KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_6929f5059552.exe

Verdict: MALICIOUS

Verdict: suspicious; 102 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1071.001
- T1105
- 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
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	6929f5059552a1f509ad4824ccfa11afefc8120351b09cb74003d263622b4a39
SHA-1:	3a8753068470fe0eb44a249a2e6f603769ee3986
MD5:	05276914dca447d79476329ccf07a345
Size:	641,024 bytes

Packer Detection

No packer detected.

PE Information

Architecture: 64-bit

Type: Executable

Entry Point: 0x49ADC

Sections: 6

Name	Virtual Size	Entropy
.text	0x6EFF8	6.43
.rdata	0x206D2	5.43
.data	0xC7E4	2.91
.pdata	0x62D0	5.64
.rsrc	0x48E4	3.82
.reloc	0xDA4	5.39

Imports

KERNEL32.dll

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

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

waveInOpen
waveInUnprepareHeader
waveInPrepareHeader
waveInStop
waveInStart
waveInAddBuffer
mciSendStringW
mciSendStringA
PlaySoundW
waveInClose

WS2_32.dll

socket
connect
recv
send
WSAGetLastError
WSAStartup
getaddrinfo
inet_ntoa
closesocket

urlmon.dll

URLOpenBlockingStreamW
URLDownloadToFileW

gdiplus.dll

GdipLoadImageFromStream
GdipDisposeImage
GdipAlloc
GdipSaveImageToStream
GdipGetImageEncodersSize
GdipCloneImage
GdipGetImageEncoders
GdiplusStartup
GdipFree

WININET.dll

InternetReadFile

InternetCloseHandle
InternetOpenW
InternetOpenUrlW

Strings (200 found)

```
!This program cannot be run in DOS mode.
K:s`B;
K:s`
K:s`I;
K:Rich
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
x AVH
\$@H
l$HH
t$PH
|$XH
\$0H
t$8H
D$@H
L$`L
T$ H
T$HH
UVWAVAWH
t$ D
t$ D
t$ D
t$ D
t$ D
t$ E
t$ E
t$ D
t$ D
t$ E
t$ E
t$ D
t$ D
t$ D
PA_A^_^]
\$0H
\$0H
t$8H
\$0H
\$0H
\$0H
\$0H
\$0H
\$0H
\$0H
t$8H
```

`\$8H`

`\$0H`

... and 150 more

Malware Config

Indicators of Compromise (7)

Domains (7)

`zaa.co`

`mainhold.duckdns.org`

`assets.msn.com`

`www.bing.com`

`winnerscorner.gleeze.com`

`config.edge.skype.com`

`edge-consumer-static.azureedge.net`

MITRE ATT&CK (20)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1071.001			detonation-evidence
T1105			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: suspicious

Threat score: 69/100 (medium)

Factors: c2, evasion, attack_techniques

Network Connections (9)

Destination	Domain	Proto
10.0.2.3:443		tcp
10.0.2.3:80		tcp
10.0.2.3:6040		tcp
224.0.0.251:5353		udp
10.0.2.3:53		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
255.255.255.255:67		udp
10.0.2.255:138		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)
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)
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. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
8. [conn] pid 0: udp 10.0.2.255:137
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 mainhold.duckdns.org -> 10.0.2.3
15. [conn] pid 0: tcp 10.0.2.3:6040
16. [conn] pid 0: tcp 10.0.2.3:80
17. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
18. [conn] pid 0: udp 10.0.2.3:53

19. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3
20. [conn] pid 0: tcp 10.0.2.3:443
21. [conn] pid 0: tcp 10.0.2.3:443
22. [conn] pid 0: udp 10.0.2.3:53
23. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
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
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
Registry
smss.exe - \SystemRoot\System32\smss.exe
dllhost.exe
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
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=crashpad-handler "--user-data-dir
wlrmdr.exe
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=utility --utility-sub-type=networ
SecurityHealth
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=renderer --pdf-upsell-enabled --v
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --v
msedge.exe
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
cmd.exe
conhost.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s SstpSvc
services.exe - C:\Windows\system32\services.exe

...and 20 more