KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_26a079d8aa45.exe

Verdict: SUSPICIOUS

Verdict: suspicious; 195782 anti-VM checks (rdtsc)

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- Process Injection: Dynamic-link Library Injection
- Indicator Removal: File Deletion
- System Information Discovery
- Native API
- Modify Registry
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	26a079d8aa4562500ba24d38f4c93d8696e90ccb91d8481f581f7995b235d9b4
SHA-1:	9e69795f8536df8d9fef86295b1e329b038c4400
MD5:	18daa4731d5b880e9566d8a231e872c5
Size:	1,829,376 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x79B0
Sections:	6

Name	Virtual Size	Entropy

.text	0x7330	6.2
.rdata	0x2298	4.7
.data	0x1E80	3.19
.pdata	0x3FC	4.31
.rsrc	0x1B4246	7.98
.reloc	0x20	0.41

Imports

ADVAPI32.dll

GetTokenInformation
RegDeleteValueA
RegOpenKeyExA
RegQueryInfoKeyA
FreeSid
OpenProcessToken
RegSetValueExA
RegCreateKeyExA
LookupPrivilegeValueA
AllocateAndInitializeSid

KERNEL32.dll

_lopen
_llseek
CompareStringA
GetLastError
GetFileAttributesA
GetSystemDirectoryA
LoadLibraryA
DeleteFileA
GlobalAlloc
GlobalFree

GDI32.dll

GetDeviceCaps

USER32.dll

ShowWindow
MsgWaitForMultipleObjects
SetWindowPos
GetDC
GetWindowRect
DispatchMessageA
GetSystemMetrics
CallWindowProcA
SetWindowTextA
MessageBoxA

msvcrt.dll

?terminate@@YAXXZ
_commode
_fmode
_acmdln
__C_specific_handler
memset
__setusermatherr

_ismbblead

_cexit

_exit

COMCTL32.dll

Cabinet.dll

VERSION.dll

VerQueryValueA

GetFileVersionInfoSizeA

GetFileVersionInfoA

Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich(
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
t"L+
L$ SVWH
L$X3
 _^[
VWAVH
D$pL
D$`A
D$PD
l$HH
l$8A
T$`M
L$pH3
A^_^
p UH
E+E3
D$ E3
D$PH
t$HA
t$8D
t$0D
t$(D
D97v.
MGH3
D$ A
@8+tiH
\$0H
l$8H
t$@H
UVWATAUAVAWH
MPL+
}P"u
L$0H
|$0H
```

```
\<:u
D$@L
D$@A
L$@H
L$@D
L$ D
t$0H
t"D8)H
D$0H
```
... 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 (12)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
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

224.0.0.251:5353		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
10.0.2.255:138		udp

TLS Handshake Failures (cert-pinning) (50)

```
api.edgeoffer.microsoft.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
www.bing.com  (remote error: tls: unknown certificate)
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)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
www.bing.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
www.bing.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: udp 10.0.2.255:137
7. [conn] pid 0: tcp 10.0.2.3:80
8. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
9. [conn] pid 0: tcp 10.0.2.3:80
10. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
11. [conn] pid 0: tcp 10.0.2.3:80
12. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
13. [conn] pid 0: udp 10.0.2.3:53
14. [dns] pid 0: DNS 1 jndhxyteljvpbja.jndhxyteljvpbja -> 10.0.2.3
15. [conn] pid 0: udp 10.0.2.3:53
16. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
17. [conn] pid 0: tcp 10.0.2.3:443
18. [conn] pid 0: tcp 10.0.2.3:443
19. [conn] pid 0: tcp 10.0.2.3:443
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab
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 DcomLaunch -p
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{133EAC4F-5891-4D04-BADA-D84870380A80}
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
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
RuntimeBroker.
conhost.exe - \??\C:\Windows\system32\conhost.exe 0x4
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
NVDisplay.Cont - "C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContain
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
dbInstaller.ex
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv auQVFBuUNE2c3lh+DE08AQ.0
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
```

...and 20 more