KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_b7fd8d6dddf0.exe

Verdict: LIKELY-MALICIOUS

Verdict: likely-malicious; 78 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Likely malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- Process Injection

Hashes

SHA-256:	b7fd8d6dddf0e4321dd5303ecd50d4a9d833ab4a80e0a01face12116363a8103
SHA-1:	873421118a0984c7f3a8cccac26f3bd010e70f2f
MD5:	65290a0084c07a7c3916db8bc86a16ac
Size:	1,090,048 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0xEE5F0
Sections:	4

Name	Virtual Size	Entropy
.text	0x101D7B	5.65
.rdata	0x6954	5.83
.data	0x11BAC0	1.17
.reloc	0x14	0.23

Strings (200 found)

```
!This program cannot be run in DOS mode.
C!Rich
```

```
.text
`.rdata
@.data
.reloc
@USVWATAVAWH
'm>H
E@H3
EwxNm
H9}X
H9}XvBH
L;}Xr
pA_A^A\_^[]
USVWATAUAVAWH
\$XH
D$`2
D$dza::
D$te
D$X3
L$PI
\$HH
|$@L
D$8M
D$0H
\$(H
\$HH
|$@L
D$8M
D$0H
\$(H
\$HH
|$@L
D$8M
D$0H
\$(H
L$PH
L$PL;
D$x+>
D$Pj
A_A^A]A\_^[]
L$ H
USVWAUAVH
t$`M
\$XM
D$PI
phH+
D$PH3
D$PH+
D$PE
```

... and 150 more

Malware Config

Indicators of Compromise (50)

URLs (11)

https://sot.tbo88men.top/
https://t.me/np33yk
https://steamcommunity.com/profiles/76561198671804195
http://crl.comodo.net/AAACertificateServices.crl0
http://www.microsoft.com0
http://www.quovadis.bm0
https://ocsp.quovadisoffshore.com0
https://sot.tbo88men.top
https://steamcommunity.com/
https://steamcommunity.com:443/profiles/76561198671804195
https://t.me/

IPv4 addresses (16)

1.3.132.0
1.3.36.3
1.9.16.1
1.9.16.2
2.23.43.1
2.5.29.1
2.5.29.10
2.5.29.14
2.5.29.15
2.5.29.17
2.5.29.19
2.5.29.31
2.5.29.32
2.5.29.35
2.5.29.37
41.3.6.1

Domains (23)

mljomjl.ml
sot.tbo88men.top
t.me
steamcommunity.com
api.msn.com
assets.msn.com
www.bing.com
arc.msn.com
crl.comodo.net
www.microsoft.com0
www.quovadis.bm0
ocsp.quovadisoffshore.com0
access.nextlsoft.com
ate.com
ipv6-literal.net
izenpe.com
munity.com
ndowsupdate.com
ssl.com
stugwarepanelv2.com
t.josteamcommunity.com
tbo88men.top
www.stugwarepanelv2.com

MITRE ATT&CK (3)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1055	Process Injection		pt_trace

Per-Process ATT&CK Attribution (1)

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

				Proces
urlhaus_b7fd8d	4656	87	T1055	

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 70/100 (high)

Factors: c2, attack_techniques

Network Connections (8)

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

Memory-Recovered IOCs (runtime deobfuscation) (45)

Decoded from guest memory at the hypervisor - recovered from obfuscation static analysis cannot unpack.

```
[url] http://crl.comodo.net/AAACertificateServices.crl0
[url] http://www.microsoft.com0
[url] http://www.quovadis.bm0
[url] https://ocsp.quovadisoffshore.com0
[url] https://sot.tbo88men.top
[url] https://sot.tbo88men.top/
[url] https://steamcommunity.com/
[url] https://steamcommunity.com/profiles/76561198671804195
[url] https://steamcommunity.com:443/profiles/76561198671804195
[url] https://t.me/
[url] https://t.me/np33yk
[domain] access.nextlsoft.com
[domain] ate.com
[domain] crl.comodo.net
[domain] ipv6-literal.net
[domain] izenpe.com
[domain] munity.com
[domain] ndowsupdate.com
```

[domain] ocsp.quovadisoffshore.com0
[domain] sot.tbo88men.top
[domain] ssl.com
[domain] steamcommunity.com
[domain] stugwarepanelv2.com
[domain] t.josteamcommunity.com
[domain] t.me
...and 20 more

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 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
wininit.exe - wininit.exe
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s SstpSvc
winlogon.exe - winlogon.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
smss.exe - \SystemRoot\System32\smss.exe 000000dc 00000084
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe - \SystemRoot\System32\smss.exe
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv AHB0Vs+XzE63mBX8dgZk/g.0
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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
msedge.exe
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
SecurityHealth
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=gpu-process --gpu-preferences=SAA
taskhostw.exe
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
SIHClient.exe - C:\Windows\System32\sihclient.exe  /cv AHB0Vs+XzE63mBX8dgZk/g.0.2
netsh.exe - netsh  advfirewall set allprofiles state off
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
wlrmdr.exe
svchost.exe - C:\Windows\system32\svchost.exe -k UnistackSvcGroup
fontdrvhost.ex - "fontdrvhost.exe"
```

...and 20 more