1)

95.135.181.73

Domains (7)

aaa.ga
95.135.181.73
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	
T1082	System Information Discovery	Discovery	

T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
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
224.0.0.251:5353		udp
95.135.181.73:80		tcp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
10.0.2.255:138		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 224.0.0.252:5355
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 10.0.2.3:80
13. [conn] pid 0: tcp 95.135.181.73:80
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
lsass.exe - C:\Windows\system32\lsass.exe
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
svchost.exe - C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
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
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
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
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
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
```

```
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
```

...and 20 more