KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_54692596ddec.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 321 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
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	54692596ddec105cb0a4de07623bacd32fb45525b041114b71db1ceaa1a3e176
SHA-1:	4e9789fa88892713c4f640b34c5c599d13a188d1
MD5:	1446c7d0ac4247e20c57fc07cf53693a
Size:	1,001,472 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0xF5DE2
Sections:	3

Name	Virtual Size	Entropy
.text	0xF3DE8	7.76
.rsrc	0x4CC	3.72
.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
X )UU
X )UU
X )UU
(@Z~
.@ZX
&@Z~
?ZX~
$@ZX~
?ZX~
f@[(0
$@[[
$@[[
I@[Z#
@X(=
(YlZXi
V@ZYi
XkoF
[Y(9
XkoF
XkoF
XkoF
XkoF
*.rp
@[i(
#333333
?Zi(
#333333
ZXs-
@ZX(
.@Y#
Y#333333
$@[[
$@[[
?ZYX
5@Y#
F@[Z#333333
#ffffff
0@Y(
.@ZX~
@U@6
```

%r)"

%rC"

%rO"

... and 150 more

Malware Config

Indicators of Compromise (4)

Domains (4)

```
assets.msn.com
www.bing.com
config.edge.skype.com
edge-consumer-static.azureedge.net
```

MITRE ATT&CK (6)

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	
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

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
10.0.2.3:53		udp
10.0.2.3:443		tcp
255.255.255.255:67		udp
224.0.0.251:5353		udp
10.0.2.255:137		udp
10.0.2.255:138		udp
224.0.0.252:5355		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)
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 10.0.2.3:53
5. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
6. [conn] pid 0: tcp 10.0.2.3:80
7. [conn] pid 0: udp 10.0.2.255:137
8. [conn] pid 0: tcp 10.0.2.3:80
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 assets.msn.com -> 10.0.2.3
12. [conn] pid 0: tcp 10.0.2.3:443
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 10.0.2.3:80
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
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
fontdrvhost.ex - "fontdrvhost.exe"
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s LicenseManager
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
```

backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://www.msftconnect
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
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=gpu-process --gpu-preferences=SAA
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
urlhaus_546925 - "C:\Users\Public\Downloads\urlhaus_54692596ddec.exe"
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
MSBuild.exe
cmd.exe - "C:\Windows\SysWOW64\cmd.exe"
powershell.exe - "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Use
WmiPrvSE.exe - C:\Windows\system32\wbem\wmiprvse.exe-secured-Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p

...and 20 more