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 **Super_app.exe** received on **2009.09.29 23:44:42 (UTC)**
Current status: **finished**
Result: **32/40 (80.00%)**

Compact | Print results

| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 5.0.0.2 | 2009.09.29 | Win-Trojan/Peflog.7168 |
| AntiVir | 7.9.1.27 | 2009.09.29 | SPR/Perflogger.163.C |
| Antiy-AVL | 2.0.3.7 | 2009.09.29 | Monitor/Win32.Perflogger |
| Authentium | 5.1.2.4 | 2009.09.29 | - |
| Avast | 4.8.1351.0 | 2009.09.29 | Win32:Perflogger-AJ |
| AVG | 8.5.0.412 | 2009.09.29 | Perflogger.S |
| BitDefender | 7.2 | 2009.09.30 | Trojan.Perflog.EO |
| CAT-QuickHeal | 10.00 | 2009.09.29 | Win32.Monitor.Perflogger.163 |
| ClamAV | 0.94.1 | 2009.09.29 | Trojan.Perflog |
| Comodo | 2469 | 2009.09.29 | UnclassifiedMalware |
| DrWeb | 5.0.0.12182 | 2009.09.30 | Trojan.Peflog.31 |
| eSafe | 7.0.17.0 | 2009.09.29 | Spyware.Gen |
| eTrust-Vet | 31.6.6768 | 2009.09.29 | - |
| F-Prot | 4.5.1.85 | 2009.09.29 | W32/MonitorX.CJ |
| F-Secure | 8.0.14470.0 | 2009.09.30 | Monitor.Win32.Perflogger.163 |
| Fortinet | 3.120.0.0 | 2009.09.29 | Keylog/Perfect |
| GData | 19 | 2009.09.30 | Trojan.Perflog.EO |
| Ikarus | T3.1.1.72.0 | 2009.09.29 | not-a-virus:Monitor.Win32.Perflogger |
| Jiangmin | 11.0.800 | 2009.09.27 | Trojan/Agent.iut |
| K7AntiVirus | 7.10.856 | 2009.09.29 | not-a-virus:Monitor.Win32.Perflogger |
| Kaspersky | 7.0.0.125 | 2009.09.30 | not-a-virus:Monitor.Win32.Perflogger.163 |
| McAfee | 5756 | 2009.09.29 | potentially unwanted program Keylog-Perfect |
| McAfee+Artemis | 5756 | 2009.09.29 | Suspect-29!ADABABDB29C8 |
| McAfee-GW-Edition | 6.8.5 | 2009.09.29 | Heuristic.BehavesLike.Win32.Dropper.I |
| Microsoft | 1.5005 | 2009.09.23 | MonitoringTool:Win32/PerfectKeylogger |
| NOD32 | 4468 | 2009.09.29 | Win32/Spy.PerfKey |
| Norman | 6.01.09 | 2009.09.29 | - |
| nProtect | 2009.1.8.0 | 2009.09.29 | - |
| Panda | 10.0.2.2 | 2009.09.29 | W32/Xor-encoded.A |
| PCTools | 4.4.2.0 | 2009.09.29 | Trojan.DL.ILoveHonk.A |
| Prevx | 3.0 | 2009.09.30 | - |
| Rising | 21.49.14.00 | 2009.09.29 | Trojan.Perflog.fc |
| Sophos | 4.45.0 | 2009.09.29 | Perfect Keylogger |
| Sunbelt | 3.2.1858.2 | 2009.09.30 | Perfect Keylogger |

| | | | |
|---|---|---|---|
| Symantec | 1.4.4.12 | 2009.09.30 | Spyware.Perfect |
| TheHacker | 6.5.0.2.022 | 2009.09.30 | - |
| TrendMicro | 8.500.0.1002 | 2009.09.29 | - |
| VBA32 | 3.12.10.11 | 2009.09.29 | Trojan.Win32.Lca |
| ViRobot | 2009.9.29.1963 | 2009.09.29 | - |
| VirusBuster | 4.6.5.0 | 2009.09.29 | Trojan.DL.ILoveHonk.A |

