KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_b038b23220a6.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 36 anti-VM checks (mixed)

Analysis Overview

Score: 8/10

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:	b038b23220a6948af729f5fe9243481ab0a16e8a27378c08e1bc6eb51c7398ac
SHA-1:	cfae11ef7a6a46d3cc47f8455afc49c02a726c66
MD5:	56b09b7356441f70f08737347734f13d
Size:	5,162,848 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x750B0
Sections:	6

Name	Virtual Size	Entropy
.text	0x178C76	5.99
.rdata	0x338AE4	4.0
.data	0x2D7DC	5.36
.idata	0x44C	3.88

.reloc	0x143C8	6.73
.symtab	0x1C52F	5.08

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: "U5CgDLGViVZ1_FKENsUz/kXQ09iIx1ffVMmmbp9n-/oMYno71fEFZLcWBf5tpX/m4pa5WGWANnEZ_kRPeQO"
l$19
t$d9
l$`9
D$@9
l$P)
T$'9
L$P9
T$<9
L$h9
;cpu.u
t$4)
?onua
?ofuP
9fuG
>alu
\$(1
D$ 9
\$#!
\$"!
H$9J$
H(9J(
H,8J,
H-8J-
J49H4
H89J8u|
H<8J<us
```

```
H=8J=uj
HD9JDub
HH9JHuZ
HL8JLuQ
HM8JMuH
JT9HTu@
HX9JXu8
H\8J\u/
H]8J]u&
Hd9Jdu
Hh9Jhu
Hl8Jlu
Hm8Jmu
\$$!
T$D9
D$,1
```

... and 150 more

Malware Config

Indicators of Compromise (10)

URLs (2)

```
https://dns.google/dns-query
https://cloudflare-dns.com/dns-query
```

IPv4 addresses (2)

```
8.8.8.8
1.1.1.1
```

Domains (6)

```
dns.google
cloudflare-dns.com
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	
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: 80/100 (high)

Factors: c2, beaconing, attack_techniques

C2 beaconing: 1

Network Connections (12)

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
8.8.4.4:443		tcp
8.8.8.8:443		tcp
1.1.1.1:443		tcp
1.0.0.1:443		tcp
224.0.0.252:5355		udp
10.0.2.255:138		udp
10.0.2.255:137		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)
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 224.0.0.251:5353
3. [conn] pid 0: udp 224.0.0.252:5355
4. [conn] pid 0: udp 10.0.2.255:137
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 8.8.8.8:443
10. [conn] pid 0: tcp 8.8.4.4:443
11. [conn] pid 0: tcp 1.1.1.1:443
12. [conn] pid 0: tcp 1.0.0.1:443
13. [conn] pid 0: tcp 8.8.8.8:443
14. [conn] pid 0: tcp 8.8.4.4:443
15. [conn] pid 0: tcp 1.1.1.1:443
16. [conn] pid 0: tcp 1.0.0.1:443
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: udp 10.0.2.3:53
19. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: tcp 10.0.2.3:443
22. [conn] pid 0: udp 10.0.2.3:53
23. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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)

dwm.exe - "dwm.exe"
System
wininit.exe - wininit.exe
Registry
services.exe - C:\Windows\system32\services.exe
winlogon.exe - winlogon.exe
smss.exe - \SystemRoot\System32\smss.exe 000000d8 00000088
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
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" --type=utility --utility-sub-type=entity
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
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
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=networ
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
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
wlrmdr.exe
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_s
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
SecurityHealth - "C:\Windows\System32\SecurityHealthSystray.exe"

...and 20 more