KVMX

Evidence-First Malware Analysis

Analysis Report: 63545fa19548.bin

Verdict: MALICIOUS

63545fa19548.bin is a 32-bit executable with 5 sections. Packer detected: Unknown packer (high entropy in .rdata). Verdict: malicious.

Analysis Overview

Score: 9/10

Threat level: Malicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Native API
- Shared Modules
- Data Encrypted for Impact
- Service Stop
- Debugger Evasion

Hashes

SHA-256:	63545fa195488ff51955f09833332b9660d18f8afb16bdf579134661962e548a
SHA-1:	e686139d5ed8528117ba6ca68fe415e4fb02f2be
MD5:	5b7e6e352bacc93f7b80bc968b6ea493
Size:	399,360 bytes

Packer Detection

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

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x128B
Sections:	5

Name	Virtual Size	Entropy
.text	0x44C2	6.43
.rdata	0x5A810	7.76
.data	0x18C0	2.49

.rsrc	0xB0C	5.42
.reloc	0xAFE	4.02

Imports

KERNEL32.dll

- GetFullPathNameA
- CreateFileA
- HeapAlloc
- HeapFree
- GetProcessHeap
- ExpandEnvironmentStringsA
- WriteFile
- CloseHandle
- HeapReAlloc
- GetStringTypeW

SHELL32.dll

- ShellExecuteA

Strings (200 found)

```
!This program cannot be run in DOS mode.
YRichS
.text
`.rdata
@.data
.rsrc
@.reloc
QVWh
h0x@
YQPVh
hLa@
8csm
hda@
hTa@
uTVWh
5T`@
h<k@
PPPPP
<v*V
^SSSSS
t$<"u
t?VSP
Y[_^
PPPPP
>"u&
< tK<
wf93t
f90u
f90u
=h`@
VVV+
@PSVV
```

```
t*VV
j@j ^V
SWf9M
j@j
F\pk@
F\=pk@
5H`@
hPl@
hDl@
h8l@
h0l@
=T`@
Y__^[
9csm
5('F
t!Ht
5<'F
PPPPP
```

... and 150 more

Indicators of Compromise (1)

File paths (1)

```
/dd/yy
```

MITRE ATT&CK (7)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1106	Native API	Execution	
T1129	Shared Modules	Execution	
T1486	Data Encrypted for Impact	Impact	
T1489	Service Stop	Impact	
T1622	Debugger Evasion	Defense Evasion	