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 **prism.exe** received on **02.03.2009 17:11:26 (CET)**
Current status: **finished**
Result: **1/39 (2.57%)**

Compact

Print results

Antivirus	Version	Last Update	Result
a-squared	4.0.0.93	2009.02.03	-
AhnLab-V3	5.0.0.2	2009.02.03	-
AntiVir	7.9.0.71	2009.02.03	-
Authentium	5.1.0.4	2009.02.03	-
Avast	4.8.1281.0	2009.02.03	-
AVG	8.0.0.229	2009.02.03	-
BitDefender	7.2	2009.02.03	-
CAT-QuickHeal	10.00	2009.02.03	-
ClamAV	0.94.1	2009.02.03	-
Comodo	961	2009.02.03	-
DrWeb	4.44.0.09170	2009.02.03	-
eSafe	7.0.17.0	2009.02.01	-
eTrust-Vet	31.6.6339	2009.02.03	-
F-Prot	4.4.4.56	2009.02.02	-
F-Secure	8.0.14470.0	2009.02.03	-
Fortinet	3.117.0.0	2009.02.03	-
GData	19	2009.02.03	-
Ikarus	T3.1.1.45.0	2009.02.03	-
K7AntiVirus	7.10.617	2009.02.03	-
Kaspersky	7.0.0.125	2009.02.03	-
McAfee	5514	2009.02.02	-
McAfee+Artemis	5514	2009.02.02	-
Microsoft	1.4306	2009.02.03	-
NOD32	3821	2009.02.03	probably a variant of Win32/Genetik

Norman	6.00.02	2009.02.03 -
nProtect	2009.1.8.0	2009.02.03 -
Panda	9.5.1.2	2009.02.02 -
PCTools	4.4.2.0	2009.02.03 -
Prevx1	V2	2009.02.03 -
Rising	21.15.10.00	2009.02.03 -
SecureWeb-Gateway	6.7.6	2009.02.03 -
Sophos	4.38.0	2009.02.03 -
Sunbelt	3.2.1835.2	2009.01.16 -
Symantec	10	2009.02.03 -
TheHacker	6.3.1.5.245	2009.02.03 -
TrendMicro	8.700.0.1004	2009.02.03 -
VBA32	3.12.8.12	2009.02.03 -
ViRobot	2009.2.3.1587	2009.02.03 -
VirusBuster	4.5.11.0	2009.02.03 -

Additional information

```
File size: 10007032 bytes
MD5...: 382a61b3e874c95f3487ea5a8eb345aa
SHA1..: 8bcdbcb0cdf3c7a09e3b6a0f0b7a7ce550d5cc40
SHA256:
11409bb46d1663e189e46f0691126a722876f6ed42344088670fc2bb862a629f
SHA512:
70dc4935d48909d9adfda05f2f0931f29b856f2072418013be33fe6973bef813
b0a7b7a23bc944a181e9f2e1e566d9fd70957038aa55281a62f11ea77659cba4
ssdeep:
196608:dQM5I4s6/1oI9HSSFfFeB5aNVoVu48pgWHablpmN6xqKiiScDcZnqGhdn
qY5Z+9r:dQcvHNle/aNqVJsgWHaZp3xKPoGhdnqn
PEiD..: Armadillo v1.71
TrID..: File type identification
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%)
PEInfo: PE Structure information

( base data )
entrypointaddress.: 0x5eb51a
timedatestamp.....: 0x49490f43 (Wed Dec 17 14:40:03 2008)
machinetype.......: 0x14c (I386)

( 4 sections )
name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0x600106 0x601000 6.29
9f610d29f2ad034ed9dc850aeb4ee493
.rdata 0x602000 0x33dc2 0x34000 5.66
0228898547df5e4de19d3ddf3883524d
```

.data 0x636000 0xbc768 0x48000 5.02
7d4e83e99eeed133c91706ae2169de07
.rsrc 0x6f3000 0x30b9e8 0x30c000 5.21
47443e377510eca964c9f4075b2d746d

