KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_748c32e37183.exe

Verdict: MALICIOUS

Verdict: suspicious; 40 anti-VM checks (mixed)

Analysis Overview

Score: 3/10

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
- File and Directory Discovery

Hashes

SHA-256:	748c32e3718319e569d7a71eab5ace7589ed012764902b55475faab82a63c89b
SHA-1:	49d293bee3fe99fbc0cf857347d9e5259dc41b94
MD5:	c29ddb54bb464846ba7e2de1d3eff471
Size:	525,312 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	0x4B70	3.99
.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

Indicators of Compromise (1)

Domains (1)

```
zaa.co
```

MITRE ATT&CK (21)

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	
T1083	File and Directory Discovery		pt_trace
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (3)

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

Proces				
0x14eadc000		543	T1083	
csrss.exe	420	100	T1055, T1055.002, T1057, T1083	
NVDisplay.Cont	1244	406	T1055	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (59)

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. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
10. [conn] pid 0: tcp 10.0.2.3:80
11. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
12. [conn] pid 0: tcp 10.0.2.3:80
13. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
14. [conn] pid 0: tcp 10.0.2.3:80
15. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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: tcp 10.0.2.3:80
19. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
20. [conn] pid 0: udp 10.0.2.3:53
21. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
22. [conn] pid 0: tcp 10.0.2.3:80
23. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
24. [conn] pid 0: tcp 10.0.2.3:80
25. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt

...and 34 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
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
services.exe - C:\Windows\system32\services.exe
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp

svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv 5+CICm5a5USqdNEV/ng7Vw.0
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b28855 /state1:0x41c64e6d
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc

...and 20 more