# KVMX

Evidence-First Malware Analysis

## Analysis Report: dd396a3f66ad.bin

### Verdict: MALICIOUS

dd396a3f66ad.bin is a 32-bit executable with 5 sections. Packer detected: Unknown packer (high entropy in .rsrc). Verdict: malicious.

### Analysis Overview

# Score: 9/10

### Threat level: Malicious

**Malicious Activity Summary**

- Family: loader-multi-stage
- 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
- System Information Discovery
- Ingress Tool Transfer
- Native API
- Brute Force
- Modify Registry
- Clipboard Data
- Shared Modules
- Access Token Manipulation
- Hijack Execution Flow: DLL Side-Loading
- Debugger Evasion

### Hashes

| | |
|---|---|
| **SHA-256:** | dd396a3f66ad728660023cb116235f3cb1c35d679a155b08ec6a9ccaf966c360 |
| **SHA-1:** | 0610e911ade5d666a45b41f771903170af58a05a |
| **MD5:** | 5df0cf8b8aa7e56884f71da3720fb2c6 |
| **Size:** | 10,508,800 bytes |

### Packer Detection

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

### PE Information

**Architecture:** 32-bit

**Type:** Executable

**Entry Point:** 0x27F4A

**Sections:** 5

| Name | Virtual Size | Entropy |
|---|---|---|
| .text | 0x8DD2E | 6.68 |
| .rdata | 0x2E10E | 5.76 |
| .data | 0x8F74 | 1.2 |
| .rsrc | 0x93D1A0 | 8.0 |
| .reloc | 0x7130 | 6.78 |

## Imports

**WSOCK32.dll**

- WSACleanup
- socket
- ioctlsocket
- setsockopt
- ntohs
- recvfrom
- inet_addr
- htons
- WSAStartup
- __WSAFDIsSet

**VERSION.dll**

- GetFileVersionInfoW
- GetFileVersionInfoSizeW
- VerQueryValueW

**WINMM.dll**

- timeGetTime
- waveOutSetVolume
- mciSendStringW

**COMCTL32.dll**

- ImageList_ReplaceIcon
- ImageList_Destroy
- ImageList_Remove
- ImageList_SetDragCursorImage
- ImageList_BeginDrag
- ImageList_DragEnter
- ImageList_DragLeave
- ImageList_EndDrag
- ImageList_DragMove
- InitCommonControlsEx

**MPR.dll**

- WNetUseConnectionW
- WNetCancelConnection2W
- WNetGetConnectionW
- WNetAddConnection2W

**WININET.dll**

- InternetQueryDataAvailable

InternetCloseHandle
InternetOpenW
InternetSetOptionW
InternetCrackUrlW
HttpQueryInfoW
InternetQueryOptionW
HttpOpenRequestW
HttpSendRequestW
FtpOpenFileW

**PSAPI.DLL**

GetProcessMemoryInfo

**IPHLPAPI.DLL**

IcmpCreateFile
IcmpCloseHandle
IcmpSendEcho

**USERENV.dll**

DestroyEnvironmentBlock
UnloadUserProfile
CreateEnvironmentBlock
LoadUserProfileW

**UxTheme.dll**

IsThemeActive

**KERNEL32.dll**

DuplicateHandle
CreateThread
WaitForSingleObject
HeapAlloc
GetProcessHeap
HeapFree
Sleep
GetCurrentThreadId
MultiByteToWideChar
MulDiv

**USER32.dll**

AdjustWindowRectEx
CopyImage
SetWindowPos
GetCursorInfo
RegisterHotKey
ClientToScreen
GetKeyboardLayoutNameW
IsCharAlphaW
IsCharAlphaNumericW
IsCharLowerW

**GDI32.dll**

StrokePath
DeleteObject
GetTextExtentPoint32W
ExtCreatePen
GetDeviceCaps
EndPath
SetPixel
CloseFigure

CreateCompatibleBitmap

CreateCompatibleDC

**COMDLG32.dll**

GetOpenFileNameW

GetSaveFileNameW

**ADVAPI32.dll**

GetAce

RegEnumValueW

RegDeleteValueW

RegDeleteKeyW

RegEnumKeyExW

RegSetValueExW

RegOpenKeyExW

RegCloseKey

RegQueryValueExW

RegConnectRegistryW

**SHELL32.dll**

DragQueryPoint

ShellExecuteExW

DragQueryFileW

SHEmptyRecycleBinW

SHGetPathFromIDListW

SHBrowseForFolderW

SHCreateShellItem

SHGetDesktopFolder

SHGetSpecialFolderLocation

SHGetFolderPathW

**ole32.dll**

CoTaskMemAlloc

CoTaskMemFree

CLSIDFromString

ProgIDFromCLSID

CLSIDFromProgID

OleSetMenuDescriptor

MkParseDisplayName

OleSetContainedObject

CoCreateInstance

IIDFromString

**OLEAUT32.dll**

LoadTypeLibEx

VariantCopyInd

SysReAllocString

SysFreeString

SafeArrayDestroyDescriptor

SafeArrayDestroyData

SafeArrayUnaccessData

SafeArrayAccessData

SafeArrayAllocData

SafeArrayAllocDescriptorEx

## Strings (200 found)

```
!This program cannot be run in DOS mode.
```

```
RichR
.text
`.rdata
@.data
.rsrc
@.reloc
u/;u
9=tXL
=tXL
5xXL
=lXL
=lXL
5dXL
%hXL
%dXL
t\HH
\SVW
D$(P
%hXL
%dXL
D$(P
WSPV
_^[]
~LWS
Iu-V
#E(VW
99u1
_^[]
98u[
uaSVW
t$8]4t
Pj0V
9^Xt=9^\tE
QQSVW
=4XL
54XL
54XL
98u#h
;Gxs
;Gds
^j|Xf
50XL
=DXL
=HXL
%@XL
(SVWh
8V:t
tC~)
uVWQ
```

*... and 150 more*

## Malware Config

**Family:** loader-multi-stage

## MITRE ATT&CK (17)

| 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 | |
| T1082 | System Information Discovery | Discovery | |
| T1105 | Ingress Tool Transfer | Command and Control | |
| T1106 | Native API | Execution | |
| T1110 | Brute Force | Credential Access | |
| 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 | |
| T1622 | Debugger Evasion | Defense Evasion | |