# KVMX

Evidence-First Malware Analysis

## Analysis Report: c851749fd6c9.bin

### Verdict: MALICIOUS

c851749fd6c9.bin is a 32-bit executable with 4 sections. Verdict: malicious.

## Analysis Overview

# Score: 9/10

### Threat level: Malicious

**Malicious Activity Summary**

- Family: info-stealer-like
- Obfuscated Files or Information
- Process Injection
- Process Injection: Dynamic-link Library Injection
- Input Capture: Keylogging
- Process Discovery
- Indicator Removal: File Deletion
- Application Layer Protocol: Web Protocols
- Ingress Tool Transfer
- Native API
- Modify Registry
- Screen Capture
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Credentials from Password Stores: Credentials from Web Browsers

## Hashes

| | |
|---|---|
| **SHA-256:** | c851749fd6c9fa19293d8ee2c5b45b3dc8561115ddfe7166fbaefcb9b353b7c4 |
| **SHA-1:** | c7ccd43a721a508b807c9bf6d774344df58e752f |
| **MD5:** | fb598b93c04baafe98683dc210e779c9 |
| **Size:** | 94,208 bytes |

## Packer Detection

No packer detected.

## PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0xFD88 |

**Sections:** 4

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0xEFDA | 6.06 |
| .rdata | 0x4A92 | 5.37 |
| .data | 0xC24 | 0.58 |
| .rsrc | 0xEDC | 6.58 |

## Imports

**KERNEL32.dll**

- GetModuleFileNameA
- GetLongPathNameA
- CreateMutexA
- OpenMutexA
- Process32Next
- Process32First
- CreateToolhelp32Snapshot
- SizeofResource
- LockResource
- LoadResource

**USER32.dll**

- GetWindowTextLengthA
- GetForegroundWindow
- UnhookWindowsHookEx
- CloseClipboard
- GetClipboardData
- OpenClipboard
- SetClipboardData
- EmptyClipboard
- ExitWindowsEx
- MessageBoxA

**GDI32.dll**

- CreateDCA
- CreateCompatibleDC
- GetDeviceCaps
- CreateCompatibleBitmap
- SelectObject
- StretchBlt
- GetObjectA
- GetDIBits
- DeleteObject
- DeleteDC

**ADVAPI32.dll**

- OpenProcessToken
- LookupPrivilegeValueA
- AdjustTokenPrivileges
- RegCreateKeyExA
- RegQueryInfoKeyA
- RegEnumKeyExA
- RegEnumValueA
- RegDeleteValueA

RegCreateKeyA

RegSetValueExA

**SHELL32.dll**

ShellExecuteA

ExtractIconA

Shell_NotifyIconA

ShellExecuteExA

ShellExecuteW

**MSVCP60.dll**

?begin@?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAEPADXZ

?end@?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAEPADXZ

?assign@?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAEAAV12@ABV12@@Z

?replace@?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAEAAV12@IIPBD@Z

??8std@@YA_NPBDABV?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@0@@Z

??Y?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAEAAV01@PBD@Z

??4?$basic_string@GU?$char_traits@G@std@@V?$allocator@G@2@@std@@QAEAAV01@ABV01@@Z

??0?$basic_string@GU?$char_traits@G@std@@V?$allocator@G@2@@std@@QAE@ABV?$allocator@G@1@@Z

?find_last_of@?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QBEIDI@Z

??9std@@YA_NABV?$basic_string@GU?$char_traits@G@std@@V?$allocator@G@2@@0@PBG@Z

**MSVCRT.dll**

_wrename

_controlfp

__set_app_type

__p__fmode

__p__commode

_adjust_fdiv

__setusermatherr

_initterm

__getmainargs

_acmdln

**WINMM.dll**

waveInOpen

waveInStop

waveInClose

waveInAddBuffer

waveInPrepareHeader

waveInUnprepareHeader

waveInStart

**SHLWAPI.dll**

PathFileExistsA

**WS2_32.dll**

htons

gethostbyname

closesocket

socket

send

WSAGetLastError

connect

recv

WSAStartup

**urlmon.dll**

URLDownloadToFileA

**gdiplus.dll**

- GdipLoadImageFromStreamICM
- GdipDisposeImage
- GdipCloneImage
- GdipAlloc
- GdipSaveImageToStream
- GdipSaveImageToFile
- GdipLoadImageFromStream
- GdiplusStartup
- GdipGetImageEncoders
- GdipFree

**WININET.dll**

- InternetCloseHandle
- InternetOpenUrlA
- InternetOpenA
- InternetReadFile

## Strings (200 found)

```
!This program cannot be run in DOS mode.
vu^vi
vu^viq^
wu^&ps^
vu^vi~^
vu^Rich
.text
`.rdata
@.data
.rsrc
WWWh
WWWh
hXMV
hXMV
VWtF
hXQA
5XQA
5XQA
5XQA
VPj
5XQA
^Vj"
=hQA
=lQA
=pQA
=tQA
YYj V
=ARA
%ARA
YYPVhT
hhRA
PPQh
hXRA
hXRA
hxRA
```

SSVh#(@
=8YA
tl9~8tg
8F4t{8
tk8E
F<;F8r
8^5uu8
^5^3
_^[]
WVhd
h;,@
hxRA
E(PVh
YYPVh
E8PV
*... and 150 more*

## Malware Config

**Family:** info-stealer-like

## MITRE ATT&CK (15)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1027 | Obfuscated Files or Information | Defense Evasion | |
| T1055 | Process Injection | Defense Evasion | |
| T1055.001 | Process Injection: Dynamic-link | Defense Evasion | |
| T1056.001 | Input Capture: Keylogging | Credential Access | |
| T1057 | Process Discovery | Discovery | |
| T1070.004 | Indicator Removal: File Deletion | Defense Evasion | |
| T1071.001 | Application Layer Protocol: Web | Command and Control | |
| T1105 | Ingress Tool Transfer | Command and Control | |
| T1106 | Native API | Execution | |
| T1112 | Modify Registry | Defense Evasion | |
| T1113 | Screen Capture | Collection | |
| T1115 | Clipboard Data | Collection | |
| T1129 | Shared Modules | Execution | |
| T1134 | Access Token Manipulation | Privilege Escalation | |
| T1555.003 | Credentials from Password Stores | Credential Access | |