KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_f3d5f11778fa.exe

Verdict: SUSPICIOUS

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

Analysis Overview

Score: 3/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1105
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- System Information Discovery
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- File and Directory Discovery
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	f3d5f11778fa3955a20e8b73a3e284eebd6dcc14f12f0a38657086c26b5ea596
SHA-1:	b0bf580e2710c62c2c82c3bf4079752e0390b7a6
MD5:	7e4697b83f8a31b5d0650b34e01c4702
Size:	596,832 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x75E0
Sections:	7

Name	Virtual Size	Entropy
.text	0x19E61	6.53
.rdata	0xCE2C	5.13
.data	0x1AEA8	1.94
.pdata	0x147C	5.06
.fptable	0x100	0.0
.rsrc	0x65424	8.0
.reloc	0x664	4.88

Imports

KERNEL32.dll

- TerminateProcess
- CreateThread
- GetCurrentThreadId
- OpenThread
- FlushInstructionCache
- GetTickCount
- VirtualAlloc
- VirtualProtect
- VirtualFree
- GetModuleHandleA

USER32.dll

- DispatchMessageW
- GetSystemMetrics
- GetCursorPos
- wsprintfA
- MsgWaitForMultipleObjectsEx
- PeekMessageW
- TranslateMessage
- MessageBoxW
- wsprintfW
- GetAsyncKeyState

ADVAPI32.dll

- RegCloseKey
- GetTokenInformation
- OpenProcessToken
- RegQueryInfoKeyW
- RegOpenKeyExW
- GetUserNameW

COMCTL32.dll

- InitCommonControlsEx

SHLWAPI.dll

- PathFileExistsW
- StrCmpIW

UxTheme.dll

- IsAppThemed
- IsThemeActive

USERENV.dll

- GetUserProfileDirectoryW

ole32.dll

CoInitializeEx

CoUninitialize

VERSION.dll

GetFileVersionInfoSizeW

Strings (200 found)

```
!Cannot execute in real-mode session       $
QWepw
k9fY_
MqW)
LRich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
L$ L
SVWATAUAVAWH
D$8ole3
D$<2.dlf
D$@l
D$HH
\$ M
\$LE2
D$`H
D$tH
D$23
d$3L
L$LD
|$13
d$3H
|$0E3
D$`H
D$tH
|$13
A_A^A]A\_^[
\$0H
t$8H
I*Ai
|$ f
|$ fA
D$8H
D$(H
\$ A
"r?L
\$`H
t$hH
|$pH
r4E3
TCDA
D$`H
```

D$ H

t$@A

t$@H

... and 150 more

MITRE ATT&CK (14)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			detonation-evidence
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	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1134	Access Token Manipulation	Privilege Escalation	
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 (4)

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

			Proces
0x146c4c000		373	T1083
svchost.exe	1292	137	T1057
0x4c0c000		24	T1055
0x1410e0000		51	T1083

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (60)

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 224.0.0.252:5355
6. [conn] pid 0: udp 10.0.2.255:137
7. [conn] pid 0: udp 10.0.2.3:53
8. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
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: tcp 10.0.2.3:80
14. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
15. [conn] pid 0: tcp 10.0.2.3:80
16. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
17. [conn] pid 0: tcp 10.0.2.3:80
18. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
19. [conn] pid 0: tcp 10.0.2.3:80
20. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
21. [conn] pid 0: udp 10.0.2.3:53
22. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
23. [conn] pid 0: tcp 10.0.2.3:80
24. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
25. [conn] pid 0: tcp 10.0.2.3:80

...and 35 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 -s LSM
smss.exe - \SystemRoot\System32\smss.exe
fontdrvhost.ex - "fontdrvhost.exe"
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv Gz4Mfn7RFkChzDzwFr4yEA.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
dbInstaller.ex
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
```

svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall

...and 20 more