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.

File MyDefragGUI-2.1_setup.exe received on 2009.08.25 11:58:59 (UTC)
Current status: finished
Result: 1/41 (2.44%)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.24	2009.08.25	-
AhnLab-V3	5.0.0.2	2009.08.24	-
AntiVir	7.9.1.3	2009.08.25	-
Antiy-AVL	2.0.3.7	2009.08.24	-
Authentium	5.1.2.4	2009.08.25	-
Avast	4.8.1335.0	2009.08.24	-
AVG	8.5.0.406	2009.08.25	-
BitDefender	7.2	2009.08.25	-
CAT-QuickHeal	10.00	2009.08.25	-
ClamAV	0.94.1	2009.08.25	-
Comodo	2090	2009.08.25	-
DrWeb	5.0.0.12182	2009.08.25	-
eSafe	7.0.17.0	2009.08.24	Suspicious File
eTrust-Vet	31.6.6699	2009.08.25	-
F-Prot	4.4.4.56	2009.08.24	-
F-Secure	8.0.14470.0	2009.08.25	-
Fortinet	3.120.0.0	2009.08.25	-
GData	19	2009.08.25	-
Ikarus	T3.1.1.68.0	2009.08.25	-
Jiangmin	11.0.800	2009.08.25	-
K7AntiVirus	7.10.826	2009.08.24	-
Kaspersky	7.0.0.125	2009.08.25	-
McAfee	5719	2009.08.24	-
McAfee+Artemis	5719	2009.08.24	-
McAfee-GW-Edition	6.8.5	2009.08.25	-
Microsoft	1.4903	2009.08.25	-
NOD32	4365	2009.08.25	-
Norman		2009.08.25	-
nProtect	2009.1.8.0	2009.08.25	-
Panda	10.0.0.14	2009.08.25	-
PCTools	4.4.2.0	2009.08.25	-
Prevx	3.0	2009.08.25	-
Rising	21.44.11.00	2009.08.25	-

Sophos	4.44.0	2009.08.25	-
Sunbelt	3.2.1858.2	2009.08.25	-
Symantec	1.4.4.12	2009.08.25	-
TheHacker	6.3.4.3.387	2009.08.25	-
TrendMicro	8.950.0.1094	2009.08.25	-
VBA32	3.12.10.10	2009.08.25	-
ViRobot	2009.8.25.1901	2009.08.25	-
VirusBuster	4.6.5.0	2009.08.24	-

Additional information

File size: 2246905 bytes
MD5 : 85875121710d4e5690cd5c9c05dd4f64
SHA1 : 11e57b7d2de4582233ffc401a087c40ce731afbf
SHA256: d882037966a474b11baeafb474f10083be3a52d914aa944c8445a59c22567001
PEInfo: PE Structure information

(base data)
entrypointaddress.: 0x1D00
timedatestamp.....: 0x4A50FE07 (Sun Jul 5 21:24:55 2009)
machinetype.......: 0x14C (Intel I386)

(5 sections)
name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0xE8C 0x1000 5.91 84cc4b3cb970ac80b502cc026a15384b
.rdata 0x2000 0x488 0x1000 1.74 81997a7222e80dda02ee83d1e147d54b
.data 0x3000 0x560 0x1000 1.01 d4a8a270215b2fec747caabfd58d8f7b
.gentee 0x4000 0x101E2 0x11000 7.86 8a73c095be0878dbce661cf20879b702
.rsrc 0x15000 0x10C84 0x11000 7.07 98d9d36057c4ab1433355a9a895506ee

(3 imports)

> kernel32.dll: CloseHandle, WriteFile, CreateDirectoryA, lstrcpyA, CreateFileA, GetFileAttributesA, lstrlenA, GetTempPathA, lstrcmpA, DeleteFileA, FreeLibrary, ExitProcess, lstrcatA, GetProcAddress, LoadLibraryA, GetModuleHandleA, GetFileSize, GetLastError, CreateMutexA, GetModuleFileNameA, VirtualAlloc, VirtualFree, GetStartupInfoA
> msvcrt.dll: _exit, _XcptFilter, exit, _acmdln, __getmainargs, _initterm, __setusermatherr, _adjust_fdiv, __p__commode, __p__fmode, __set_app_type, _except_handler3, _controlfp
> user32.dll: MessageBoxA, wsprintfA

(0 exports)
TrID : File type identification
Win32 Executable MS Visual C++ (generic) (32.7%)
UPX compressed Win32 Executable (26.5%)
Win32 EXE Yoda's Crypter (23.1%)
Win32 Executable Generic (7.4%)
Win32 Dynamic Link Library (generic) (6.5%)
ssdeep: 49152:m6SpL++wOjA18oNS7ctARgyJXcu0MlsvzCX8:bSpq+wOjobGRPJsu0Mqi8
PEiD : Armadillo v1.71

```
RDS   : NSRL Reference Data Set
-
```

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*.