KVMX

Evidence-First Malware Analysis

Analysis Report: 2e4319ff62c0.bin

Verdict: MALICIOUS

2e4319ff62c0.bin is a 32-bit DLL with 7 sections. Packer detected: Unknown packer (high entropy in .data). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection

Hashes

SHA-256:	2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b
SHA-1:	ed35b02fa029f1e724ed65c2de5de6e5c04f7042
MD5:	0826df3aaa157edff9c0325f298850c2
Size:	185,344 bytes

Packer Detection

Packer:	Unknown packer (high entropy in .data)
Confidence:	medium

PE Information

Architecture:	32-bit
Type:	DLL
Entry Point:	0x24517
Sections:	7

Name	Virtual Size	Entropy
.text	0x23536	6.66
.te32t	0xA	0.12
.bss1	0x1000	0.0
.rdata	0xB0E	6.58
.data	0xEAC	7.07
.rsrc	0x3510	4.16
.reloc	0x444A	6.15

Imports

KERNEL32.dll

- GetModuleFileNameA
- CloseHandle
- LoadLibraryA
- QueryPerformanceCounter
- GlobalAddAtomA
- GetCommandLineW
- GetDriveTypeW
- CreateFileA
- GetCurrentProcessId

USER32.dll

- SendMessageA
- CharLowerA

GDI32.dll

- BeginPath
- AngleArc
- AbortPath
- AddFontMemResourceEx
- AnimatePalette

WINSPOOL.DRV

- ClosePrinter

ADVAPI32.dll

- RegOpenKeyW

SHELL32.dll

- CommandLineToArgvW

WINMM.dll

- PlaySoundA

msvcrt.dll

- exit
- _except_handler3
- _wtoi

Strings (200 found)

```
!This program cannot be run in DOS mode.
RichOi
.text
.te32t
`.bss1
.rdata
@.data
.rsrc
@.reloc
SVW3
jdY+
jkY+
j+X_^[+
fWf_3
XU]3
_u2g
```

```
K-5}
od[-PPj
j;Y+
jDX+
+PPPj
7NuT
\\aC3
jfj<X
jHX+
j_X3
jDX3
5PpB
jGj=h
CGQU
h0EB
XuW@
E H8
Q0uP\
xM4&
- .SB
P18|
R[3R
[094
5X9l
Bh`U
`@tP(
S^6YSm5mH}
W?@)
h@tv
8t1*
*PA_PG
Xw99
0T`0
*(^d
```

... and 150 more

MITRE ATT&CK (2)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	