



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 **IMG00020090208-JPG.EXE** received on **02.11.2009 22:50:16 (CET)**

Current status: **finished**

Result: **25/39 (64.10%)**

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.0.0.93	2009.02.11	Backdoor.Rbot!IK
AhnLab-V3	2009.2.12.0	2009.02.11	-
AntiVir	7.9.0.76	2009.02.11	DR/Agent2.dfj
Authentium	5.1.0.4	2009.02.11	-
Avast	4.8.1335.0	2009.02.11	Win32:Trojan-gen {Other}
AVG	8.0.0.229	2009.02.11	Worm/Generic_r.DU.dropper
BitDefender	7.2	2009.02.11	MemScan:Backdoor.RBot.YBJ
CAT-QuickHeal	10.00	2009.02.11	TrojanDropper.Agent.yyg
ClamAV	0.94.1	2009.02.11	Trojan.Dropper-18604
Comodo	973	2009.02.11	-
DrWeb	4.44.0.09170	2009.02.11	BackDoor.IRC.Sdbot.3762
eSafe	7.0.17.0	2009.02.11	Win32.VirToolCeeInje
eTrust-Vet	31.6.6350	2009.02.11	-
F-Prot	4.4.4.56	2009.02.11	-
F-Secure	8.0.14470.0	2009.02.11	-
Fortinet	3.117.0.0	2009.02.11	W32/Agent2.DFJ!tr
GData	19	2009.02.11	MemScan:Backdoor.RBot.YBJ
Ikarus	T3.1.1.45.0	2009.02.11	Backdoor.Rbot
K7AntiVirus	7.10.582	2009.01.09	-
Kaspersky	7.0.0.125	2009.02.11	Trojan.Win32.Agent2.dfj
McAfee	5523	2009.02.11	-
McAfee+Artemis	5523	2009.02.11	Generic.dx
Microsoft	1.4306	2009.02.11	VirTool:Win32/CeeInject.gen!J
NOD32	3845	2009.02.11	Win32/IRCBot.AGP
Norman	6.00.02	2009.02.11	Ircbot.AMAM.dropper
nProtect	2009.1.8.0	2009.02.11	MemScan:Backdoor.RBot.YBJ
Panda	9.4.3.20	2009.02.11	Trj/Zlob.KH
PCTools	4.4.2.0	2009.02.11	-
Prevx1	V2	2009.02.11	Malicious Software

Rising	21.16.22.00	2009.02.11	-
SecureWeb-Gateway	6.7.6	2009.02.11	Trojan.Dropper.Agent2.dfj
Sophos	4.38.0	2009.02.11	Mal/Behav-243
Sunbelt	3.2.1851.2	2009.02.11	-
Symantec	10	2009.02.11	Backdoor.IRC.Bot
TheHacker	6.3.1.85.252	2009.02.11	-
TrendMicro	8.700.0.1004	2009.02.11	-
VBA32	3.12.8.12	2009.02.11	Trojan.Win32.Agent2.dfj
ViRobot	2009.2.11.1600	2009.02.11	-
VirusBuster	4.5.11.0	2009.02.11	Trojan.DR.Agent.Gen.15

Additional information

File size: 102913 bytes

MD5...: 891accd8bec7b745a893e140857b642b

SHA1...: e3607a8c2e4609dcd7659f4dcd1d8c31147739bd

SHA256:

8e8b1aa6b7bc0448639f6dc37226ca7ef256b9dc69198fbb3c734f598f01b6b7

SHA512:

828b5347973eb5c06cb5266ffd198ef9e900ace3657d2c4e9ff9c96a8a072530
5b47feaf900cd8f5e18c75e6f097f5f3926b370b4629c65ea00089cf08b91e68

ssdeep:

3072:+nj9jtfU+INndIc0JcD5f16TJ/RvvwpWBca7F0j:+jbei8X0J/Rvvwhd

PEiD...: -

TrID...: File type identification

Win64 Executable Generic (59.6%)

Win32 Executable MS Visual C++ (generic) (26.2%)

Win32 Executable Generic (5.9%)

Win32 Dynamic Link Library (generic) (5.2%)

Generic Win/DOS Executable (1.3%)

