

[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](#) | [Česky](#) | [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 **packupdate_build107_2045.exe** received on **2010.05.21 16:01:26 (UTC)**

Current status: **finished**

Result: **9/41 (21.95%)**

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.05.10	-
AhnLab-V3	2010.05.21.00	2010.05.20	Trojan/Win32.FakeAV
AntiVir	8.2.1.242	2010.05.21	TR/Crypt.XPACK.Gen
Antiy-AVL	2.0.3.7	2010.05.21	-
Authentium	5.2.0.5	2010.05.21	-
Avast	4.8.1351.0	2010.05.21	-
Avast5	5.0.332.0	2010.05.21	-
AVG	9.0.0.787	2010.05.21	-
BitDefender	7.2	2010.05.21	-
CAT-QuickHeal	10.00	2010.05.21	-
ClamAV	0.96.0.3-git	2010.05.21	-
Comodo	4898	2010.05.21	TrojWare.Win32.FraudTool.CuAV.~GGI
DrWeb	5.0.2.03300	2010.05.21	-
eSafe	7.0.17.0	2010.05.20	-
eTrust-Vet	35.2.7502	2010.05.21	-
F-Prot	4.6.0.103	2010.05.20	-
F-Secure	9.0.15370.0	2010.05.21	-
Fortinet	4.1.133.0	2010.05.21	-
GData	21	2010.05.21	-
Ikarus	T3.1.1.84.0	2010.05.21	Trojan-Downloader.Win32.FakeVimes
Jiangmin	13.0.900	2010.05.20	-
Kaspersky	7.0.0.125	2010.05.21	-

McAfee	5.400.0.1158	2010.05.21	-
McAfee-GW-Edition	2010.1	2010.05.21	-
Microsoft	1.5802	2010.05.21	-
NOD32	5136	2010.05.21	-
Norman	6.04.12	2010.05.21	W32/FakeAV.AM!genr
nProtect	2010-05-21.01	2010.05.21	-
Panda	10.0.2.7	2010.05.21	-
PCTools	7.0.3.5	2010.05.21	-
Prevx	3.0	2010.05.21	-
Rising	22.48.04.04	2010.05.21	-
Sophos	4.53.0	2010.05.21	Mal/FakeAV-BW
Sunbelt	6334	2010.05.21	Trojan.Win32.Generic.pak!cobra
Symantec	20101.1.0.89	2010.05.21	-
TheHacker	6.5.2.0.284	2010.05.20	-
TrendMicro	9.120.0.1004	2010.05.21	TROJ_FRAUD.SMDV
TrendMicro-HouseCall	9.120.0.1004	2010.05.21	TROJ_FRAUD.SMDV
VBA32	3.12.12.5	2010.05.21	-
ViRobot	2010.5.20.2326	2010.05.21	-
VirusBuster	5.0.27.0	2010.05.21	-

Additional information

File size: 366080 bytes

MD5 : b766610e556c2d632557e89b703a66a8

SHA1 : b54ace3077ff38af34e4e38378b3712afe132c3c

SHA256: cec4add7357936c46f0751829dc85956f582490f8736e507ea78460d75b6acf5

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0xCF9E10

timedatestamp.....: 0x4892AF59 (Fri Aug 1 08:38:17 2008)

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

(3 sections)

name viradd virsiz rawdsiz ntrpy md5

UPX0 0x1000 0xCA6000 0x0 0.00 d41d8cd98f00b204e9800998ecf8427e

UPX1 0xCA7000 0x53000 0x53000 7.85 e8198787125e9472de1a70f4fee49a56

.rsrc 0xCFA000 0x5000 0x5000 3.67 0548f11f8adf9682505930dc0e6af815

(8 imports)

> advapi32.dll: GetAce

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

> ole32.dll: CreateBindCtx

```
> oleaut32.dll: VariantCopy
> rpcrt4.dll: NdrOleFree
> shell32.dll: SHGetMalloc
> user32.dll: SetMenu
> version.dll: VerFindFileW

( 0 exports )

TrID : File type identification
UPX compressed Win32 Executable (39.5%)
Win32 EXE Yoda's Crypter (34.3%)
Win32 Executable Generic (11.0%)
Win32 Dynamic Link Library (generic) (9.8%)
Generic Win/DOS Executable (2.5%)

ThreatExpert: http://www.threatexpert.com/report.aspx?md5=b766610e556c2d632557e89b703a66a8

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

ssdeep:
6144:1UUjEHIXBnpKXdKxvzG1823cIh2pnU0sj0iX9prIlZDyuv3QhMJnt1YgwQG:KhIXBpKXIpc18ghanXsj0iX9pslZr/

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

Prevx Info: http://info.prevx.com/aboutprogramtext.asp?PX5=EC463F8B00E2AB3E968B051230072600ED78AB87

PEiD : -

packers (Kaspersky): PE_Patch.UPX, UPX

packers (F-Prot): UPX

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