

Analysis Report: urlhaus_ae5f17cf80ec.exe

Verdict: MALICIOUS

Verdict: suspicious; 263 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1105
- Obfuscated Files or Information
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- Application Layer Protocol: Web Protocols
- 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:	ae5f17cf80ec169d0d65dff3ab79c9080db0bcbb38d5a5a8b394e20672b19221
SHA-1:	1185106a3fc3bde0d91629e90b7ef36e956d04eb
MD5:	eb8a0620cb4087918fb7622b40438562
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	0x492C	3.83
.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

GdiplLoadImageFromStream
GdiplDisposeImage
GdiplAlloc
GdiplSaveImageToStream
GdiplGetImageEncodersSize
GdiplCloneImage
GdiplGetImageEncoders
GdiplStartup
GdiplFree

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

l\$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

t\$8H

\\$8H
\\$0H
... and 150 more

Malware Config

Indicators of Compromise (8)

Domains (8)

zaa.co
www.ikukuomaproject.com
assets.msn.com
www.bing.com
config.edge.skype.com
www.ikukuomaprojectbackup.com
edge-consumer-static.azureedge.net
www.ikukuomaprojectbackup1.com

MITRE ATT&CK (20)

Technique	Name	Tactic	Source
T1497.001			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	
T1071.001	Application Layer Protocol: Web	Command and Control	
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
10.0.2.3:80		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
10.0.2.3:2404		tcp
224.0.0.251:5353		udp
10.0.2.255:137		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)
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)
www.bing.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)
www.bing.com (tlsstate: deadline exceeded)
www.bing.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)

Behavioral Timeline (100)

- 1. [conn] pid 0: udp 224.0.0.251:5353
- 2. [conn] pid 0: udp 224.0.0.252:5355
- 3. [conn] pid 0: udp 255.255.255.255:67
- 4. [conn] pid 0: udp 224.0.0.251:5353
- 5. [conn] pid 0: udp 224.0.0.252:5355
- 6. [conn] pid 0: udp 224.0.0.252:5355
- 7. [conn] pid 0: udp 10.0.2.255:137
- 8. [conn] pid 0: udp 10.0.2.3:53
- 9. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
- 10. [conn] pid 0: tcp 10.0.2.3:80
- 11. [conn] pid 0: udp 224.0.0.252:5355
- 12. [conn] pid 0: tcp 10.0.2.3:80
- 13. [conn] pid 0: tcp 10.0.2.3:80
- 14. [conn] pid 0: udp 10.0.2.3:53
- 15. [dns] pid 0: DNS 1 www.ikukuomaproject.com -> 10.0.2.3
- 16. [conn] pid 0: tcp 10.0.2.3:2404
- 17. [conn] pid 0: udp 10.0.2.3:53
- 18. [dns] pid 0: DNS 1 assets.msn.com -> 10.0.2.3

```
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. [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
csrss.exe - %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=0n SubSystem=
services.exe - C:\Windows\system32\services.exe
dwm.exe - "dwm.exe"
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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 appmodel -p -s camsvc
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=gpu-process --gpu-preferences=SA
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=utility --utility-sub-type=stora
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
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
lsass.exe - C:\Windows\system32\lsass.exe
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
winlogon.exe - winlogon.exe
wininit.exe - wininit.exe
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv 2/T+MFwREkCrJnNqIq4c9Q.0
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
```

...and 20 more

Report ID: HD7sA_XVwHZCPmZH2d4zcXojjFRBQclsHMR1EDMKAk

Generated by KVMX - kvmx.ai