



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 **r.exe** received on **2010.07.15 02:54:47 (UTC)**

Current status: **finished**

Result: **25/42 (59.53%)**

[Compact](#)

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	5.0.0.31	2010.07.15	Trojan.Win32.Rozena!IK
AhnLab-V3	2010.07.15.00	2010.07.14	-
AntiVir	8.2.4.10	2010.07.14	TR/Crypt.XPACK.Gen2
Antiy-AVL	2.0.3.7	2010.07.14	-
Authentium	5.2.0.5	2010.07.15	W32/Rozena.A.gen!Eldorado
Avast	4.8.1351.0	2010.07.14	Win32:Hijack-GL
Avast5	5.0.332.0	2010.07.15	Win32:Hijack-GL
AVG	9.0.0.836	2010.07.15	Cryptic.A
BitDefender	7.2	2010.07.15	Gen:Trojan.Heur.TP.cqW@b4JHR@ni
CAT-QuickHeal	11.00	2010.07.15	-
ClamAV	0.96.0.3-git	2010.07.15	-
Comodo	5430	2010.07.15	TrojWare.Win32.Rozena.A
DrWeb	5.0.2.03300	2010.07.15	Trojan.Siggen1.61739
eSafe	7.0.17.0	2010.07.14	-
eTrust-Vet	36.1.7708	2010.07.15	Win32/SillyDl.VKG
F-Prot	4.6.1.107	2010.07.15	W32/Rozena.A.gen!Eldorado
F-Secure	9.0.15370.0	2010.07.15	Gen:Trojan.Heur.TP.cqW@b4JHR@ni
Fortinet	4.1.143.0	2010.07.14	-
GData	21	2010.07.15	Gen:Trojan.Heur.TP.cqW@b4JHR@ni
Ikarus	T3.1.1.84.0	2010.07.15	Trojan.Win32.Rozena

Jiangmin	13.0.900	2010.07.14	-
Kaspersky	7.0.0.125	2010.07.14	-
McAfee	5.400.0.1158	2010.07.15	Swrort.a
McAfee-GW-Edition	2010.1	2010.07.14	Heuristic.LooksLike.Trojan.Rozena.I
Microsoft	1.5902	2010.07.15	Trojan:Win32/Swrort.A
NOD32	5279	2010.07.15	a variant of Win32/Rozena.AA
Norman	6.05.11	2010.07.14	-
nProtect	2010-07-14.01	2010.07.14	-
Panda	10.0.2.7	2010.07.14	Suspicious file
PCTools	7.0.3.5	2010.07.15	-
Prevx	3.0	2010.07.15	Medium Risk Malware
Rising	22.56.03.01	2010.07.15	-
Sophos	4.55.0	2010.07.15	Mal/Swrort-A
Sunbelt	6585	2010.07.15	Trojan.Win32.Swrort.A (v)
SUPERAntiSpyware	4.40.0.1006	2010.07.15	Trojan.Agent/Gen-FakeAlert
Symantec	20101.1.1.7	2010.07.15	-
TheHacker	6.5.2.1.315	2010.07.15	-
TrendMicro	9.120.0.1004	2010.07.14	TROJ_SWRORT.SMF
TrendMicro-HouseCall	9.120.0.1004	2010.07.15	TROJ_SWRORT.SMF
VBA32	3.12.12.6	2010.07.14	-
ViRobot	2010.7.12.3932	2010.07.14	-
VirusBuster	5.0.27.0	2010.07.14	-

Additional information

File size: 37888 bytes

MD5...: 2ef637962a6b8742b32be0917b10955a

SHA1...: 6e66fa73f04e9db00d80c531255ff631e9947148

SHA256: 4f245a32fd6888c120abfd6b6c18b183ccc190fabfc7e68236f153a322ddff3b

ssdeep: 768:p+Mh2rKIUIi7VO7AFyqwONPM5+aQ6lRZ95x:8MnIk8T8PMgKh5x

PEiD...: -

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0x1288

timedatestamp.....: 0x4a3644f0 (Mon Jun 15 12:56:16 2009)

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

(4 sections)

name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0x6224 0x6400 6.73 7eb34c5faaaa6bf6831cf6b616290a03
.rdata 0x8000 0x1aa2 0x1c00 5.35 f4e61c2563d5cbfa83c59671c271ad66
.data 0xa000 0x17fc 0xe00 2.29 5ceee242822c8946ed3d6f49d64ec481
.rsrc 0xc000 0x1b4 0x200 5.10 c52ee9fcdbbfff3ba2f8da39a1bd23689

(1 imports)

> KERNEL32.dll: GetCommandLineA, GetStartupInfoA,
SetUnhandledExceptionFilter, GetModuleHandleW, Sleep, GetProcAddress,
ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA,
FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW,
WideCharToMultiByte, GetLastError, GetEnvironmentStringsW, SetHandleCount,
GetFileType, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue,
TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId,
InterlockedDecrement, HeapCreate, VirtualFree, HeapFree,
QueryPerformanceCounter, GetTickCount, GetCurrentProcessId,
GetSystemTimeAsFileTime, LeaveCriticalSection, EnterCriticalSection,
TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter,
IsDebuggerPresent, LoadLibraryA, InitializeCriticalSectionAndSpinCount,
GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapAlloc, VirtualAlloc,
HeapReAlloc, RtlUnwind, HeapSize, GetLocaleInfoA, LCMapStringA,
MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW

(0 exports)

RDS...: NSRL Reference Data Set

-

pdfid.: -

trid...: Win32 Executable MS Visual C++ (generic) (65.2%)
Win32 Executable Generic (14.7%)
Win32 Dynamic Link Library (generic) (13.1%)
Generic Win/DOS Executable (3.4%)
DOS Executable Generic (3.4%)

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

Symantec Reputation Network: Suspicious.Insight

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

<a href='http://info.prevx.com/aboutprogramtext.asp?PX5=0CC390D000BBBA85947500B15DBA0D00E3E60BC9'

target='_blank'>http://info.prevx.com/aboutprogramtext.asp?
PX5=0CC390D000BBBA85947500B15DBA0D00E3E60BC9

! **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