KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_9d25feaab502.exe

Verdict: SUSPICIOUS

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

Analysis Overview

Score: 4/10

Threat level: Suspicious

Malicious Activity Summary

- T1497.001
- T1105
- Process Injection: Dynamic-link Library Injection
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Process Injection
- Process Discovery
- Access Token Manipulation: Token Impersonation/Theft
- Process Injection: Portable Executable Injection
- File and Directory Discovery
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	9d25feaab50222517f6179cccdda791c0d3b3516a353fe426c5e40f77fcbbc0e
SHA-1:	57c76b8063528fa20b6af83d2d728a735d9a5bab
MD5:	2622dc67f73396b698ae2b60ee82a5e0
Size:	2,828,136 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x759E0
Sections:	6

Name	Virtual Size	Entropy

.text	0x104C9B	6.21
.rdata	0x173228	6.88
.data	0x31C7C	5.78
.idata	0x44C	3.87
.reloc	0xBED0	6.66
.symtab	0x1FE84	5.12

Imports

kernel32.dll

- WriteFile
- WriteConsoleW
- WerSetFlags
- WerGetFlags
- WaitForMultipleObjects
- WaitForSingleObject
- VirtualQuery
- VirtualFree
- VirtualAlloc
- TlsAlloc

Strings (200 found)

```
!This program cannot be run in DOS mode.
.text
`.rdata
@.data
.idata
.reloc
B.symtab
 Go build ID: "900AeZYVjIJudMm9qDad/-RJTgfG8dGbDnKBbphK9/tCxLrz3IPwLeRSQvwIDL/dB_4nMSFVdhBeNSoiWh3"
l$19
t$d9
l$`9
D$@9
l$P)
T$'9
L$P9
T$<9
L$h9
;cpu.u
t$4)
?onua
?ofuP
9fuG
>alu
\$(1
D$ 9
\$#!
\$"!
H$9J$
H(9J(
H,8J,
```

`H-8J-`
`J49H4`
`H89J8u|`
`H<8J<us`
`H=8J=uj`
`HD9JDub`
`HH9JHuZ`
`HL8JLuQ`
`HM8JMuH`
`JT9HTu@`
`HX9JXu8`
`H\8J\u/`
`H]8J]u&`
`Hd9Jdu`
`Hh9Jhu`
`Hl8Jlu`
`Hm8Jmu`
`\$$!`
`T$D9`
`D$,1`
... and 150 more

MITRE ATT&CK (12)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			detonation-evidence
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1082	System Information Discovery	Discovery	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1055	Process Injection		pt_trace
T1057	Process Discovery		pt_trace
T1134.001	Access Token Manipulation: Token		pt_trace
T1055.002	Process Injection: Portable Exec		pt_trace
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
csrss.exe	424	117	T1055, T1055.002, T1057, T1083, T1134.001
NVDisplay.Cont	1248	956	T1055
svchost.exe	1268	230	T1055, T1055.002, T1057
0x14599f000		277	T1057

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 45/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (65)

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 40 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
taskhostw.exe - taskhostw.exe SYSTEM
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog

svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
XtuService.exe - C:\Windows\SysWOW64\XtuService.exe
smss.exe - \SystemRoot\System32\smss.exe 000000c4 00000084
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
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 netsvcs -p -s UserManager
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv E8fTrYt8IUC3jFS+n8OlRw.0
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b25855 /state1:0x41c64e6d

...and 20 more