KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_3ddce244c308.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 63 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:	3ddce244c308f1ce27307b16467f29bd7f3e2333c535cb4a0c5d93a0b7296230
SHA-1:	2d2dc3e2beb02d79d39c17c3388b51566f29edf2
MD5:	f01afca27ee2c5d8779eed816bf8c91d
Size:	283,648 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x26A0
Sections:	1

Name	Virtual Size	Entropy
.text	0x44400	7.99

Strings (200 found)

```
MZER
```

```
!This program cannot be run in DOS mode.
Rich
.text
;Aau$
dXC<
Pt;Q$s>
;HXsi
Jt;H$
Jt;H\
Br?_D;
!o1WQU
Zs]k
6Byu
g]@x
 :6\
Lf)a
C[#}"Q
Ky=%K7
O7(;
n!xf
mn1#
.[=T
DoeTR
sGMkJ
=U-S
b%g}
9>HJ E
o"$I
(%.qCy$#:
?Bm=t
Q=/$X
EY&wZr
g./KS&
PAb'
o_&i
T6+)
ur3#
POeE
Oj2-{
?I{h
`wVfz
 *cn
#G'dTq
+ pS6
w)C3"
}z%3@
P]<U
<ESA
u":mAJ
```

... and 150 more

Malware Config

Indicators of Compromise (12)

URLs (4)

```
http://www.cprondemand.com/pm3y/
http://www.oxesqfws.com/tskl/
http://www.slotime118.com/il8x/
http://www.gourmetolia.nl/2322/
```

Domains (8)

```
www.cprondemand.com
www.oxesqfws.com
www.slotime118.com
www.gourmetolia.nl
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
10.0.2.3:443		tcp
10.0.2.3:53		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
10.0.2.255:137		udp
224.0.0.251:5353		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 10.0.2.255:137
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
7. [conn] pid 0: tcp 10.0.2.3:80
8. [conn] pid 0: tcp 10.0.2.3:80
9. [conn] pid 0: tcp 10.0.2.3:80
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 assets.msn.com -> 10.0.2.3
13. [conn] pid 0: tcp 10.0.2.3:443
14. [conn] pid 0: tcp 10.0.2.3:443
15. [conn] pid 0: udp 10.0.2.3:53
16. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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
wininit.exe - wininit.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
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
```

svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
dbInstaller.ex
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv Vl4zrXKrA06mwR0Uje91kA.0
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
dxgiadaptercac - "C:\Windows\system32\dxgiadaptercache.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc

...and 20 more