KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_f0e29d11e180.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 792 anti-VM checks (mixed)

Analysis Overview

Score: 3/10

Threat level: Suspicious

Malicious Activity Summary

- Sandbox-evasion / anti-VM probing observed
- T1027.002
- T1497.001
- Obfuscated Files or Information
- Virtualization/Sandbox Evasion

Hashes

SHA-256:	f0e29d11e1800cf4ef616458f74cd3cfccd0e39559423344e92574fc78023259
SHA-1:	7ef9a8e90e0f3dc0f51d87eec0fc00716e572e71
MD5:	930114eafd4d5b3b863c795bb99e9ce5
Size:	302,080 bytes

Packer Detection

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

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x10E0
Sections:	1

Name	Virtual Size	Entropy
.text	0x48C00	7.99

Strings (200 found)

```
!This program cannot be run in DOS mode.
5Rich
```

```
.text
D$ Yp
D$$k
D$9f
D$?3
@USVWH
@09H
$^I;
fffff
ffffff
C:D+
?qfH
D$0$
D$8H
D$ H
D$(H
D$0H
D$8H
_^[]
'RuH
D$*H
D$:f
D$>f
5Hk{
0'|;C
D$@I
sFffff
_^[]
_^[]
tyL+
_^[]
|$ UH
@09H
@82t'L
A88u
;Ctu
`I;C
D$!f
D$'H
y|;K
D$(N
L< H
D$ axkg
D$$fnaoH
D$(&mpmfffff
L< H
pu[H
{.9{.t
```

... and 150 more

Indicators of Compromise (4)

Domains (4)

```
api.msn.com
```

assets.msn.com
www.bing.com
arc.msn.com

MITRE ATT&CK (4)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1497	Virtualization/Sandbox Evasion	Defense Evasion	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: evasion, attack_techniques

Sandbox evasion (T1497)

Dynamic: 52 descriptor-table red-pill spoof(s) (SIDT/SGDT) with no payload executed ? sandbox-evasion bail

Network Connections (8)

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

TLS Handshake Failures (cert-pinning) (50)

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

...and 75 more events

Packet capture: available (full PCAP)

Spawned Processes (25)

System
Registry
smss.exe - \SystemRoot\System32\smss.exe
sc.exe
UsoClient.exe
ClipESUConsume
RuntimeBroker.
SearchApp.exe
mobsync.exe
sppsvc.exe
msedge.exe
rundll32.exe
taskhostw.exe
svchost.exe
upfc.exe
NVDisplay.Cont
dwm.exe
smss.exe - \SystemRoot\System32\smss.exe 000000bc 00000084
csrss.exe
smss.exe - \SystemRoot\System32\smss.exe 000000d8 00000084
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
conhost.exe

```
urlhaus_f0e29d
explorer.exe
SppExtComObj.E
```