KVMX

Evidence-First Malware Analysis

Analysis Report: bfb9db791b82.bin

Verdict: MALICIOUS

bfb9db791b82.bin is a 32-bit executable with 9 sections. Packer detected: Custom packer (non-standard sections: .mysec, .mysec3, .mysec2). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Shared Modules
- Impair Defenses: Disable or Modify Tools
- Debugger Evasion

Hashes

SHA-256:	bfb9db791b8250ffa8ebc48295c5dbbca757a5ed3bbb01de12a871b5cd9afd5a
SHA-1:	e536b70e3ffe309f7ae59918da471d7bf4cadd1c
MD5:	e6b43b1028b6000009253344632e69c4
Size:	298,496 bytes

Packer Detection

Packer:	Custom packer (non-standard sections: .mysec, .mysec3, .mysec2)
Confidence:	medium

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x2CFB
Sections:	9

Name	Virtual Size	Entropy
.text	0x1F982	6.63
.rdata	0x429E	5.27
.data	0x4E66AC8	1.12
.mysec	0x400	0.0

.mysec3	0x400	0.0
.mysec2	0x400	0.0
.rcrs	0x16C6C	6.0
.rsrc	0x2238	6.39
.reloc	0x885C	1.74

Imports

KERNEL32.dll

- lstrlenW
- CreateMailslotW
- GetLastError
- GetProcAddress
- LoadLibraryW
- VirtualProtect
- DuplicateHandle
- CloseHandle
- GetTickCount
- GetFileAttributesExA

ADVAPI32.dll

- OpenSCManagerA
- SetAclInformation
- AreAnyAccessesGranted

Strings (200 found)

```
!This program cannot be run in DOS mode.
RichO
.text
`.rdata
@.data
.mysec
`.mysec3
`.mysec2
`.rcrs
.rsrc
@.reloc
VVVVV
LSVW
M<%_
1L%,
PPPPPPP
r%>
(OW-
$Pj@
(h@9B
VVVV
h\9B
ht9B
h|>B
tG9}
0WWWWW
SSSSS
```

```
VVVVV
_^[]
_^[]
~,WPV
98t^
tVPV
t/9U
SSSSS
Ph8fB
_VVVVV
0WWWWW
X_^]
jXh ?B
YQPVh
QQSVWd
QSVW
Y__^[
PPPPP
PPPPP
PPPPP
PPPPP
@u^V
, <Xw
```

... and 150 more

MITRE ATT&CK (5)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1129	Shared Modules	Execution	
T1562.001	Impair Defenses: Disable or Modi	Defense Evasion	
T1622	Debugger Evasion	Defense Evasion	