KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_438a199c6002.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 117 anti-VM checks (mixed)

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1027.002
- T1497.001
- T1071.001
- Obfuscated Files or Information
- Process Injection

Hashes

SHA-256:	438a199c60026b897fdda4da23d69e103cad34864a070d1b7659cf462628505f
SHA-1:	bf119129aa816d95af82b5ed9194aaba52b0d90f
MD5:	e0bf699a9016ef9a7740953c6ec4feb0
Size:	284,672 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x26C0
Sections:	1

Name	Virtual Size	Entropy
.text	0x44800	7.99

Strings (200 found)

```
MZER
!This program cannot be run in DOS mode.
```

```
Rich
.text
zGGG
FGGG
TT|5i
52,1
Pt;Q8s=
5DV$
Jt;H8
Jt;H|
a\K_^
(;.<
_F.A
uDJP
zWtL
;ELT6
8IVp
KP;F
mcIT
F6=?
{sP7
6Yo6
R]I_
tF3I
We^|,
oL&l
7i9`3r
in>i
5P"G
$_06
{r2H
KH>z
/%U;
&6k)
-eV3W<
[uxC
)e@{
k+wH
23n4
kDu.
r[/-
EEJ]e
R[o7
caQg
RPB\
IOeNq
_`Ola0
?R4r
```

... and 150 more

Malware Config

Indicators of Compromise (26)

URLs (11)

`http://www.columbia.edu/ou2w/`
`http://www.lmarguerite.one/1o4u/`
`http://www.ivi.ru/s7gr/`
`http://www.hydrarain.com/h1mx/`
`http://www.teamswanborn.nl/fp78/`
`http://www.xston.site/w05h/`
`http://www.bridgerits.dev/3ftu/`
`http://www.rocketwash.online/7uq0/`
`http://www.promptfile.com/hicb/`
`http://www.jinrichiguar6.cc/2y8v/`
`http://www.akue.fr/9w2k/`

Domains (15)

`www.columbia.edu`
`www.lmarguerite.one`
`www.ivi.ru`
`www.hydrarain.com`
`www.teamswanborn.nl`
`www.xston.site`
`www.bridgerits.dev`
`www.rocketwash.online`
`www.promptfile.com`
`www.jinrichiguar6.cc`
`www.akue.fr`
`api.msn.com`
`assets.msn.com`
`www.bing.com`
`arc.msn.com`

MITRE ATT&CK (5)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
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
NVDisplay.Cont	1228	11	T1055	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 40/100 (medium)

Factors: c2, attack_techniques

Network Connections (8)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
224.0.0.252:5355		udp
10.0.2.3:53		udp
224.0.0.251:5353		udp
10.0.2.255:137		udp
255.255.255.255:67		udp
10.0.2.255:138		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)
login.live.com  (tlsstate: deadline exceeded)
www.bing.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)
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
fontdrvhost.ex - "fontdrvhost.exe"
wininit.exe - wininit.exe
Registry
lsass.exe - C:\Windows\system32\lsass.exe
dwm.exe - "dwm.exe"
winlogon.exe - winlogon.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
smss.exe - \SystemRoot\System32\smss.exe
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
winrs.exe - "C:\Windows\SysWOW64\winrs.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
slui.exe - "C:\Windows\System32\SLUI.exe" RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c9
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
msedge.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k UnistackSvcGroup
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
BdeUISrv.exe - C:\Windows\System32\BdeUISrv.exe -Embedding
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.IrisService.AppXwt29n3t7x7q6fgyrrbb
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
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
taskhostw.exe
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
sppsvc.exe - C:\Windows\system32\sppsvc.exe
cmd.exe
```

...and 20 more