KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_9c389d5cc294.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: Dynamic-link Library Injection
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	9c389d5cc29456269003267ca586ba20168884bfc5bc22bc8e44866fa1cf519d
SHA-1:	87866e34f786cc1aa4f0ca129a04cba72afe23d7
MD5:	bc40fa0a76a14871c59644404430cf25
Size:	2,840,920 bytes

Packer Detection

No packer detected.

PE Information

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

Name	Virtual Size	Entropy
.text	0x104C1B	6.21
.rdata	0x1765C8	6.9
.data	0x31C7C	5.78
.idata	0x44C	3.88
.reloc	0xBEE4	6.66

.symtab	0x1FE8B	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: "Gk6Wip7pQ5UkBjkNTo_7/A5eRuIioWK14caNQ0nCC/9dhdW3JKbsh7KCXwauWV/gnek6-lRDXYWonBz5RUS"
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 (7)

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	
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
`224.0.0.252:5355`		`udp`
`10.0.2.3:80`		`tcp`
`10.0.2.3:53`		`udp`
`224.0.0.251:5353`		`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 224.0.0.252:5355`
3. `[conn] pid 0: udp 224.0.0.251:5353`
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 224.0.0.252:5355`
7. `[conn] pid 0: udp 10.0.2.255:137`

8. [conn] pid 0: udp 10.0.2.3:53
9. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
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: tcp 10.0.2.3:80
21. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
22. [conn] pid 0: udp 10.0.2.3:53
23. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
24. [conn] pid 0: tcp 10.0.2.3:80
25. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt

...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
fontdrvhost.ex - "fontdrvhost.exe"
lsass.exe - C:\Windows\system32\lsass.exe
services.exe - C:\Windows\system32\services.exe
smss.exe - \SystemRoot\System32\smss.exe
dwm.exe - "dwm.exe"
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv fOiJ9xTssEijVTmc/yklxw.0
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
smss.exe - \SystemRoot\System32\smss.exe 000000b8 00000084
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
taskhostw.exe - taskhostw.exe network
dbInstaller.ex
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS

...and 20 more