KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_c1d55538417d.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 216449 anti-VM checks (rdtsc)

Analysis Overview

Score: 8/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- T1571
- Obfuscated Files or Information
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- Native API
- Modify Registry
- Screen Capture
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Data Encrypted for Impact
- Credentials from Password Stores: Credentials from Web Browsers
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion

Hashes

SHA-256:	c1d55538417d22ca041f9a269866ccba8957c40ee698860be340b297713eb8d9
SHA-1:	0950d60a82c2f2f4a2e4b0575ae7a15124245aff
MD5:	62026426767207280fe942f9cc6e9aab
Size:	524,800 bytes

Packer Detection

No packer detected.

PE Information

Architecture: 32-bit

Type: Executable

Entry Point: 0x3C9B9

Sections: 5

Name	Virtual Size	Entropy
.text	0x5DDDF	6.64
.rdata	0x185DC	5.77
.data	0xAD7C	3.07
.rsrc	0x489C	3.82
.reloc	0x4158	6.71

Imports

KERNEL32.dll

- DeleteFileA
- GetLogicalDriveStringsA
- SetFilePointerEx
- MoveFileW
- RemoveDirectoryW
- GetModuleHandleA
- TerminateThread
- GetFileSize
- ExpandEnvironmentStringsW
- GetEnvironmentVariableW

USER32.dll

- wsprintfW
- GetClipboardData
- UnhookWindowsHookEx
- GetForegroundWindow
- ToUnicodeEx
- GetKeyboardLayout
- SetWindowsHookExA
- CloseClipboard
- OpenClipboard
- GetKeyboardState

GDI32.dll

- BitBlt
- CreateCompatibleBitmap
- SelectObject
- CreateCompatibleDC
- StretchBlt
- GetDIBits
- DeleteDC
- DeleteObject
- CreateDCA
- GetObjectA

ADVAPI32.dll

- CryptAcquireContextA
- CryptGenRandom
- CryptReleaseContext
- GetUserNameW

RegEnumKeyExA
GetTokenInformation
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
RegQueryInfoKeyW

SHELL32.dll

Shell_NotifyIconA
ShellExecuteExA
ShellExecuteW
ExtractIconA

ole32.dll

CoUninitialize
CoGetObject
CoInitializeEx

WINMM.dll

PlaySoundW
waveInUnprepareHeader
waveInPrepareHeader
waveInStop
waveInClose
waveInStart
waveInAddBuffer
mciSendStringA
waveInOpen
mciSendStringW

WS2_32.dll

WSAGetLastError
WSAStartup
closesocket
send
inet_ntoa
getaddrinfo
socket
recv
connect

urlmon.dll

URLOpenBlockingStreamW
URLDownloadToFileW

gdiplus.dll

GdipLoadImageFromStream
GdipSaveImageToStream
GdipGetImageEncodersSize
GdipFree
GdipDisposeImage
GdipAlloc
GdipGetImageEncoders
GdiplusStartup
GdipCloneImage

WININET.dll

InternetCloseHandle
InternetReadFile
InternetOpenUrlW

Strings (200 found)

```
!This program cannot be run in DOS mode.
RichH
.text
`.rdata
@.data
.rsrc
@.reloc
h|2G
SUVWj
_^][
j Pf
D$,VPVj
L$(P
D$ PW
D$$PW
D$(PW
PUh$
D$,PW
D$0PW
D$4PW
_^][
QSVW
SUVW
_^][
YY_^
YY_^
3BRV
_^[]
 _^]
_^[]
 _^]
QQSUW
_][YY
QQUW
D$ U
_]YY
D$ PS
D$ PS
w49V
_^[]
w49V
_^[]
3BRV
QQSUV
t$$+
\$,Q
_^][YY
$_^]
w?VW
D$$P
```

... and 150 more

Malware Config

C2 / Network (1)

Endpoint	Source
`196.251.107.252:22061`	network

Indicators of Compromise (6)

IPv4 addresses (1)

`196.251.107.252`

Domains (5)

`zaa.co`

`assets.msn.com`

`www.bing.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

MITRE ATT&CK (21)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			detonation-evidence
T1571			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1055	Process Injection	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1057	Process Discovery	Discovery	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1113	Screen Capture	Collection	
T1115	Clipboard Data	Collection	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
T1486	Data Encrypted for Impact	Impact	
T1555.003	Credentials from Password Stores	Credential Access	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran

Behavior: malicious-behavior

Threat score: 80/100 (high)

Factors: c2, beaconing, attack_techniques

C2 beaconing: 1

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
196.251.107.252:22061		tcp
224.0.0.251:5353		udp
10.0.2.255:138		udp
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp

TLS Handshake Failures (cert-pinning) (50)

```
assets.msn.com  (tlsstate: deadline exceeded)
assets.msn.com  (tlsstate: deadline exceeded)
edge.microsoft.com  (remote error: tls: unknown certificate)
edge.microsoft.com  (remote error: tls: unknown certificate)
www.bing.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)
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)
functional.events.data.microsoft.com  (remote error: tls: unknown certificate)
```

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 196.251.107.252:22061
11. [conn] pid 0: tcp 10.0.2.3:80
12. [conn] pid 0: udp 10.0.2.3:53
13. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
14. [conn] pid 0: tcp 10.0.2.3:443

15. [conn] pid 0: tcp 10.0.2.3:443
16. [conn] pid 0: udp 10.0.2.3:53
17. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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
smss.exe - \SystemRoot\System32\smss.exe
StartMenuExper - "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceH
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
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
wlrmdr.exe - -c -s 0 -f 0 -t Empty -m Empty -a 0 -u Empty
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
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=crashpad-handler "--user-data-dir
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
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=storag
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
wissys.exe - "C:\Users\Matt.JOHNS-PC\AppData\Roaming\Config\wissys.exe"
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv 9QX1jo0zDU+HqNdDmqdODw.0
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b29055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
lsass.exe - C:\Windows\system32\lsass.exe
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSyst
services.exe - C:\Windows\system32\services.exe
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p

...and 20 more