

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 **smona127378658475017500821** received on **2010.05.13 21:39:32 (UTC)**

Current status: **finished**

Result: **2/41 (4.88%)**

[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	Suspicious:W32/Malware! Gemini
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	Trojan/Refroso.ijp
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: 2405187 bytes

MD5 : 0ed5e385262e487605a82f4a0d971b8f

SHA1 : 0149fa21920581b284703a39616e0e1d3de72ed6

SHA256: 699679b6b07f9fcf08f4c61323de07f4c82d000516634a16a20062f9d51070bb

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0x12B530

timedatestamp.....: 0x4B93CF87 (Sun Mar 7 17:08:39 2010)

machinetype.....: 0x14C (Intel I386)

(3 sections)

name viradd virsiz rawdsiz ntrpy md5

UPX0 0x1000 0xEB000 0x0 0.00 d41d8cd98f00b204e9800998ecf8427e

UPX1 0xEC000 0x41000 0x40200 8.00 05ef8dfb89faf01dff3bf40df480d2e

.rsrc 0x12D000 0x77000 0x76C00 5.21 f473691beb40b7bcf942a030cc32c393

(16 imports)

> advapi32.dll: GetAce

> comctl32.dll: ImageList_Remove

> comdlg32.dll: GetSaveFileNameW

> gdi32.dll: LineTo

> kernel32.dll: LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess

> 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: -

( 0 exports )

TrID : File type identification
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%)

Symantec reputation: Suspicious.Insight
http://www.symantec.com/security_response/writeup.jsp?docid=2010-021223-0550-99

ssdeep:
49152:PfX+OsclofUSgk/ckFZhUTc5AsrTanTRQsjrPgrNa/s:P/tkUSg2cEcY5BTsFQSjErNZ

sigcheck: publisher....: n/a
copyright....: Emiel Wieldraaijer
product.....: n/a
description..: JkDefragGUI version 1.15
original name: n/a
internal name: n/a
file version.: 0.1.1.5
comments.....: Thnx to everyone who helped
signers.....: -
signing date.: -
verified.....: Unsigned

PEiD : -

packers (Kaspersky): UPX
packers (F-Prot): UPX_LZMA

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*.

Another File