KVMX

Evidence-First Malware Analysis

Analysis Report: urlhaus_243aa79d0616.exe

Verdict: MALICIOUS

Verdict: suspicious; 42 anti-VM checks (mixed)

Analysis Overview

Score: 4/10

Threat level: Malicious

Malicious Activity Summary

- T1497.001
- T1105
- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Application Layer Protocol: Web Protocols
- Shared Modules
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion
- File and Directory Discovery
- Process Injection
- Process Discovery
- Access Token Manipulation: Token Impersonation/Theft
- Process Injection: Portable Executable Injection
- Boot or Logon Autostart Execution: Registry Run Keys

Hashes

SHA-256:	243aa79d0616ce126bd21133e2a06326eeb81104613e298a22d2cffaa292e2e7
SHA-1:	99518addf72cb85cd19122cec7bd0201aebbd7d0
MD5:	ff52c7106d382aa1094208bb24385f63
Size:	647,168 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x1EED0
Sections:	5

Name	Virtual Size	Entropy
.text	0x5922A	6.69
.rdata	0x142CE	5.45
.data	0x3C7E4	5.34
.fptable	0x80	0.0
.reloc	0x47F8	6.74

Imports

KERNEL32.dll

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

Strings (200 found)

```
!This program cannot be run in DOS mode.
1Rich=
.text
`.rdata
@.data
.fptable
.reloc
t&VW
v$VQPS
3WQPS
VQPS
+QPW
_^[]
RQVSQ
_^[]
Wh4vF
_^[]
QSVW
YY_[^
YY[kE
WjdRP
SWVRP
YY_^
6SVQRQ
_^[]
t,VS
SVWQ
6PVQ
v@Ph@B
```

`YY_^`
`VWu)`
`F(^[`
`4OVW`
`t(VW`
`U8V3`
`st+}`
`=WRQP`
`>_^[]`
`SVWj`
`_^[]`
`wJ9G`
`^_[]`
`wP;G`
`rhRj`
`VQPS`
`YYQf`
`uIh=1`
`uZhx`
`X4uJ`
`uIh=1`
... and 150 more

Indicators of Compromise (2)

IPv4 addresses (1)

`111.111.111.111`

Domains (1)

`zaa.co`

MITRE ATT&CK (14)

Technique	Name	Tactic	Source
T1497.001			detonation-evidence
T1105			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	
T1129	Shared Modules	Execution	
T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	
T1083	File and Directory Discovery		pt_trace
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
T1547.001	Boot or Logon Autostart Executio	Persistence	behavioral_inference

Per-Process ATT&CK Attribution (1)

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

			Proces
0x14b2b8000		226	T1055, T1055.002, T1057, T1083, T1134.001

Dynamic Detonation

Coverage: ran

Behavior: suspicious

Threat score: 45/100 (medium)

Factors: dropped_exe, attack_techniques

Network Connections (6)

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

Behavioral Timeline (64)

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 39 more events

Packet capture: available (full PCAP)

Persistence (1)

[Startup folder] malray.bat -> /ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/malray.bat

Spawned Processes (7)

System

Registry

```
svchost.exe
smss.exe - \SystemRoot\System32\smss.exe
smss.exe
csrss.exe
autochk.exe - \??\C:\Windows\system32\autochk.exe *
```