(13 imports)
> VIC32.DLL: convert1bitto8bit, savepcx, savetif, convertrgbtopal, dibtoimage, allocimage, savegifex, allocDIB, freeimage, bmpinfo, loadbmp, tiffinfo, loadtif, pcxinfo, loadpcx, loadjpg, gifinfo, loadgif, jpeginfo, getpixelcolor
> COMCTL32.dll: ImageList_DragMove, -, ImageList_DragLeave, ImageList_EndDrag, ImageList_Create, ImageList_Remove, InitCommonControlsEx, -, -, -, _TrackMouseEvent, ImageList_AddMasked, ImageList_Destroy, ImageList_DragEnter, ImageList_BeginDrag
> oledlg.dll: -, -, -, -
> KERNEL32.dll: IsBadReadPtr, WritePrivateProfileStringA, GetPrivateProfileIntA, GetPrivateProfileStringA, IsDBCSLeadByte, GlobalFlags, CreateToolhelp32Snapshot, Process32First, Process32Next, VirtualAlloc, VirtualFree, SetErrorMode, ExpandEnvironmentStringsA, GetShortPathNameA, FindNextFileA, SizeofResource, GetSystemDefaultLangID, GetNumberFormatA, LoadResource, LockResource, FreeResource, SuspendThread, GetExitCodeProcess, GetProfileIntA, SetHandleCount, GetWindowsDirectoryA, SearchPathA, GetLocaleInfoA, GetSystemTime, RemoveDirectoryA, CopyFileA, SetEndOfFile, OpenMutexA, SetFileAttributesA, TryEnterCriticalSection, FindFirstChangeNotificationA, FindNextChangeNotification, FindCloseChangeNotification, FlushFileBuffers, OpenFile, GetVersionExA, FindFirstFileA, GetDriveTypeA, FindResourceA, LoadLibraryExA, GetUserDefaultLangID, GetProfileStringA, CreateThread, Sleep, DeleteCriticalSection, InitializeCriticalSection, lstrcpyW, GetModuleHandleA, GlobalSize, GetProcAddress, GlobalUnlock, GlobalReAlloc, GetAtomNameA, AddAtomA, DeleteAtom, LoadLibraryA, FreeLibrary, SetCurrentDirectoryA, GetDateFormatA, GetTimeFormatA, GetFullPathNameA, GetCurrentDirectoryA, LocalAlloc, GlobalAlloc, GlobalFree, GlobalHandle, GetACP, ReleaseMutex, SetThreadPriority, TerminateThread, CreateMutexA, SetLastError, GlobalAddAtomA, WaitForSingleObject, EnterCriticalSection, LeaveCriticalSection, ResumeThread, GlobalGetAtomNameA, DeleteFileA, GlobalDeleteAtom, InterlockedIncrement, CompareStringA, SetFilePointer, GlobalMemoryStatus, GetSystemDirectoryA, GetDiskFreeSpaceExA, CreateDirectoryA, GetFileAttributesExA, ReadFile, CreateFileMappingA, GetFileSize, MapViewOfFile, UnmapViewOfFile, WriteFile, GetCurrentThreadId, FindClose, GetFileAttributesA, MulDiv, lstrcmpA, lstrcpynA, lstrcmpiA, GetTickCount, lstrcpyA, lstrcatA, lstrlenA, WideCharToMultiByte, MultiByteToWideChar, GetTimeZoneInformation, SystemTimeToFileTime, GetLocalTime, FileTimeToSystemTime, GetModuleFileNameA, GlobalLock, CreateFileA, CloseHandle, FormatMessageA, LocalFree, InterlockedDecrement, GetTempPathA, GetTempFileNameA, GetLastError, TerminateProcess, GetCurrentProcess, HeapSize, GetStringTypeA, GetStringTypeW, UnhandledExceptionFilter, GetStdHandle, GetFileType, FreeEnvironmentStringsA, IsBadWritePtr, HeapCreate, HeapDestroy, GetEnvironmentVariableA, SetUnhandledExceptionFilter, TlsGetValue, TlsAlloc, CompareStringW, LCMapStringW, LCMapStringA, FreeEnvironmentStringsW, GetEnvironmentStrings, GetEnvironmentStringsW, GetCurrentProcessId, IsValidLocale, IsValidCodePage, EnumSystemLocalesA, GetUserDefaultLCID, IsBadCodePtr, SetStdHandle, CreateProcessA, CreateFileW,

