

Analysis Report: urlhaus_07b1a32c53c1.exe

Verdict: MALICIOUS

Verdict: likely-malicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 7/10

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:	07b1a32c53c1efab24f54151b1158bad7404374f0dfdee558e7ad80ad278575a
SHA-1:	bbdbbbaa2596aa7a8a85fa4d4090c4a0387d7d74
MD5:	2d4fe10deb30092875ad0e5327904cd9
Size:	641,024 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	0x48E8	3.82
.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
194.59.31.77:5050	network

Indicators of Compromise (10)

IPv4 addresses (2)

194.59.31.77
94.59.31.77

Domains (8)

zaa.co
ccu.cc
assets.msn.com
www.bing.com
config.edge.skype.com
escalatefud.duckdns.org
edge-consumer-static.azureedge.net
ipv6-literal.net

MITRE ATT&CK (22)

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	
T1083	File and Directory Discovery		pt_trace

T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference
-----------	----------------------------------	-------------	----------------------

Per-Process ATT&CK Attribution (5)

Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).

				Process
0x127af7000		56	T1083	
svchost.exe	3080	239	T1057, T1134	
svchost.exe	1528	179	T1134	
0x148297000		98	T1057	
svchost.exe	3964	218	T1057	

Dynamic Detonation

Coverage: ran
Behavior: malicious-behavior
Threat score: 70/100 (high)
Factors: c2, attack_techniques

Network Connections (10)

Destination	Domain	Proto
10.0.2.3:80		tcp
10.0.2.3:443		tcp
10.0.2.3:53		udp
194.59.31.77:5050		tcp
10.0.2.255:138		udp
10.0.2.3:5050		tcp
255.255.255.255:67		udp
10.0.2.255:137		udp
224.0.0.252:5355		udp
224.0.0.251:5353		udp

Memory-Recovered IOCs (runtime deobfuscation) (4)

Decoded from guest memory at the hypervisor - recovered from obfuscation static analysis cannot unpack.

[domain] escalatefud.duckdns.org
[domain] ipv6-literal.net
[ip] 194.59.31.77
[ip] 94.59.31.77

TLS Handshake Failures (cert-pinning) (50)

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)
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)
www.bing.com (tlsstate: deadline exceeded)

```
functional.events.data.microsoft.com (remote error: tls: unknown certificate)
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)
```

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: tcp 10.0.2.3:80
10. [conn] pid 0: tcp 194.59.31.77:5050
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
winlogon.exe - winlogon.exe
smss.exe - \SystemRoot\System32\smss.exe
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
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir
RuntimeBroker. - C:\Windows\System32\RuntimeBroker.exe -Embedding
msedge.exe - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network
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=utility --utility-sub-type=storage
```

```
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=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
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
dwm.exe - "dwm.exe"
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv cJW5RsGSKUG3RB+g1GCXMg.0
NVDIplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContain
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
...and 20 more
```

Report ID: rbf3wm3OsTrtZgpjmzmlXWdqlO2YnVtqrceLqF4Lyok

Generated by KVMX - kvmx.ai