KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_84e0669351cd.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
- Application Layer Protocol: Web Protocols
- System Information Discovery
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	84e0669351cdf4ce4006082749c8810219134c1d332f2b226697c5ed00f3c04c
SHA-1:	1993cc64e69f1f07d4b5dc051bbd6be1a04ee656
MD5:	aaea22c0545af555ecf5357c0bfcc18c
Size:	10,349,416 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	64-bit
Type:	Executable
Entry Point:	0x73D60
Sections:	8

Name	Virtual Size	Entropy
.text	0xF7791	6.24
.rdata	0x1B1EA8	6.99
.data	0x58028	4.53
.pdata	0x4F8C	5.24

.xdata	0xB4	1.78
.idata	0x53E	4.02
.reloc	0x4148	5.41
.symtab	0x1BCB6	5.05

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
.pdata
@.xdata
@.idata
.reloc
B.symtab
 Go build ID: "-sLTirI4LNPBwP_Z6fKD/KB_kx220G06yLo1Ag7QN/VgQtv6pD9dytzVnGviGf/jaOGqiQ_CaP7j5pB-S4t"
|$XL
T$xH
T$`L
L$hE
t$OL
d$pH
L$pf
|$hL
\$EH9
L$pH
|$hH
t$xH9
t$XH9
|$`L
\$;H9
L$PH
T$xH
D$PH
L$xH9
|$`I
wDH)
|$ @
```

```
t$(D
t$(D
l$ M9,$u
M9,$u
v,UH
D$ H
D$ H
8cpu.u
D$PH
t$pH
L$HH
\$`H)
\$ M
\$XH
onuzH
ofu]F
fuQH
T$@1
```
... and 150 more

Indicators of Compromise (1)

Domains (1)

```
n.win
```

MITRE ATT&CK (8)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			detonation-evidence
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
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
10.0.2.3:80		tcp
10.0.2.3:53		udp
255.255.255.255:67		udp
224.0.0.251:5353		udp
10.0.2.255:137		udp

224.0.0.252:5355		udp

Behavioral Timeline (57)

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 10.0.2.255:137
5. [conn] pid 0: udp 10.0.2.3:53
6. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
7. [conn] pid 0: tcp 10.0.2.3:80
8. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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: udp 10.0.2.3:53
20. [dns] pid 0: DNS 1 www.msftconnecttest.com -> 10.0.2.3
21. [conn] pid 0: tcp 10.0.2.3:80
22. [http] pid 0: GET http://www.msftconnecttest.com/connecttest.txt
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: udp 10.0.2.3:53

...and 32 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
dwm.exe - "dwm.exe"
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
smss.exe - \SystemRoot\System32\smss.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
LogonUI.exe - "LogonUI.exe" /flags:0x2 /state0:0xa3b2d055 /state1:0x41c64e6d
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv rPbPcLeU80mREhW1xoYv8g.0
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
NVDisplay.Cont - C:\Windows\System32\DriverStore\FileRepository\nvamig.inf_amd64_5a5c892944a7f61d\Display.NvContaine
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
fontdrvhost.ex - "fontdrvhost.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder

```
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
taskhostw.exe - taskhostw.exe ExploitGuardPolicy
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
lsass.exe - C:\Windows\system32\lsass.exe
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
```

...and 20 more