

Srpski | Македонски | العربية | Suomi | ihMdl | 한국어 | עברית | 日本語 | Slovenščina | Dansk | Русский | Română | Türkçe | Nederlands | Ελληνικά | Français | Svenska | Português | Italiano | 繁體中文 | 简体中文 | Magyar | Deutsch | Český | Polski | Español



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\_115.exe** received on **2010.05.13 21:32:18 (UTC)**

Current status: **finished**

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

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.05.10	-
AhnLab-V3	2010.05.14.00	2010.05.13	-
AntiVir	8.2.1.242	2010.05.13	-
Antiy-AVL	2.0.3.7	2010.05.13	-
Authentium	5.2.0.5	2010.05.13	-
Avast	4.8.1351.0	2010.05.13	-
Avast5	5.0.332.0	2010.05.13	-
AVG	9.0.0.787	2010.05.13	-
BitDefender	7.2	2010.05.13	-
CAT-QuickHeal	10.00	2010.05.13	-
ClamAV	0.96.0.3-git	2010.05.13	-
Comodo	4833	2010.05.13	-
DrWeb	5.0.2.03300	2010.05.13	-
eSafe	7.0.17.0	2010.05.13	-
eTrust-Vet	35.2.7487	2010.05.13	-
F-Prot	4.5.1.85	2010.05.13	-
F-Secure	9.0.15370.0	2010.05.13	-
Fortinet	4.1.133.0	2010.05.13	-
GData	21	2010.05.13	-
Ikarus	T3.1.1.84.0	2010.05.13	-
Jiangmin	13.0.900	2010.05.13	-
Kaspersky	7.0.0.125	2010.05.13	-
McAfee	5.400.0.1158	2010.05.13	-
McAfee-GW-Edition	2010.1	2010.05.13	-

Microsoft	1.5703	2010.05.13	-
NOD32	5113	2010.05.13	-
Norman	6.04.12	2010.05.13	-
nProtect	2010-05-13.01	2010.05.13	-
Panda	10.0.2.7	2010.05.13	-
PCTools	7.0.3.5	2010.05.13	-
Prevx	3.0	2010.05.13	-
Rising	22.47.03.04	2010.05.13	-
Sophos	4.53.0	2010.05.13	-
Sunbelt	6299	2010.05.13	-
Symantec	20101.1.0.89	2010.05.13	-
TheHacker	6.5.2.0.280	2010.05.13	-
TrendMicro	9.120.0.1004	2010.05.13	-
TrendMicro-HouseCall	9.120.0.1004	2010.05.13	-
VBA32	3.12.12.4	2010.05.13	-
ViRobot	2010.5.13.2314	2010.05.13	-
VirusBuster	5.0.27.0	2010.05.13	-

#### Additional information

File size: 3661824 bytes

MD5...: 7b0821690172b27ddb438d1a24b04c5d

SHA1...: bc247a6ac7ec9cba5acf9bf158a77e489549873c

SHA256: 631f554f3862e8a3076daf3515834ad8f5db1f944f3739afcac3b753bc5f2883

ssdeep: 98304:yxFRDBBJ3V/2n/hA4OF8+panaNAwJjSoyl1NU:yxFRtBJF/Y/hA4E8uNXS91/U

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

.rsrsc 0x4f000 0x331408 0x332000 7.97 98bebcacf73255bf29178eff34e729fcc

( 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,

```
GetClipBox, 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.: -

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%)

Symantec Reputation Network: Suspicious.Insight

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2010-021223-0550-99](http://www.symantec.com/security_response/writeup.jsp?docid=2010-021223-0550-99)

packers (F-Prot): UPX\_LZMA

sigcheck:

publisher.....: n/a

copyright.....: n/a

product.....: n/a

description...: n/a

original name: n/a

internal name: n/a

file version..: 0.1.1.5

comments.....: n/a

signers.....: -

signing date..: -

verified.....: Unsigned

**!** **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

---

VirusTotal © [Hispacec Sistemas](#) -  [Blog](#) - Contact: [info@virustotal.com](mailto:info@virustotal.com) - [Terms of Service & Privacy Policy](#)