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0x100645c

timedatestamp.....: 0x41107bc1 (Wed Aug 04 06:01:37 2004)

machinetype.....: 0x14c (I386)

(3 sections)

name viradd virsiz rawdsiz ntrpy md5

.text 0x1000 0x992c 0x9a00 6.57 17a6fbe18a834b6f3462304415675d36

.data 0xb000 0x1be4 0x400 4.25 99858e86526942a66950c7139f78a725

.rsrc 0xd000 0xee7c 0xf000 6.83 22162a6bcd7236eea7bd78b1d3beefa

(6 imports)

> ADVAPI32.dll: FreeSid, AllocateAndInitializeSid, EqualSid,
GetTokenInformation, OpenProcessToken, AdjustTokenPrivileges,
LookupPrivilegeValueA, RegCloseKey, RegDeleteValueA, RegOpenKeyExA,
RegSetValueExA, RegQueryValueExA, RegCreateKeyExA, RegQueryInfoKeyA
> KERNEL32.dll: LocalFree, LocalAlloc, GetLastError,
GetCurrentProcess, lstrlenA, GetModuleFileNameA,
GetSystemDirectoryA, _lclose, _llseek, _lopen,
WritePrivateProfileStringA, GetWindowsDirectoryA, CreateDirectoryA,
GetFileAttributesA, ExpandEnvironmentStringsA, lstrcpyA,
GlobalFree, GlobalUnlock, GlobalLock, GlobalAlloc, IsDBCSLeadByte,
GetShortPathNameA, GetPrivateProfileStringA, GetPrivateProfileIntA,
lstrcmpiA, RemoveDirectoryA, FindClose, FindNextFileA, DeleteFileA,
SetFileAttributesA, lstrcmpA, FindFirstFileA, FreeResource,

```
GetProcAddress, LoadResource, SizeofResource, FindResourceA,
lstrcatA, CloseHandle, WriteFile, SetFilePointer, SetFileTime,
LocalFileTimeToFileTime, DosDateTimeToFileTime,
GetCurrentDirectoryA, GetTempFileNameA, ExitProcess, CreateFileA,
LoadLibraryExA, lstrcpynA, GetVolumeInformationA, FormatMessageA,
GetCurrentDirectoryA, GetVersionExA, GetExitCodeProcess,
WaitForSingleObject, CreateProcessA, GetTempPathA, GetSystemInfo,
CreateMutexA, SetEvent, CreateEventA, CreateThread, ResetEvent,
TerminateThread, GetDriveTypeA, GetModuleHandleA, GetStartupInfoA,
GetCommandLineA, QueryPerformanceCounter, GetTickCount,
GetCurrentThreadId, GetCurrentProcessId, GetSystemTimeAsFileTime,
TerminateProcess, UnhandledExceptionFilter,
SetUnhandledExceptionFilter, ReadFile, LoadLibraryA,
GetDiskFreeSpaceA, MulDiv, EnumResourceLanguagesA, FreeLibrary,
LockResource
> GDI32.dll: GetDeviceCaps
> USER32.dll: ExitWindowsEx, wsprintfA, CharNextA, CharUpperA,
CharPrevA, SetWindowLongA, GetWindowLongA, CallWindowProcA,
DispatchMessageA, MsgWaitForMultipleObjects, PeekMessageA,
SendMessageA, SetWindowPos, ReleaseDC, GetDC, GetWindowRect,
SendDlgItemMessageA, GetDlgItem, SetForegroundWindow,
SetWindowTextA, MessageBoxA, DialogBoxIndirectParamA, ShowWindow,
EnableWindow, GetDlgItemTextA, EndDialog, GetDesktopWindow,
MessageBeep, SetDlgItemTextA, LoadStringA, GetSystemMetrics
> COMCTL32.dll: -
> VERSION.dll: GetFileVersionInfoA, VerQueryValueA,
GetFileVersionInfoSizeA
```

(0 exports)

ThreatExpert info: <http://www.threatexpert.com/report.aspx?md5=891accd8bec7b745a893e140857b642b>

Prevx info: <http://info.prevx.com/aboutprogramtext.asp?PX5=F03CF11032BBF26CBE2C00ADBB15DD00D0FAE17F>

packers (F-Prot): CAB

! **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