KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_89e1d9efd0f1.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:	89e1d9efd0f1fff32f4a31dc06499e39219606b1984b7428267cd64faf36b8e5
SHA-1:	d95d5e7e28330af199412b424a8bb0be54d3c12e
MD5:	e8fe02e4043bd822ef385a96ce640ab4
Size:	570,096 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x7350
Sections:	7

Name	Virtual Size	Entropy

.text	0x1F9D7	6.6
.rdata	0xDB74	5.26
.data	0x1AE78	1.94
.pdata	0x1698	5.14
.fptable	0x100	0.0
.rsrc	0x57B18	7.47
.reloc	0x688	4.93

Imports

KERNEL32.dll

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

USER32.dll

- TranslateMessage
- MessageBoxW
- GetSystemMetrics
- GetCursorPos
- PeekMessageW
- DispatchMessageW
- wsprintfA
- MsgWaitForMultipleObjectsEx
- 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)

```
!Win32 subsystem is required to run        $
2]08
`E$Q
{LpY_*
NRich
.text
`.rdata
@.data
.pdata
@.fptable
.rsrc
@.reloc
L$ L
SVWATAUAVAWH
D$8ole3
D$<2.dlf
D$@l
T$xH
D$HH
\$ L
\$LE2
D$XH
D$lH
D$23
 u_L
L$LD
D$13
d$0H
D$XH
L$lH
D$13
A_A^A]A\_^[
\$0H
t$8H
S:*q55
I*Ai
55555:*q55H
|$ f
|$ fA
:*u5
D$8H
D$(H
\$ A
"r?L
\$`H
t$hH
|$pH
:*5@SH
```

55555S

:*5@SH

... 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

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
0x15abfe000		202	T1057
0x149164000		1328	T1055, T1083
0x145bab000		52	T1057, T1083
0x14b4e2000		80	T1057

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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