# KVMX

Evidence-First Malware Analysis

## Analysis Report: 18aab0e981ee.bin

### Verdict: MALICIOUS

18aab0e981ee.bin is a 32-bit executable with 5 sections. Verdict: malicious.

## Analysis Overview

# Score: 9/10

### Threat level: Malicious

**Malicious Activity Summary**

- Indicator Removal: File Deletion
- Application Layer Protocol: Web Protocols
- File and Directory Discovery
- Native API
- Modify Registry
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading

## Hashes

| | |
|---|---|
| **SHA-256:** | 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9 |
| **SHA-1:** | e4b8f4b6cab18b9748f83e9fffd275ef5276199e |
| **MD5:** | cce284cab135d9c0a2a64a7caec09107 |
| **Size:** | 2,932,642 bytes |

## Packer Detection

No packer detected.

## PE Information

| | |
|---|---|
| **Architecture:** | 32-bit |
| **Type:** | Executable |
| **Entry Point:** | 0x33C4 |
| **Sections:** | 5 |

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0x631A | 6.45 |
| .rdata | 0x1384 | 5.14 |
| .data | 0x20318 | 3.9 |

| | | |
|---|---|---|
| .ndata | 0x1C000 | 0.0 |
| .rsrc | 0x4260 | 5.92 |

## Imports

**KERNEL32.dll**

- SetEnvironmentVariableW
- SetFileAttributesW
- Sleep
- GetTickCount
- GetFileSize
- GetModuleFileNameW
- GetCurrentProcess
- CopyFileW
- SetCurrentDirectoryW
- GetFileAttributesW

**USER32.dll**

- GetWindowRect
- GetSystemMenu
- SetClassLongW
- IsWindowEnabled
- SetWindowPos
- GetSysColor
- GetWindowLongW
- SetCursor
- LoadCursorW
- CheckDlgButton

**GDI32.dll**

- SelectObject
- SetTextColor
- SetBkMode
- CreateFontIndirectW
- CreateBrushIndirect
- DeleteObject
- GetDeviceCaps
- SetBkColor

**SHELL32.dll**

- ShellExecuteExW
- SHGetPathFromIDListW
- SHGetSpecialFolderLocation
- SHGetFileInfoW
- SHFileOperationW
- SHBrowseForFolderW

**ADVAPI32.dll**

- AdjustTokenPrivileges
- RegCreateKeyExW
- RegOpenKeyExW
- SetFileSecurityW
- OpenProcessToken
- LookupPrivilegeValueW
- RegEnumValueW
- RegDeleteKeyW
- RegDeleteValueW

RegCloseKey

**COMCTL32.dll**

ImageList_Create

ImageList_AddMasked

ImageList_Destroy

**ole32.dll**

OleUninitialize

OleInitialize

CoTaskMemFree

CoCreateInstance

## Strings (200 found)

```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.ndata
.rsrc
 s495L
tZj\V
>FFf;
v'f9
ur9]
uOWh
tDH;
PWhr
jHjZW
t99]
PSWV
VQSPW
QVPW
SQVPW
8u/j!
Y;=L
t%9]
PjdQ
v#Vh`.@
(SV3
Instu`
softuW
NulluN
YtS9]
j@Vh@
tI+E
tG9u
SVWj _3
D$4h
j [f;
AAf9
Aj"A[f
u6Wh
t*Vh
```

t-SV

D$ Ph0

D$$SPS

Vj%SSS

WSWh

tWf="

WPWj0

D$$+D$

D$,+D$$P

*... and 150 more*

## Indicators of Compromise (1)

### IPv4 addresses (1)

1.0.0.0

## MITRE ATT&CK (9)

| Technique | Name | Tactic | Source |
|---|---|---|---|
| T1070.004 | Indicator Removal: File Deletion | Defense Evasion | |
| T1071.001 | Application Layer Protocol: Web | Command and Control | |
| T1083 | File and Directory Discovery | Discovery | |
| T1106 | Native API | Execution | |
| T1112 | Modify Registry | Defense Evasion | |
| T1115 | Clipboard Data | Collection | |
| T1129 | Shared Modules | Execution | |
| T1134 | Access Token Manipulation | Privilege Escalation | |
| T1574.002 | Hijack Execution Flow: DLL Side- | Privilege Escalation | |