KVMX

Evidence-First Malware Analysis

Analysis Report: b3e1e9d97d74.bin

Verdict: SUSPICIOUS

b3e1e9d97d74.bin is a 32-bit executable with 4 sections. Verdict: suspicious.

Analysis Overview

Score: 5/10

Threat level: Suspicious

Malicious Activity Summary

- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Indicator Removal: File Deletion
- Native API
- Modify Registry
- Clipboard Data
- Shared Modules
- Debugger Evasion

Hashes

SHA-256:	b3e1e9d97d74c416c2a30dd11858789af5554cf2de62f577c13944a19623777d
SHA-1:	c07dfdea8da2da5bad036e7c2f5d37582e1cf684
MD5:	fe1bc60a95b2c2d77cd5d232296a7fa4
Size:	320,760 bytes

Packer Detection

No packer detected.

PE Information

Architecture:	32-bit
Type:	Executable
Entry Point:	0x497A0
Sections:	4

Name	Virtual Size	Entropy
.text	0x493E5	6.29
.rdata	0x291E	5.68
.data	0x1A8	2.7
.rsrc	0xB30	3.63

Imports

KERNEL32.dll

- CreateFileW
- LoadLibraryA
- lstrlenA
- lstrcpyA
- lstrcmpW
- WriteFile
- WriteConsoleInputW
- WideCharToMultiByte
- WaitForSingleObject
- WaitForMultipleObjects

USER32.dll

- SetKeyboardState
- SetForegroundWindow
- SetFocus
- SetCursor
- SendMessageW
- SendIMEMessageExW
- RegisterDeviceNotificationW
- RegisterClassW
- PostMessageW
- PeekMessageW

GDI32.dll

- SelectObject
- SetBrushOrgEx
- SetDCBrushColor
- SetICMMode
- SetPixelV
- CancelDC
- PathToRegion
- CloseFigure
- GetBkColor
- AbortDoc

ADVAPI32.dll

- RegEnumValueW
- RegOpenKeyW
- StartServiceCtrlDispatcherW
- SetServiceStatus
- SetSecurityDescriptorOwner
- SetSecurityDescriptorDacl
- SetEntriesInAclW
- ReportEventW
- RegisterServiceCtrlHandlerExW
- RegisterEventSourceW

SHELL32.dll

- Shell_NotifyIconW
- ShellExecuteExA
- SHPathPrepareForWriteW
- SHLoadNonloadedIconOverlayIdentifiers
- SHInvokePrinterCommandW
- SHGetSpecialFolderPathA

SHGetSpecialFolderLocation

SHGetSettings

SHGetPathFromIDListW

SHGetMalloc

SHLWAPI.dll

StrChrW

StrCmpNIA

StrCmpNIW

StrCmpNW

StrRChrA

StrRChrIA

StrRStrIW

StrStrIA

StrChrA

COMCTL32.dll

InitCommonControlsEx

msvcrt.dll

__p__commode

__p__fmode

__set_app_type

__setusermatherr

_abnormal_termination

_acmdln

_adjust_fdiv

_c_exit

_cexit

_controlfp

IMM32.dll

ImmDisableIME

Strings (200 found)

```
!This program cannot be run in DOS mode.
+Rich
.text
`.rdata
@.data
.rsrc
ta}3mlv
Dx`r
dn`r
88me`rVrx
ootVce
o D=R ]
een{
88t!
888t
dxts
`tin
8p88
88N.
u( 88
uQW?i
```

```
88 !4
B8(W3F
t<88
t9sw:
/OHv
QW 0-d
"vf8
A88)
X!k0
ARSm2
88n8]
*%Ok
8imYH:88j
?UQh
hL%A
St88
udRt
u\d] F
_ J9
h$!A
886t
=4FC
54?C
@8Mt
;.88|
5(887C
36?t
xn8uD
8q882
```
... and 150 more

MITRE ATT&CK (8)

Technique	Name	Tactic	Source
T1055.001	Process Injection: Dynamic-link	Defense Evasion	
T1056.001	Input Capture: Keylogging	Credential Access	
T1070.004	Indicator Removal: File Deletion	Defense Evasion	
T1106	Native API	Execution	
T1112	Modify Registry	Defense Evasion	
T1115	Clipboard Data	Collection	
T1129	Shared Modules	Execution	
T1622	Debugger Evasion	Defense Evasion	