KVMX

Evidence-First Malware Analysis

Analysis Report: 7056ca2f6a9f.bin

Verdict: SUSPICIOUS

7056ca2f6a9f.bin is a 64-bit executable with 10 sections. Packer detected: Unknown packer (high entropy in .rsrc). Verdict: suspicious.

Analysis Overview

Score: 5/10

Threat level: Suspicious

Malicious Activity Summary

- Obfuscated Files or Information
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Indicator Removal: File Deletion
- Application Layer Protocol: Web Protocols
- Native API
- Modify Registry
- Screen Capture
- Clipboard Data
- Shared Modules
- Data Encrypted for Impact
- Service Stop
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion

Hashes

SHA-256:	7056ca2f6a9f3c525845b116c7bf564ced3284a4083ea80d7e9ef51a16f612c4
SHA-1:	5a6860bc33f3e965c333ae8c593b90ad6a9459f1
MD5:	751adc0b31a17f79d479c3b7a274c6da
Size:	1,708,656 bytes

Packer Detection

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

PE Information

Architecture:	64-bit
Type:	Executable

Entry Point: 0xBF894

Sections: 10

Name	Virtual Size	Entropy
.text	0xECFB6	6.45
.rdata	0x44ACC	5.4
.data	0x420C	2.08
.pdata	0x71DC	5.91
.00cfg	0x38	0.51
.gxfg	0x2AE0	5.14
.tls	0x11	0.0
_RDATA	0x15C	3.24
.rsrc	0x5B440	7.82
.reloc	0x21F0	5.44

Imports

GDI32.dll

- BitBlt
- CreateBitmap
- CreateCompatibleBitmap
- CreateCompatibleDC
- CreateFontA
- CreateFontIndirectA
- CreatePalette
- CreatePen
- CreateSolidBrush
- DeleteDC

IMM32.dll

- ImmGetCompositionStringW
- ImmGetContext
- ImmReleaseContext
- ImmSetCompositionFontA
- ImmSetCompositionWindow

ole32.dll

- CoCreateInstance
- CoInitialize
- CoUninitialize

USER32.dll

- AppendMenuA
- BeginPaint
- CheckDlgButton
- CheckMenuItem
- CheckRadioButton
- CloseClipboard
- CreateCaret
- CreateDialogParamA
- CreateMenu
- CreatePopupMenu

KERNEL32.dll

- Beep

ClearCommBreak
CloseHandle
CompareStringW
ConnectNamedPipe
CreateEventA
CreateFileA
CreateFileMappingA
CreateFileW
CreateMutexA

SHELL32.dll

ShellExecuteA

COMDLG32.dll

ChooseColorA
ChooseFontA
GetOpenFileNameA
GetOpenFileNameW
GetSaveFileNameA
GetSaveFileNameW

ADVAPI32.dll

AllocateAndInitializeSid
CopySid
EqualSid
GetLengthSid
GetUserNameA
InitializeSecurityDescriptor
RegCloseKey
RegCreateKeyExA
RegDeleteKeyA
RegEnumKeyA

Strings (200 found)

```
!This program cannot be run in DOS mode.$
.text
`.rdata
@.data
.pdata
@.00cfg
@.gxfg
@.tls
_RDATA
@.rsrc
@.reloc
VWSH
D$pL
L$xH
D$8H
\$pH
\$(H
L$8H1
@[_^
D$hH
L$hH1
```

D$(H
D$PH
D$`H
AWAVAUATVWUSH
A+EHA
A+ED
D$TI
D$h1
\$pL
\$pI
D$ L
L$ L
D$ L
t$pH
L$TA
\$(H
A9EDu
A9MH
A+uD
u0A+MH
D$TL
t fA
M8A+EH
D$TD
A+ED
tFE9
A+EHA
A+ED
D$0D
... and 150 more

Indicators of Compromise (1)

IPv4 addresses (1)

```
3.2.1.0
```

MITRE ATT&CK (14)

Technique	Name	Tactic	Source
T1027	Obfuscated Files or Information	Defense Evasion	
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1071.001	Application Layer Protocol: Web	Command and Control	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1113	Screen Capture	Collection	
T1115	Clipboard Data	Collection	
T1129	Shared Modules	Execution	
T1486	Data Encrypted for Impact	Impact	
T1489	Service Stop	Impact	

T1574.002	Hijack Execution Flow: DLL Side-	Privilege Escalation	
T1622	Debugger Evasion	Defense Evasion	