KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_23a856800376.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 277 anti-VM checks (mixed)

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1027.002
- T1497.001
- T1071.001
- T1105
- Obfuscated Files or Information
- Process Injection
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	23a8568003768b2f4e2fc3bd47a6d6d054c11ce622737d27df4c4f1bb0c28146
SHA-1:	11af95f07370e84620ebb8d0feca1920035bf3f7
MD5:	e21fe731e011bcf0a181f2c894da220b
Size:	284,160 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	0x44600	7.99

Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich
.text
;Pau
Pt;Q<sD
Jt;H<
Jt;H,
xF_^
@c76U
>W}.a
3IU8
R8J9
e2 H$
n/^p
4#n5
PsD!
+Z Z
,][n
N`tu>X
z)6
H:hT
#P>/
F31T
K|.wI+
(}X4
x0U1
XIhg
f5AI
\hr2
KT)C^
>Bib
tM@4
cib1
(+FU`@
[gjl
UHnE
IN:XZP
ZYsN'
q1{I
XDGj
jk>B
0^90d
5Ez3
V Np
$^(n
[$J!
t/2\H
_H=J
Lf3Y
QlxDX'Q$
```

... and 150 more

Malware Config

C2 / Network (5)

Endpoint	Source
api.msn.com	decrypted_c2
assets.msn.com	decrypted_c2
config.edge.skype.com	decrypted_c2
displaycatalog.mp.microsoft.com	decrypted_c2
www.bing.com	decrypted_c2

Indicators of Compromise (21)

URLs (8)

- http://www.030085435.xyz/rm3c/
- http://www.ferraz-shawmut.ru/2jt4/
- http://www.ydh7444333a10.shop/u6bf/
- http://www.bsxdj.vip/2b55/
- http://www.goexpress20.com/7oyw/
- http://www.arwaterfowlstudio.com/rfr2/
- http://www.lumberpa.com/w3hj/
- http://www.kosmulska.org/o6rq/

Domains (13)

- www.030085435.xyz
- www.ferraz-shawmut.ru
- www.ydh7444333a10.shop
- www.bsxdj.vip
- www.goexpress20.com
- www.arwaterfowlstudio.com
- www.lumberpa.com
- www.kosmulska.org
- assets.msn.com
- www.bing.com
- api.msn.com
- config.edge.skype.com
- edge-consumer-static.azureedge.net

MITRE ATT&CK (7)

Technique	Name	Tactic	Source
T1027.002			detonation-evidence
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1055	Process Injection		pt_trace
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

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	1212	852	T1055	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 45/100 (medium)

Factors: c2, attack_techniques

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
10.0.2.3:53		udp
224.0.0.252:5355		udp
255.255.255.255:67		udp
224.0.0.251:5353		udp
10.0.2.255:137		udp
169.254.255.255:137		udp
10.0.2.255:138		udp

TLS Handshake Failures (cert-pinning) (50)

```
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
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)
www.bing.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 169.254.255.255:137
4. [conn] pid 0: udp 255.255.255.255:67
5. [conn] pid 0: udp 224.0.0.251:5353
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 224.0.0.252:5355

12. [conn] pid 0: tcp 10.0.2.3:80
13. [conn] pid 0: tcp 10.0.2.3:80
14. [conn] pid 0: udp 10.0.2.3:53
15. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
16. [conn] pid 0: tcp 10.0.2.3:443
17. [conn] pid 0: tcp 10.0.2.3:443
18. [conn] pid 0: udp 10.0.2.3:53
19. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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 10.0.2.3:80
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 10.0.2.3:80

...and 75 more events

Packet capture: available (full PCAP)

Persistence (1)

[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat

Spawned Processes (50)

System
Registry
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
lsass.exe - C:\Windows\system32\lsass.exe
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s CryptSvc
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv ONnFsLN8xUmRmcl7ptfNyw.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p

...and 20 more