KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_e85149704da6.exe

Verdict: MALICIOUS

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

Analysis Overview

Score: 4/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- Process Discovery

Hashes

SHA-256:	e85149704da6ee8f9bc1c55304c560d1a792180489d4859a64cf0a4e056ccf52
SHA-1:	16646bfd7f6554cd170fb373ce813c24f37e829e
MD5:	f8e68cddf13a94d821a4b265172a0e32
Size:	640,000 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x1E663
Sections:	5

Name	Virtual Size	Entropy
.text	0x5799E	6.7
.rdata	0x1404E	5.45
.data	0x3C7B4	5.34

.fptable	0x80	0.0
.reloc	0x4748	6.71

Imports

KERNEL32.dll

- LoadLibraryA
- GetProcAddress
- GetCurrentProcess
- HeapSize
- QueryPerformanceCounter
- QueryPerformanceFrequency
- GetSystemTimePreciseAsFileTime
- Sleep
- GetCurrentThreadId
- WideCharToMultiByte

Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich-
.text
`.rdata
@.data
.fptable
.reloc
)h <F
t&VW
v$VQPS
3WQPS
VQPS
+QPW
_^[]
RQVSQ
_^[]
Wh\VF
_^[]
QSVW
YY_[^
YY[kE
f;D$
WjdRP
u8SWQRP
6SWVRP
0_^[
YY_^
h0rF
h$rF
6SVQRQ
_^[]
t,VS
SVWQ
6PVQ
```

```
v@Ph@B
h<rF
htrF
WhtrF
Wh sF
h<rF
htrF
VWu)
F(^[
h<rF
WhXtF
WhpuF
h<rF
h<rF
hXtF
h<rF
```

... and 150 more

Indicators of Compromise (2)

IPv4 addresses (1)

```
111.111.111.111
```

Domains (1)

```
zaa.co
```

MITRE ATT&CK (9)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1105	Ingress Tool Transfer	Command and Control	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1057	Process Discovery		pt_trace

Per-Process ATT&CK Attribution (3)

Which process attributed which technique, from the Intel-PT per-CR3 demux (each syscall resolved under its own process address space).

			Proces
LogonUI.exe	1028	91	T1057
NVDisplay.Cont	1320	381	T1055, T1083
0x53bc000		73	T1057

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 35/100 (medium)

Factors: evasion, attack_techniques

Network Connections (6)

Destination	Domain	Proto
255.255.255.255:67		udp
224.0.0.252:5355		udp
10.0.2.255:137		udp
10.0.2.3:53		udp
10.0.2.3:80		tcp
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 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 4 more events

Packet capture: available (full PCAP)

Spawned Processes (50)

```
System
Registry
svchost.exe - C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -s WPDBusEnum
smss.exe - \SystemRoot\System32\smss.exe
fontdrvhost.ex - "fontdrvhost.exe"
dwm.exe - "dwm.exe"
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
svchost.exe - C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
svchost.exe - C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
```

```
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
upfc.exe - C:\Windows\System32\Upfc.exe /launchtype boot /cv PPS509q2Hk2xAXBuPDIwaA.0
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
svchost.exe - C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
svchost.exe - C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
svchost.exe - C:\Windows\system32\svchost.exe -k RPCSS -p
services.exe - C:\Windows\system32\services.exe
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
smss.exe - \SystemRoot\System32\smss.exe 00000080 00000084
svchost.exe - C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
svchost.exe - C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
svchost.exe - C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
svchost.exe - C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
svchost.exe - C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
```

...and 20 more