KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_ec0078d806fc.exe

Verdict: SUSPICIOUS

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

Analysis Overview

Score: 3/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- 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

Hashes

SHA-256:	ec0078d806fcb7b0ef538a51ae03217888ce1bd3e96a73beceecc2c12675d77d
SHA-1:	018356c22bf7997520cc341b97eb7e6e4b4ccb67
MD5:	bf8ec2994ca75d5e09c66a0fc740459e
Size:	609,656 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	0x67CF8	7.99
.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)

```
!Please run under supported environment    $
Rich
.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
P@SH
r4E3
TCDA
PP@SH
D$`H
D$ H
t$@A
t$@H
```

`|$8H`

... and 150 more

MITRE ATT&CK (11)

Technique	Name	Tactic	Source
T1497.001			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	

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 30/100 (medium)

Factors: evasion, attack_techniques

Network Connections (6)

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

Behavioral Timeline (29)

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 4 more events

Packet capture: available (full PCAP)

Spawned Processes (12)

```
System
Registry
svchost.exe
smss.exe - \SystemRoot\System32\smss.exe
csrss.exe
services.exe
smss.exe
wininit.exe
ClipRenew.exe
autochk.exe - \??\C:\Windows\system32\autochk.exe *
WmiPrvSE.exe
slui.exe
```