

Analysis Report: urlhaus_8a494cf5613a.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 930 anti-VM checks (mixed)

Analysis Overview

Score: 8/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- 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
- Ingress Tool Transfer
- 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:	8a494cf5613a27de7739d417506a93aa98c51453230f61de36d18d53e5456d97
SHA-1:	0617b24e963b97ba0fa031d09509b05ab06176d5
MD5:	842c0ec2c16fd14a656b3caa6b0d93fc
Size:	641,536 bytes

Packer Detection

No packer detected.

PE Information

Architecture: 64-bit
Type: Executable
Entry Point: 0x49A34
Sections: 6

Name	Virtual Size	Entropy
.text	0x6EF58	6.43
.rdata	0x20662	5.43
.data	0xC7F4	2.91
.pdata	0x62DC	5.66
.rsrc	0x4AF4	3.99
.reloc	0xDA0	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

C2 / Network (1)

Endpoint	Source
173.224.219.231:443	network

Indicators of Compromise (7)

IPv4 addresses (1)

173.224.219.231

Domains (6)

zaa.co
ccu.cc
api.msn.com
assets.msn.com
www.bing.com
arc.msn.com

MITRE ATT&CK (19)

Technique	Name	Tactic	Source
T1497.001			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	
T1105	Ingress Tool Transfer	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	

Dynamic Detonation

Coverage: ran
Behavior: malicious-behavior

Threat score: 75/100 (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
173.224.219.231:443		tcp
10.0.2.3:53		udp
10.0.2.255:137		udp
224.0.0.252:5355		udp
10.0.2.255:138		udp
224.0.0.251:5353		udp
255.255.255.255:67		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)

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 224.0.0.252:5355
- 5. [conn] pid 0: udp 10.0.2.255:137
- 6. [conn] pid 0: udp 10.0.2.3:53
- 7. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
- 8. [conn] pid 0: tcp 10.0.2.3:80
- 9. [conn] pid 0: udp 10.0.2.3:53
- 10. [dns] pid 0: DNS 1 login.live.com -> 10.0.2.3
- 11. [conn] pid 0: tcp 10.0.2.3:443
- 12. [conn] pid 0: udp 10.0.2.3:53
- 13. [dns] pid 0: DNS 1 ctldl.windowsupdate.com -> 10.0.2.3
- 14. [conn] pid 0: tcp 10.0.2.3:80

15. [conn] pid 0: tcp 10.0.2.3:80
16. [conn] pid 0: tcp 10.0.2.3:80
17. [conn] pid 0: tcp 10.0.2.3:443
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 173.224.219.231:443
21. [conn] pid 0: tcp 173.224.219.231:443
22. [conn] pid 0: tcp 173.224.219.231:443
23. [conn] pid 0: tcp 10.0.2.3:443
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)

Spawned Processes (50)

System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
smss.exe - \SystemRoot\System32\smss.exe
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
SearchApp.exe - "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:CortanaUI.A
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:ShellFeedsUI.AppXnj65k2d1a1rnztt2t2nng5ctn
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s BDESVC
svchost.exe - C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
RUXIMICS.exe - %ProgramFiles%\RUXIM\RUXIMICS.EXE /onlyloadcampaigns
dllhost.exe - C:\Windows\system32\DllHost.exe /Processid:{722D0F89-B69C-4700-AE8C-4A44350E4876}
mobsync.exe - C:\Windows\System32\mobsync.exe -Embedding
UserOOBEBroker - C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
conhost.exe - ???C:\Windows\system32\conhost.exe 0x4
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXnn6fnh4raxtmg45ba8k2f4yk
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
Usoclient.exe - "C:\Windows\system32\usoclient.exe" StartScan
taskhostw.exe
backgroundTask - "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.DesktopSpotlight.AppXz2j21w56bgxkg
DeviceCensus.e - "C:\Windows\system32\devicecensus.exe" SystemCxt
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storag
taskhostw.exe - taskhostw.exe None
ClipESUConsume - "C:\Windows\system32\ClipESUConsumer.exe" -processRefund
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s PushToInstall
spssvc.exe - C:\Windows\system32\spssvc.exe
conhost.exe
...and 20 more