



Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **JkDefragU3_110.exe** received on **2009.11.16 21:08:10 (UTC)**

Current status: **finished**

Result: **0/41 (0%)**

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.41	2009.11.16	-
AhnLab-V3	5.0.0.2	2009.11.16	-
AntiVir	7.9.1.65	2009.11.16	-
Antiy-AVL	2.0.3.7	2009.11.16	-
Authentium	5.2.0.5	2009.11.16	-
Avast	4.8.1351.0	2009.11.16	-
AVG	8.5.0.425	2009.11.16	-
BitDefender	7.2	2009.11.16	-
CAT-QuickHeal	10.00	2009.11.16	-
ClamAV	0.94.1	2009.11.16	-
Comodo	2958	2009.11.16	-
DrWeb	5.0.0.12182	2009.11.16	-
eSafe	7.0.17.0	2009.11.16	-
eTrust-Vet	35.1.7123	2009.11.16	-
F-Prot	4.5.1.85	2009.11.16	-
F-Secure	9.0.15370.0	2009.11.11	-
Fortinet	3.120.0.0	2009.11.16	-
GData	19	2009.11.16	-
Ikarus	T3.1.1.74.0	2009.11.16	-
Jiangmin	11.0.800	2009.11.16	-
K7AntiVirus	7.10.897	2009.11.16	-
Kaspersky	7.0.0.125	2009.11.16	-
McAfee	5804	2009.11.16	-
McAfee+Artemis	5804	2009.11.16	-

McAfee-GW-Edition	6.8.5	2009.11.16	-
Microsoft	1.5202	2009.11.16	-
NOD32	4613	2009.11.16	-
Norman	6.03.02	2009.11.16	-
nProtect	2009.1.8.0	2009.11.16	-
Panda	10.0.2.2	2009.11.16	-
PCTools	7.0.3.5	2009.11.16	-
Prevx	3.0	2009.11.16	-
Rising	22.22.00.08	2009.11.16	-
Sophos	4.47.0	2009.11.16	-
Sunbelt	3.2.1858.2	2009.11.12	-
Symantec	1.4.4.12	2009.11.16	-
TheHacker	6.5.0.2.071	2009.11.16	-
TrendMicro	9.0.0.1003	2009.11.16	-
VBA32	3.12.10.11	2009.11.15	-
ViRobot	2009.11.16.2039	2009.11.16	-
VirusBuster	4.6.5.0	2009.11.16	-

Additional information

File size: 4694016 bytes

MD5...: 42d314b849233a3168b7ef0865cf1aa6

SHA1...: 36901e4f64c7735923a50ea3884f1618c098ef57

SHA256: b6a318005fbf36a340534a8e1975e7fd9064cbe283c2979071a11e3542ccf1ba

ssdeep: 98304:kxF14cHAB5g/fHBQ2KwWU5wJYShtrDVxWIfYwnS8u/IkRyLIU:kxFlwBS/
+VwW7JDtrD3JAnRyLIU

PEiD...: -

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0x1be36

timedatestamp.....: 0x443a0518 (Mon Apr 10 07:11:20 2006)

machinetype.....: 0x14c (I386)

(4 sections)

name viradd virsiz rawdsiz ntrpy md5

.text 0x1000 0x385ed 0x39000 6.55 0090e44fa5bc2837f44c4830722a873c

.rdata 0x3a000 0xe7fa 0xf000 4.78 647cfa1253caf1c655995affc337d5f4

.data 0x49000 0x5f74 0x3000 3.48 abd4e83f8c668f3b12fafdc4d04bf119

.rsrc 0x4f000 0x42da80 0x42e000 7.91 81ac288d6583f32e294730ca60f56b25

(12 imports)

> KERNEL32.dll: WritePrivateProfileStringW, lstrcpw, GlobalFlags,
FlushFileBuffers, LockFile, UnlockFile, SetEndOfFile, DuplicateHandle,
FindClose, FindFirstFileW, GetVolumeInformationW, GetFullPathNameW,
SetErrorMode, FileTimeToLocalFileTime, GetFileAttributesW, GetFileTime,
GetTickCount, GetStartupInfoW, RtlUnwind, ExitProcess, TerminateProcess,
HeapFree, HeapAlloc, HeapReAlloc, VirtualProtect, VirtualAlloc,
GetSystemInfo, VirtualQuery, HeapSize, GetStdHandle, GetModuleFileNameA,
UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings,

FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA,
GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, HeapDestroy,
HeapCreate, VirtualFree, QueryPerformanceCounter,
SetUnhandledExceptionFilter, IsBadWritePtr, LCMAPStringA, LCMAPStringW,
GetTimeZoneInformation, GetOEMCP, GetCPInfo, IsBadReadPtr, IsBadCodePtr,
GetStringTypeA, GetStringTypeW, SetStdHandle, CompareStringA,
CompareStringW, SetEnvironmentVariableA, TlsFree, LocalReAlloc,
TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle,
GlobalReAlloc, LeaveCriticalSection, InterlockedIncrement,
FileTimeToSystemTime, GlobalFindAtomW, GetModuleHandleA, LoadLibraryA,
lstrcatW, GetVersionExA, GlobalAddAtomW, GetCurrentThread, lstrcmpW,
GlobalDeleteAtom, ConvertDefaultLocale, GetVersion, GetLocaleInfoW,
lstrlenA, InterlockedDecrement, SetLastError, lstrcpyW, lstrcpynW,
WideCharToMultiByte, LoadLibraryW, MulDiv, GlobalAlloc, GlobalLock,
GlobalUnlock, GlobalFree, FormatMessageW, LocalAlloc, LocalFree, lstrlenW,
WriteFile, FreeResource, CreateFileW, GetFileSize, LoadLibraryExW,
FreeLibrary, SetFilePointer, ReadFile, CreateMutexW, GetCurrentProcessId,
GetCurrentProcess, GetProcessTimes, ReleaseMutex, WaitForSingleObject,
UnmapViewOfFile, CreateFileMappingW, MapViewOfFileEx, GetCurrentThreadId,
DeleteCriticalSection, InitializeCriticalSection, RaiseException,
GetModuleFileNameW, FindResourceExW, CreateDirectoryW, OutputDebugStringW,
GetSystemTimeAsFileTime, Sleep, GetDiskFreeSpaceExW, GetLastError,
MultiByteToWideChar, OpenProcess, CloseHandle, GetThreadLocale,
GetLocaleInfoA, GetACP, InterlockedExchange, GetVersionExW,
GetModuleHandleW, GetProcAddress, GetUserDefaultLangID,
EnumResourceLanguagesW, VerLanguageNameW, LoadResource, LockResource,
SizeofResource, FindResourceW, GetProcessHeap
> USER32.dll: BeginPaint, EndPaint, DestroyMenu, GetSysColorBrush,
CharUpperW, CharNextW, SetRect, CopyAcceleratorTableW, InvalidateRgn,
SetCapture, ReleaseCapture, GetNextDlgGroupItem, MessageBeep,
RegisterClipboardFormatW, PostThreadMessageW, RegisterWindowMessageW,
WinHelpW, GetCapture, CreateWindowExW, GetClassInfoExW, GetClassLongW,
SetPropW, GetPropW, RemovePropW, SendDlgItemMessageW, SendDlgItemMessageA,
SetFocus, IsChild, GetWindowTextLengthW, GetWindowTextW, SetActiveWindow,
GetTopWindow, DestroyWindow, GetMessageTime, GetMessagePos,
MapWindowPoints, AdjustWindowRectEx, ScreenToClient, EqualRect,
GetClassInfoW, RegisterClassW, ClientToScreen, CallWindowProcW,
IntersectRect, SystemParametersInfoA, GetWindowPlacement, PtInRect,
GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDlgItem,
SetMenuItemBitmaps, GetFocus, ModifyMenuW, EnableMenuItem, CheckMenuItem,
GetMenuCheckMarkDimensions, GetLastActivePopup, IsWindowEnabled, SetCursor,
PostQuitMessage, SetWindowsHookExW, CallNextHookEx, GetMessageW,
DispatchMessageW, GetActiveWindow, IsWindowVisible, GetKeyState,
PeekMessageW, GetCursorPos, ValidateRect, UnhookWindowsHookEx,
GetMenuState, GetMenuItemID, GetMenuItemCount, GetSubMenu, SetWindowLongW,
IsWindow, LoadBitmapW, wsprintfW, DrawStateW, DestroyIcon, SetWindowLongW,
