KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_13fbe68c0d4a.exe

Verdict: LIKELY-MALICIOUS

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

Analysis Overview

Score: 8/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1571
- Application Layer Protocol: Web Protocols
- Dynamic Resolution
- Process Discovery
- Scheduled Task/Job: Scheduled Task

Hashes

SHA-256:	13fbe68c0d4a0927657b0b28eee50ab13aa13de7a250416f4a15150154250111
SHA-1:	db5b321d7cb55d5081b342f3894549608ff02859
MD5:	6dd7bd55e4471a6f724f2ed3a29c54ff
Size:	1,071,616 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x10694E
Sections:	3

Name	Virtual Size	Entropy
.text	0x104954	5.54
.rsrc	0xA47	4.49
.reloc	0xC	0.1

Imports

mscoree.dll

_CorExeMain

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
 )UU
X )UU
X )UU
LaU*
?_d`*F
?_b`*
8b`*
*.sX
6?(I
*Fr}
-&r[
pr<O
+rKP
*ZrqP
*.s-
*.sH
+*vs
prSS
,R+t
&*o3
&*o3
+*.s
+*.s
*.sv
%- &~
&&~
&%rv
,ZsF
,ZsR
,Zs(
-(sa
`AsA
`,X(-
-*(#
.4+o
[X(9
*.s^
Y*.~K
p*r,
Zi(7
.ts9
iX(f
*.sQ
*6sy
*Js?
```

. +&

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
217.195.153.81:50000	network

Indicators of Compromise (6)

IPv4 addresses (1)

217.195.153.81

Domains (5)

paint.net

api.msn.com

assets.msn.com

www.bing.com

arc.msn.com

MITRE ATT&CK (6)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1571			detonation-evidence
T1071.001	Application Layer Protocol: Web	Command and Control	
T1568	Dynamic Resolution	Command and Control	
T1057	Process Discovery		pt_trace
T1053.005	Scheduled Task/Job: Scheduled Ta	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (6)

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

Proces				
0x15606f000		376	T1057	
lsass.exe	652	129	T1055, T1057	
svchost.exe	1016	98	T1055	
0x14366f000		79	T1057	
NVDisplay.Cont	1200	400	T1055	
taskhostw.exe	3008	19	T1083	

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 85/100 (high)

Factors: c2, beaconing, attack_techniques

C2 beaconing: 1

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
10.0.2.3:53		udp
10.0.2.255:138		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
217.195.153.81:50000		tcp
10.0.2.255:137		udp
224.0.0.251:5353		udp

TLS Handshake Failures (cert-pinning) (50)

```
login.live.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.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)
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 224.0.0.252:5355
 7. [conn] pid 0: udp 10.0.2.255:137
 8. [conn] pid 0: udp 224.0.0.252:5355
 9. [conn] pid 0: udp 10.0.2.3:53
10. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
11. [conn] pid 0: tcp 10.0.2.3:80
12. [conn] pid 0: udp 10.0.2.3:53
13. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
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 10.0.2.3:443
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)

Spawned Processes (50)

```
System
Registry
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
fontdrvhost.ex - "fontdrvhost.exe"
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
jsc.exe - "C:\Windows\Microsoft.NET\Framework\v4.0.30319\jsc.exe"
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
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
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
schtasks.exe - "schtasks.exe" /query /tn "SystemHealthMonitor"
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=networ
RuntimeBroker.
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
```

...and 20 more