

VT Community [Sign in](#) ▼[Languages](#) ▼

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

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **JkDefragGUI.exe**
 Submission date: **2011-05-24 21:01:52 (UTC)**
 Current status: **finished**
 Result: **1/ 42 (2.4%)**

VT Community



not reviewed
 Safety score: -

[Compact](#)[Print results](#)

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.05.25.00	2011.05.24	-
AntiVir	7.11.8.126	2011.05.24	-
Antiy-AVL	2.0.3.7	2011.05.24	-
Avast	4.8.1351.0	2011.05.24	-
Avast5	5.0.677.0	2011.05.24	-
AVG	10.0.0.1190	2011.05.24	-
BitDefender	7.2	2011.05.24	-
CAT-QuickHeal	11.00	2011.05.24	-
ClamAV	0.97.0.0	2011.05.24	-
Commtouch	5.3.2.6	2011.05.24	-
Comodo	8822	2011.05.24	-
DrWeb	5.0.2.03300	2011.05.24	-
eSafe	7.0.17.0	2011.05.24	-
eTrust-Vet	36.1.8346	2011.05.24	-
F-Prot	4.6.2.117	2011.05.24	-
F-Secure	9.0.16440.0	2011.05.24	-
Fortinet	4.2.257.0	2011.05.22	-
GData	22	2011.05.24	-
Ikarus	T3.1.1.104.0	2011.05.24	-
Jiangmin	13.0.900	2011.05.24	Trojan/Refroso.ijp
K7AntiVirus	9.103.4713	2011.05.24	-
Kaspersky	9.0.0.837	2011.05.24	-
McAfee	5.400.0.1158	2011.05.24	-

McAfee-GW-Edition	2010.1D	2011.05.24	-
Microsoft	1.6903	2011.05.24	-
NOD32	6149	2011.05.24	-
Norman	6.07.07	2011.05.24	-
nProtect	2011-05-24.01	2011.05.24	-
Panda	10.0.3.5	2011.05.24	-
PCTools	7.0.3.5	2011.05.19	-
Prevx	3.0	2011.05.24	-
Rising	23.59.01.04	2011.05.24	-
Sophos	4.65.0	2011.05.24	-
SUPERAntiSpyware	4.40.0.1006	2011.05.24	-
Symantec	20111.1.0.186	2011.05.24	-
TheHacker	6.7.0.1.203	2011.05.23	-
TrendMicro	9.200.0.1012	2011.05.24	-
TrendMicro-HouseCall	9.200.0.1012	2011.05.24	-
VBA32	3.12.16.0	2011.05.24	-
VIPRE	9377	2011.05.24	-
ViRobot	2011.5.24.4476	2011.05.24	-
VirusBuster	13.6.370.1	2011.05.24	-

Additional information[Show all](#)**MD5** : 6dfd3bb7e6ee2e1052272b0131439f6a**SHA1** : 1512e4e79b6411c8d0f74a069cdee6b39179ee25**SHA256**: 142ba410d8877328ed1ea4dbd39c9bd19a0b38e88f7b2363af6b9e258a1b1652**ssdeep**: 49152:aHSiUmgvqHv/lSDAAbuAXWtc5zsrTanTmQSnqgmRBPgrNa/s:2SiUmgvkvdsD/b4Y5KTs aQSnFm4rNZ**File size** : 2444777 bytes**First seen**: 2011-05-24 21:01:52**Last seen** : 2011-05-24 21:01:52**TrID:**

UPX compressed Win32 Executable (43.8%)
 Win32 EXE Yoda's Crypter (38.1%)
 Win32 Executable Generic (12.2%)
 Generic Win/DOS Executable (2.8%)
 DOS Executable Generic (2.8%)

sigcheck:

publisher....: n/a
 copyright....: Emiel Wieldraaijer
 product.....: n/a
 description..: JkDefragGUI version 1.17
 original name: n/a
 internal name: n/a
 file version.: 0.1.1.7
 comments.....: Thnx to everyone who helped
 signers.....: -

signing date.: -
verified.....: Unsigned
PEiD: UPX 2.93 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

packers (F-Prot): UPX_LZMA

PEInfo: PE structure information

[[basic data]]

entrypointaddress: 0x139440
timedatestamp....: 0x4BC81615 (Fri Apr 16 07:47:33 2010)
machinetype.....: 0x14c (I386)

[[3 section(s)]]

name, viradd, virsiz, rawdsiz, ntropy, md5
UPX0, 0x1000, 0xF7000, 0x0, 0.00, d41d8cd98f00b204e9800998ecf8427e
UPX1, 0xF8000, 0x42000, 0x42000, 8.00, d279731f6c11b7243937126796a7a2cf
.rsrc, 0x13A000, 0x7B000, 0x7AA00, 5.01, 2b483f1b68251f90be7e48c08ec5ed81

[[16 import(s)]]

KERNEL32.DLL: LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess

ADVAPI32.dll: GetAce

COMCTL32.dll: ImageList_Remove

COMDLG32.dll: GetSaveFileNameW

GDI32.dll: LineTo

MPR.dll: WNetGetConnectionW

ole32.dll: CoInitialize

OLEAUT32.dll: -

PSAPI.DLL: EnumProcesses

SHELL32.dll: DragFinish

USER32.dll: GetDC

USERENV.dll: LoadUserProfileW

VERSION.dll: VerQueryValueW

WININET.dll: FtpOpenFileW

WINMM.dll: timeGetTime

WSOCK32.dll: -

ExifTool:

file metadata
CharacterSet: Unicode
CodeSize: 270336
Comments: Thnx to everyone who helped
Company: Wieldraaijer
EntryPoint: 0x139440
FileDescription: JkDefragGUI version 1.17
FileFlagsMask: 0x0000
FileOS: Win32
FileSize: 2.3 MB
FileSubtype: 0
FileType: Win32 EXE
FileVersion: 0.1.1.7
FileVersionNumber: 0.1.1.7
ImageVersion: 0.0
InitializedDataSize: 503808
LanguageCode: English (British)
LegalCopyright: Emiel Wieldraaijer
LinkerVersion: 9.0
MIMEType: application/octet-stream
MachineType: Intel 386 or later, and compatibles
OSVersion: 5.0

ObjectFileType: Unknown
PEType: PE32
ProductVersionNumber: 3.3.6.1
Subsystem: Windows GUI
SubsystemVersion: 5.0
TimeStamp: 2010:04:16 09:47:33+02:00
UninitializedDataSize: 1011712
Website: <http://www.wieldraaijer.nl>

Symantec reputation: [Suspicious.Insight](#)

VT Community

This file has never been reviewed by any VT Community member. Be the first one to comment on it!

VirusTotal Team

Add your comment... **Remember that when you write comments as an anonymous user they receive the lowest possible reputation. So if you have not signed in yet don't forget to do so. How to markup your comments?**

Goodware

Malware

Spam attachment/link

P2P download

Propagating via IM

Network worm

Drive-by-download

Preview comment

Post comment

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*.