KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_565110ae685e.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 119 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
- File and Directory Discovery
- Scheduled Task/Job: Scheduled Task

Hashes

SHA-256:	565110ae685e0248e3ed684c859ccd1cc092c3ad1aa6a05fbfbefb10af46583b
SHA-1:	9426e24435e9ebd360362d15c408df8cb2ea21db
MD5:	27139922a7ac56aa3e54591cbf8e21bd
Size:	1,073,664 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	0x1393	5.2
.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	
T1083	File and Directory Discovery		pt_trace
T1053.005	Scheduled Task/Job: Scheduled Ta	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
0x142dda000		297	T1083
explorer.exe	4240	982	T1055, T1057, T1083
NVDisplay.Cont	1208	558	T1055

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
`10.0.2.3:80`		`tcp`
`10.0.2.3:443`		`tcp`

224.0.0.251:5353		udp
224.0.0.252:5355		udp
217.195.153.81:50000		tcp
10.0.2.255:137		udp
255.255.255.255:67		udp
10.0.2.3:53		udp
10.0.2.255:138		udp

TLS Handshake Failures (cert-pinning) (50)

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)
www.bing.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)
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 224.0.0.252:5355
6. [conn] pid 0: udp 10.0.2.255:137
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
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
dwm.exe - "dwm.exe"
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d855 /state1:0x41c64e6d
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctm
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
urlhaus_565110 - "C:\Users\Public\Downloads\urlhaus_565110ae685e.exe"
msedge.exe
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
cmd.exe - C:\Windows\system32\cmd.exe /c ""C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\fire_loader.
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=networ
sppsvc.exe - C:\Windows\system32\sppsvc.exe
netsh.exe - netsh  advfirewall set allprofiles state off
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv mJ4pD2zEiUuoLj3CPA4Yqw.0
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
```

...and 20 more