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 **Old_Meterpreter_Frame.exe** received on **2010.07.15 16:48:05 (UTC)**
Current status: **finished**
Result: **27/42 (64.29%)**

Compact | Print results

| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| a-squared | 5.0.0.31 | 2010.07.15 | Trojan.Win32.Rozena!IK |
| AhnLab-V3 | 2010.07.15.01 | 2010.07.15 | - |
| AntiVir | 8.2.4.12 | 2010.07.15 | TR/Crypt.XPACK.Gen2 |
| Antiy-AVL | 2.0.3.7 | 2010.07.15 | - |
| Authentium | 5.2.0.5 | 2010.07.15 | W32/Rozena.A.gen!Eldorado |
| Avast | 4.8.1351.0 | 2010.07.15 | 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@birbs8gi |
| CAT-QuickHeal | 11.00 | 2010.07.15 | Win32.Trojan.Rozena.bvj.4 |
| ClamAV | 0.96.0.3-git | 2010.07.15 | - |
| Comodo | 5438 | 2010.07.15 | TrojWare.Win32.Rozena.A |
| DrWeb | 5.0.2.03300 | 2010.07.15 | Trojan.Siggen1.61135 |
| eSafe | 7.0.17.0 | 2010.07.15 | - |
| eTrust-Vet | 36.1.7710 | 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@birbs8gi |
| Fortinet | 4.1.143.0 | 2010.07.15 | - |
| GData | 21 | 2010.07.15 | Gen:Trojan.Heur.TP.cqW@birbs8gi |
| Ikarus | T3.1.1.84.0 | 2010.07.15 | Trojan.Win32.Rozena |

| | | | |
|---|---|---|---|
| Jiangmin | 13.0.900 | 2010.07.15 | - |
| Kaspersky | 7.0.0.125 | 2010.07.15 | - |
| McAfee | 5.400.0.1158 | 2010.07.15 | Swrort.a |
| McAfee-GW-Edition | 2010.1 | 2010.07.15 | Swrort.a |
| Microsoft | 1.5902 | 2010.07.15 | Trojan:Win32/Swrort.A |
| NOD32 | 5281 | 2010.07.15 | a variant of Win32/Rozena.AA |
| Norman | 6.05.11 | 2010.07.15 | W32/Swrort.A |
| nProtect | 2010-07-15.02 | 2010.07.15 | - |
| Panda | 10.0.2.7 | 2010.07.15 | Generic Trojan |
| PCTools | 7.0.3.5 | 2010.07.15 | - |
| Prevx | 3.0 | 2010.07.15 | Medium Risk Malware |
| Rising | 22.56.03.04 | 2010.07.15 | - |
| Sophos | 4.55.0 | 2010.07.15 | Mal/Swrort-C |
| Sunbelt | 6587 | 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 | 6.5.2.1.316 | 2010.07.15 | - |
| TrendMicro | 9.120.0.1004 | 2010.07.15 | TROJ_SWRORT.SMF |
| TrendMicro-HouseCall | 9.120.0.1004 | 2010.07.15 | TROJ_SWRORT.SMF |
| VBA32 | 3.12.12.6 | 2010.07.15 | - |
| ViRobot | 2010.7.12.3932 | 2010.07.15 | - |
| VirusBuster | 5.0.27.0 | 2010.07.15 | - |

**Additional information**

File size: 37888 bytes

MD5...: a032a0c93de0e5ae021a5b23c253d637

SHA1..: 8619b1b58aa978ae2f5b394ab2e44079e494ce74

SHA256: ff44a9a972f6cad77934e1ad562ccd79efc3d75b518c11d0f6dd758b1a13b26e

ssdeep: 768:QVA0S41k0CCRIAVyhO7A5cqLrNhMmnpx6lRZ95x:Sa0lDkuwRhM8oh5x

PEiD..: -

PEInfo: PE Structure information

( base data )
entrypointaddress.: 0x1ced
timedatestamp.....: 0x4a3ceb66 (Sat Jun 20 14:00:06 2009)
machinetype.......: 0x14c (I386)

```
( 4 sections )
name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0x6224 0x6400 6.73 4b8cd8783a0ed16add3df09019f28430
.rdata 0x8000 0x1aa2 0x1c00 5.35 f4e61c2563d5cbfa83c59671c271ad66
.data 0xa000 0x17fc 0xe00 2.29 5ceee242822c8946ed3d6f49d64ec481
.rsrc 0xc000 0x1b4 0x200 5.10 c52ee9fcdbbff3ba2f8da39a1bd23689

( 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
-

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%)

<a href='http://info.prevx.com/aboutprogramtext.asp?
PX5=B97DF765003F10819484009100BC0800EDF4BF68'
target='_blank'>http://info.prevx.com/aboutprogramtext.asp?
PX5=B97DF765003F10819484009100BC0800EDF4BF68</a>

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

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
```

pdfid.: -

❗ **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