

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 **nt.dll** received on **2009.10.09 07:48:38 (UTC)**

Current status: **finished**

Result: **2/41 (4.88%)**

Compact

[Print results](#)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.41	2009.10.09	-
AhnLab-V3	5.0.0.2	2009.10.09	-
AntiVir	7.9.1.35	2009.10.08	TR/ATRAPS.Gen2
Antiy-AVL	2.0.3.7	2009.10.09	-
Authentium	5.1.2.4	2009.10.09	-
Avast	4.8.1351.0	2009.10.08	-
AVG	8.5.0.420	2009.10.04	-
BitDefender	7.2	2009.10.09	-
CAT-QuickHeal	10.00	2009.10.09	-
ClamAV	0.94.1	2009.10.09	-
Comodo	2543	2009.10.09	-
DrWeb	5.0.0.12182	2009.10.09	-
eSafe	7.0.17.0	2009.10.08	-
eTrust-Vet	35.1.7059	2009.10.09	-
F-Prot	4.5.1.85	2009.10.08	-
F-Secure	8.0.14470.0	2009.10.09	-
Fortinet	3.120.0.0	2009.10.09	-
GData	19	2009.10.09	-
Ikarus	T3.1.1.72.0	2009.10.09	-
Jiangmin	11.0.800	2009.10.08	-
K7AntiVirus	7.10.865	2009.10.08	-
Kaspersky	7.0.0.125	2009.10.09	-
McAfee	5765	2009.10.08	-
McAfee+Artemis	5765	2009.10.08	-
McAfee-GW-Edition	6.8.5	2009.10.09	Trojan.ATRAPS.Gen2
Microsoft	1.5101	2009.10.08	-

NOD32	4492	2009.10.09	-
Norman	6.01.09	2009.10.08	-
nProtect	2009.1.8.0	2009.10.08	-
Panda	10.0.2.2	2009.10.08	-
PCTools	4.4.2.0	2009.10.08	-
Prevx	3.0	2009.10.09	-
Rising	21.50.41.00	2009.10.09	-
Sophos	4.45.0	2009.10.09	-
Sunbelt	3.2.1858.2	2009.10.09	-
Symantec	1.4.4.12	2009.10.09	-
TheHacker	6.5.0.2.033	2009.10.07	-
TrendMicro	8.950.0.1094	2009.10.09	-
VBA32	3.12.10.11	2009.10.08	-
ViRobot	2009.10.9.1977	2009.10.09	-
VirusBuster	4.6.5.0	2009.10.08	-

Additional information

File size: 45056 bytes

MD5...: ef78875988ef76ec5138645b8fb9327d

SHA1...: 03a74966edc7df057ac50a92204995fd433d164d

SHA256: 435817cf5856882c039c089fa35d737ecd673e479904e916bd66bb9dd1b28af0

ssdeep: 768:nqMpKGhuzOvUm4Ta7MtuEmf5TuiENgvyptAeQU52MA5qF:nb8w4TMMtuEmlag
htDt

PEiD...: -

PEInfo: PE Structure information

(base data)

entrypointaddress.: 0x3850

timedatestamp.....: 0x4aab1328 (Sat Sep 12 03:19:04 2009)

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

(4 sections)

name viradd virsiz rawdsiz ntrpy md5

.text 0x1000 0x6886 0x7000 6.23 bba243dbf5fcbce7b6aadee2a188a218

.rdata 0x8000 0xf28 0x1000 5.21 e18365591667423b0895f4c2c6dfd426

.data 0x9000 0x2b40 0x1000 2.75 4e231672eaa52e61706e117004537707

.reloc 0xc000 0xd6a 0x1000 3.60 f621904d760f3cd11f3f9e29931fd1fd

(3 imports)

> ADVAPI32.dll: RegCloseKey, RegQueryValueExA, RegOpenKeyExA,
RegDeleteValueA, RegDeleteKeyA, RegSetValueExA, InitiateSystemShutdownA,
AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken,
CloseServiceHandle, StartServiceA, QueryServiceStatus, OpenServiceA,
OpenSCManagerA, ControlService

> USER32.dll: MessageBoxExA

> KERNEL32.dll: GetLastError, GetCurrentProcess, CloseHandle,
Process32Next, Process32First, CreateToolhelp32Snapshot,
GetFileAttributesA, BackupWrite, MultiByteToWideChar, GetFullPathNameA,
CreateFileA, SetFileAttributesA, RemoveDirectoryA, DeviceIoControl,
CreateDirectoryA, GetCommandLineA, GetVersion, ExitProcess,
TerminateProcess, GetCurrentThreadId, TlsSetValue, TlsAlloc, TlsFree,

```
SetLastError, TlsGetValue, SetHandleCount, GetStdHandle, GetFileType,  
GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA,  
FreeEnvironmentStringsA, FreeEnvironmentStringsW, WideCharToMultiByte,  
GetEnvironmentStrings, GetEnvironmentStringsW, HeapDestroy, HeapCreate,  
VirtualFree, HeapFree, WriteFile, SetFilePointer, EnterCriticalSection,  
LeaveCriticalSection, InterlockedDecrement, InterlockedIncrement,  
InitializeCriticalSection, HeapAlloc, GetCPInfo, GetACP, GetOEMCP,  
VirtualAlloc, HeapReAlloc, GetProcAddress, LoadLibraryA, SetStdHandle,  
LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW,  
FlushFileBuffers, RtlUnwind
```

(14 exports)

```
bootmodu, finimodu, msgbox, nt_continueservice, nt_hardlink,  
nt_pauseservice, nt_startservice, nt_stopservice, procllist, regdel,  
regread, regwrite, shutdown_nt, versmodu
```

RDS...: NSRL Reference Data Set

-

pdfid.: -

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

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%)

! **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