KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_18df0ec2efba.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1027.002
- T1497.001
- T1071.001
- Obfuscated Files or Information
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading

Hashes

SHA-256:	18df0ec2efba162d1774b1bf2233c2c24934d2bda49769e814f24d530a795c38
SHA-1:	01eadc4c72792e9f3aa96f3bff5c2f56f2a04081
MD5:	eff677e44d0f001884e2982bb451d1af
Size:	3,930,624 bytes

Packer Detection

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

PE Information

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

Name	Virtual Size	Entropy
.text	0xDBBB1	6.27
.rdata	0x2AA1B0	7.34
.data	0x65EA8	3.43
.pdata	0x60CC	5.18

.xdata	0xA8	1.69
.idata	0x55A	4.02
.reloc	0x6050	5.41
.symtab	0x4	0.02
.rsrc	0x108E8	3.52

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: "XWPlv5iaoPiT0wXamK32/P5yNDnNXSx50soDELq81/hhbvZ-hBAyKbslZXxrl1/M2HMD_n2zVSlZOKSkPAt"
5K$9
|$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
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`192.162.199.186:80`	network

Indicators of Compromise (7)

URLs (1)

`http://192.162.199.186/zpzp/get.php`

IPv4 addresses (1)

`192.162.199.186`

Domains (5)

`192.162.199.186`
`api.msn.com`
`assets.msn.com`
`www.bing.com`
`arc.msn.com`

MITRE ATT&CK (7)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	

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
255.255.255.255:67		udp
10.0.2.3:53		udp
192.162.199.186:80		tcp
10.0.2.255:137		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
224.0.0.251:5353		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)
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)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.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)
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 224.0.0.252:5355
5. [conn] pid 0: udp 10.0.2.255:137
6. [conn] pid 0: udp 224.0.0.252:5355
7. [conn] pid 0: udp 10.0.2.3:53
8. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
9. [conn] pid 0: tcp 10.0.2.3:80
10. [conn] pid 0: udp 10.0.2.3:53
11. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3

12. [conn] pid 0: tcp 10.0.2.3:443
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:80
17. [conn] pid 0: tcp 10.0.2.3:80
18. [conn] pid 0: tcp 10.0.2.3:443
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 10.0.2.3:443
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 10.0.2.3:443

...and 75 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
wininit.exe - wininit.exe
Registry
winlogon.exe - winlogon.exe
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
smss.exe - \SystemRoot\System32\smss.exe
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
sppsvc.exe - C:\Windows\system32\sppsvc.exe
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv zab7isi3Z0W/g6ASK/wopA.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
```

...and 20 more