GetLocaleInfoW, RtlUnwind, RaiseException, SetEnvironmentVariableA,
ExitProcess, GetVersion, GetCommandLineA, GetStartupInfoA,
GetOEMCP, GetCPInfo, SetConsoleCtrlHandler, HeapReAlloc, MoveFileA,
FileTimeToLocalFileTime, ExitThread, TlsSetValue, HeapAlloc,
HeapFree, InterlockedExchange
> GDI32.dll: GetCharWidthA, SetWinMetaFileBits,
SetTextJustification, Arc, GetPixel, GetNearestColor, ExtCreatePen,
CreateDCA, CreateICA, Escape, PlayMetaFileRecord,
SetTextCharacterExtra, OffsetClipRgn, GetGraphicsMode,
SetGraphicsMode, PolyPolygon, Chord, Polyline, SetPixel, FloodFill,
ExtFloodFill, CopyMetaFileA, EnumMetaFile, CreatePalette,
SetDIBits, GetRegionData, ExtCreateRegion, GetWindowOrgEx,
StretchDIBits, SetPolyFillMode, CreateEllipticRgn,
ScaleWindowExtEx, GetROP2, SetROP2, PtInRegion, GetMapMode,
ResetDCA, SetAbortProc, StartDocA, EndDoc, GetEnhMetaFileA,
EnumFontFamiliesExA, GetCharWidth32A, Ellipse, Polygon, BeginPath,
EndPath, SelectClipPath, Pie, CreatePenIndirect, GetWindowExtEx,
GetTextAlign, SelectPalette, RealizePalette, GetViewportOrgEx,
UnrealizeObject, SetBrushOrgEx, StartPage, EndPage,
CreateDIBSection, CreateEnhMetaFileA, SetWindowExtEx,
SetViewportExtEx, StretchBlt, CreatePatternBrush,
CreateFontIndirectW, SetWindowOrgEx, ExtSelectClipRgn, GetDIBits,
SetDIBitsToDevice, PlayEnhMetaFile, CreatePolygonRgn,
CloseEnhMetaFile, OffsetWindowOrgEx, SetStretchBltMode,
CreateBitmap, LPtoDP, IntersectClipRect, GetRgnBox, SelectClipRgn,
OffsetViewportOrgEx, SetViewportOrgEx, CreateRoundRectRgn, FillRgn,
FrameRgn, GetTextColor, CreateRectRgn, CreateRectRgnIndirect,
CombineRgn, GetWinMetaFileBits, SetMetaFileBitsEx,
GetEnhMetaFileHeader, CreateMetaFileA, CloseMetaFile,
GetMetaFileBitsEx, DeleteMetaFile, CreateHatchBrush, GetTextFaceA,
GetBkColor, CreateFontA, CreateBrushIndirect, Rectangle,
SetMapMode, SetTextAlign, TextOutA, PatBlt, BitBlt, DPtoLP,
CreateSolidBrush, SetPixelV, SaveDC, GetStockObject, RoundRect,
RestoreDC, GetCurrentObject, GetTextMetricsA, CreatePen, MoveToEx,
LineTo, CreateCompatibleDC, CreateCompatibleBitmap, DeleteDC,
SetEnhMetaFileBits, GetEnhMetaFileBits, DeleteEnhMetaFile,
GetTextExtentPointA, GetDeviceCaps, CopyEnhMetaFileA,
ExcludeClipRect, SetBkColor, SetBkMode, GetObjectA,
CreateFontIndirectA, SelectObject, SetTextColor, DeleteObject,
ExtTextOutA, GetTextExtentPoint32A
> WINSPOOL.DRV: GetPrinterA, DocumentPropertiesA, ClosePrinter,
OpenPrinterA
> comdlg32.dll: GetOpenFileNameA, GetSaveFileNameA, ChooseFontA,
CommDlgExtendedError, ChooseColorA, PrintDlgA
> ADVAPI32.dll: RegOpenKeyExA, RegQueryMultipleValuesA,
RegEnumKeyExA, AllocateAndInitializeSid, FreeSid, RegSetValueExA,
RegCreateKeyExA, GetUserNameA, RegQueryValueExA, RegQueryValueA,
RegCreateKeyA, RegDeleteKeyA, RegOpenKeyA, RegSetValueA,
RegCloseKey
> ole32.dll: OleRun, OleLoad, CreateBindCtx, SetConvertStg,
GetHGlobalFromILockBytes, StgOpenStorageOnILockBytes,
OleQueryCreateFromData, RegisterDragDrop, CoLockObjectExternal,
OleRegEnumFormatEtc, OleSetClipboard, CreateFileMoniker,
CreateItemMoniker, CoRevokeClassObject, WriteClassStg,
WriteFmtUserTypeStg, GetRunningObjectTable, CoDisconnectObject,
CreateStreamOnHGlobal, OleSaveToStream, WriteClassStm,
CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes,
StringFromCLSID, CoTaskMemFree, CLSIDFromString, CoInitialize,
CoUninitialize, CoCreateInstance, OleBuildVersion, OleInitialize,
CoRegisterClassObject, OleUninitialize, ReadClassStg,
CreateGenericComposite, GetConvertStg, ReleaseStgMedium,

CreateDataAdviseHolder, CreateOleAdviseHolder, CLSIDFromProgID, CoGetMalloc, MkParseDisplayName, CoTaskMemAlloc, ReadFmtUserTypeStg, OleDuplicateData, CoFreeUnusedLibraries, ProgIDFromCLSID, OleFlushClipboard, OleRegEnumVerbs, OleGetIconOfClass, OleRegGetUserType, OleQueryLinkFromData, OleGetClipboard, OleCreateLinkToFile, OleCreateFromFile, OleCreateFromData, OleCreateLinkFromData, OleDraw, OleCreate, OleSave, OleSetContainedObject, RevokeDragDrop
> OLEAUT32.dll: -, -, -, -, -, -, -, -, -, -, -, -, -, -, -, -, -, -, -
> WININET.dll: InternetConnectA, InternetGetLastResponseInfoA, InternetOpenUrlA, FtpRemoveDirectoryA, InternetSetStatusCallback, InternetQueryOptionA, InternetReadFile, InternetQueryDataAvailable, HttpQueryInfoA, InternetCloseHandle, HttpSendRequestA, HttpOpenRequestA, InternetSetOptionA, InternetOpenA, FtpOpenFileA, FtpPutFileA, FtpDeleteFileA, FtpSetCurrentDirectoryA, InternetFindNextFileA, FtpFindFirstFileA, FtpCreateDirectoryA
> VERSION.dll: GetFileVersionInfoA, GetFileVersionInfoSizeA, VerQueryValueA
> SHLWAPI.dll: PathAddExtensionA, SHDeleteKeyA, PathFileExistsA, PathAppendA, PathFindExtensionA, PathRemoveExtensionA, PathFindFileNameA, PathRemoveBackslashA, PathRemoveFileSpecA, PathAddBackslashA

(0 exports)

Another File