KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_124cf79f222e.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 129 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- File and Directory Discovery
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	124cf79f222ef8b88f4d0e2e474378c5a7ab8a3c513d2434037ef0acfd79c984
SHA-1:	c23d33b86e22f305fd600145f27f6a9522e29cc0
MD5:	ff1b216b6ef02dceda621ca45ed4f0c3
Size:	3,242,496 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x7FBA0
Sections:	9

Name	Virtual Size	Entropy
.text	0xDBBB1	6.27
.rdata	0x202030	6.99
.data	0x65EA8	3.43
.pdata	0x60CC	5.18

.xdata	0xA8	1.69
.idata	0x55A	4.08
.reloc	0x6058	5.41
.symtab	0x4	0.02
.rsrc	0x108E8	1.5

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: "qwvdHpNHBiZc9nxpy7ZM/FIClHgLmWAqY1coIYJf3/lu8oSHehOla53VT9ssQV/yLUDwgkOdgg0uGF1scJV"
|$XH
\$xL
T$`L
L$hE
t$OL
d$pH
L$pf
|$hL
\$EH9
L$pH
|$hH
t$XH9
|$xH)
|$`L
\$;f
L$PH
T$xH
T$PH
t$xH9
|$`I
```

```
wDH)
|$ @
t$(D
t$(D
v=UH
D$ H
D$ H
8cpu.u
|$PH
T$pH
D$HL
T$`H)
\$ M
\$XH
onuzH
ofu]F
fuQH
t$@1
D$XH
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`62.60.226.232:80`	network

Indicators of Compromise (7)

URLs (1)

`http://62.60.226.232/zpzp/get.php`

IPv4 addresses (1)

`62.60.226.232`

Domains (5)

`62.60.226.232`
`api.msn.com`
`assets.msn.com`
`www.bing.com`
`arc.msn.com`

MITRE ATT&CK (8)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1083	File and Directory Discovery		pt_trace
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (3)

Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).

Proces				
0x14671a000		373	T1083	
explorer.exe	4172	825	T1055, T1057	
0x1436f0000		143	T1057	

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 70/100 (high)

Factors: c2, dropped_exe, attack_techniques

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
62.60.226.232:80		tcp
10.0.2.3:53		udp
224.0.0.251:5353		udp
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)
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)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.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: udp 10.0.2.3:53
9. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
10. [conn] pid 0: tcp 10.0.2.3:443
11. [conn] pid 0: udp 10.0.2.3:53
12. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:80
14. [conn] pid 0: tcp 10.0.2.3:80
15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:443
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 10.0.2.3:443
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 10.0.2.3:443
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 DcomLaunch -p
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
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
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
netsh.exe - netsh  advfirewall set allprofiles state off
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s SstpSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv rgDGNrf//EOFo+oWjn0Eag.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
```

svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes

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

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

dwm.exe - "dwm.exe"

...and 20 more