DrawFocusRect, DrawEdge, GetWindowDC, LoadImageW, GetClassNameW,
GetComboBoxInfo, CopyRect, RedrawWindow, UpdateWindow, GetParent,
InvalidateRect, OffsetRect, IsRectEmpty, CreateDialogIndirectParamW,
GetNextDlgTabItem, EndDialog, GetSysColor, GetSystemMetrics, GrayStringW,
ShowWindow, MoveWindow, SetWindowTextW, GetDlgCtrlID, IsDialogMessageW,
DrawTextExW, DrawTextW, TabbedTextOutW, SetWindowRgn, IsIconic, GetMenu,
DrawIcon, GetClientRect, ReleaseDC, GetDC, GetWindowRect, FrameRect,
InflateRect, GetForegroundWindow, SetForegroundWindow, SendMessageW,
UnregisterClassW, LoadCursorW, SetSystemCursor, SendMessageTimeoutW,
PostMessageW, EnableWindow, LoadIconW, LoadStringA, GetDesktopWindow,
MessageBoxA, MessageBoxW, TranslateMessage, DefWindowProcW
> GDI32.dll: GetViewportExtEx, GetWindowExtEx, OffsetViewportOrgEx,
SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, SetWindowExtEx,
ScaleWindowExtEx, ExtSelectClipRgn, DeleteDC, CreateRectRgnIndirect,
GetRgnBox, SetBkMode, RestoreDC, SaveDC, SetBkColor, SetTextColor,

```

GetClipboard, SetTextAlign, GetTextExtentPoint32W, CreateFontIndirectW,
SetMapMode, CreateSolidBrush, CreateRectRgn, CombineRgn, DeleteObject,
GetPixel, CreateBitmap, GetDeviceCaps, SelectObject, PatBlt, GetTextColor,
GetStockObject, GetViewportOrgEx, SetViewportOrgEx, GetObjectW, Escape,
ExtTextOutW, TextOutW, RectVisible, PtVisible, BitBlt, LPToDP, DPToLP,
GetMapMode, GetBkColor, CreateCompatibleDC, CreateCompatibleBitmap
> comdlg32.dll: GetFileTitleW
> WINSPOOL.DRV: OpenPrinterW, DocumentPropertiesW, ClosePrinter
> ADVAPI32.dll: RegQueryValueW, RegSetValueExW, RegCreateKeyExW,
RegCloseKey, RegEnumKeyW, RegDeleteKeyW, RegOpenKeyExW, RegQueryValueExW,
RegOpenKeyW
> SHELL32.dll: SHGetSpecialFolderPathW, SHGetFileInfoW
> COMCTL32.dll: -, _TrackMouseEvent
> SHLWAPI.dll: PathFindExtensionW, PathFindFileNameW, PathStripToRootW,
PathIsUNCW
> oledlg.dll: OleUIBusyW
> ole32.dll: StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes,
CoGetClassObject, CLSIDFromString, CLSIDFromProgID,
CoRegisterMessageFilter, CreateILockBytesOnHGlobal, CoTaskMemFree,
CreateStreamOnHGlobal, CoCreateInstance, CoInitialize, OleFlushClipboard,
OleIsCurrentClipboard, OleUninitialize, CoFreeUnusedLibraries,
OleInitialize, CoRevokeClassObject, CoTaskMemAlloc
> OLEAUT32.dll: -, -, -, -, -, -, -, -, -, -, -, -, -, -

( 0 exports )

RDS...: NSRL Reference Data Set
-

pdfid.: -

sigcheck:
publisher.....: n/a
copyright.....: n/a
product.....: n/a
description...: n/a
original name: n/a
internal name: n/a
file version..: 0.1.1.0
comments.....: n/a
signers.....: -
signing date..: -
verified.....: Unsigned

trid...: InstallShield setup (40.4%)
Win32 Executable MS Visual C++ (generic) (35.4%)
Windows Screen Saver (12.3%)
Win32 Executable Generic (8.0%)
Generic Win/DOS Executable (1.8%)

packers (F-Prot): UPX_LZMA

```

! **ATTENTION:** VirusTotal is a free service offered by Hispasec Sistemas. There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, **these results DO NOT guarantee the harmlessness of a file.** Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and *malware*.

Another File

