

Analysis Report: urlhaus_c848d8ec8f93.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
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256: c848d8ec8f9304466f206cfbe4d4ece7fa0584dfe706f0fd8240c18730606efb
SHA-1: 399de14116f0dbae8ec9ca8e999f00a4356081c7
MD5: 08dd098116278d44e4a8b1a7943efe60
Size: 717,472 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	5.12
.data	0x1AEA8	1.94
.pdata	0x147C	5.06
.fptable	0x100	0.0
.rsrc	0x7F7B8	7.66
.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)

!This application requires Windows \$
R<Dt
\${kj
,s8kG 6
Rich
.text
@.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
P@SH
r4E3
TCDA
PP@SH

D\$`H
D\$ H
... and 150 more

MITRE ATT&CK (13)

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	
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Dynamic Detonation

Coverage: ran
Behavior: suspicious
Threat score: 30/100 (medium)
Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (58)

- 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 33 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
fontdrvhost.exe - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv QgatTxkmVU+J+5wvZl01rw.0
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2c855 /state1:0x41c64e6d
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
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 LocalSystemNetworkRestricted -s WPDBusEnum
NVIDIA.Container - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContainer
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
```

...and 20 more