**Additional information**

File size: 348311 bytes

MD5 : adababdb29c8e037e5e2ae95f9856132

SHA1 : 7827b01076656ae32f28a17cfbd30c56971fd488

SHA256: 78ce997bf1d74ad8bd644de01b9e7f028c94e05ba0dcc7356d789e60ab6e8b16

PEInfo: PE Structure information

```
( base data )
entrypointaddress.: 0x1000
timedatestamp.....: 0x3CE1015C (Tue May 14 14:21:48 2002)
machinetype.......: 0x14C (Intel I386)

( 4 sections )
name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0x11000 0x10200 6.43 cd2320e9f81690d9d5dae76de1da8879
.data 0x12000 0x6000 0x800 4.36 dcc7b4f93348ec2d9e5f22d4eded0be9
.idata 0x18000 0x1000 0xE00 4.38 667eeb8f5b5db58fe5dae93c7c1d16c1
.rsrc 0x19000 0x3000 0x2C00 3.04 6b45964b7a00da7f21e391b94a2ddd01

( 7 imports )

> advapi32.dll: AdjustTokenPrivileges, LookupPrivilegeValueA,
OpenProcessToken, RegCloseKey, RegOpenKeyExA, RegQueryValueExA,
SetFileSecurityA, SetFileSecurityW
> comctl32.dll: -
> gdi32.dll: DeleteObject
> kernel32.dll: CloseHandle, CompareStringA, CreateDirectoryA,
CreateDirectoryW, CreateFileA, CreateFileW, DeleteFileA, DeleteFileW,
DosDateTimeToFileTime, ExitProcess, ExpandEnvironmentStringsA,
FileTimeToDosDateTime, FileTimeToLocalFileTime, FileTimeToSystemTime,
FindClose, FindFirstFileA, FindFirstFileW, FindNextFileA, FindNextFileW,
FindResourceA, FormatMessageA, FreeLibrary, GetCommandLineA,
GetCurrentDirectoryA, GetCurrentProcess, GetDateFormatA,
GetFileAttributesA, GetFileAttributesW, GetFileType, GetFullPathNameA,
GetLastError, GetLocaleInfoA, GetModuleFileNameA, GetModuleHandleA,
GetNumberFormatA, GetProcAddress, GetProcessHeap, GetStdHandle,
GetTempPathA, GetTickCount, GetTimeFormatA, GetVersionExA, HeapAlloc,
HeapFree, HeapReAlloc, LoadLibraryA, LocalFileTimeToFileTime, LocalFree,
MoveFileA, MoveFileExA, MultiByteToWideChar, ReadFile,
SetCurrentDirectoryA, SetEndOfFile, SetFileAttributesA, SetFileAttributesW,
SetFilePointer, SetFileTime, SetLastError, Sleep, WaitForSingleObject,
WideCharToMultiByte, WriteFile, lstrcmpiA
> ole32.dll: CoCreateInstance, OleInitialize, OleUninitialize
> shell32.dll: SHBrowseForFolderA, SHFileOperationA, SHGetFileInfoA,
SHGetMalloc, SHGetSpecialFolderLocation, ShellExecuteExA,
SHGetPathFromIDListA
> user32.dll: CharToOemBuffA, CharUpperA, CreateWindowExA, DestroyIcon,
DestroyWindow, DialogBoxParamA, DispatchMessageA, EnableWindow, EndDialog,
FindWindowExA, GetClassNameA, GetClientRect, GetDlgItem, GetDlgItemTextA,
GetMessageA, GetSysColor, GetSystemMetrics, GetWindow, GetWindowLongA,
GetWindowRect, GetWindowTextA, GetWindowTextLengthA, LoadIconA,
LoadStringA, MapWindowPoints, MessageBoxA, OemToCharA, OemToCharBuffA,
PeekMessageA, PostMessageA, SendDlgItemMessageA, SendMessageA,
SetDlgItemTextA, SetFocus, SetMenu, SetWindowLongA, SetWindowPos,
SetWindowTextA, ShowWindow, TranslateMessage, wsprintfA, wvsprintfA

( 0 exports )

TrID  : File type identification
WinRAR Self Extracting archive (95.7%)
Win32 Executable Generic (1.5%)
Win32 Dynamic Link Library (generic) (1.4%)
Win32 Executable Watcom C++ (generic) (0.4%)
Generic Win/DOS Executable (0.3%)

ssdeep:
6144:u6YajbofxCvQYzfxlBXAhR4eLEXf1r2rEo0wCmmY2iKEg3bS6X7QoDe2xkZSB:WWIYr7Va
iXNMPEY2iK53btcoK9W

PEiD  : -
```

```
packers (Kaspersky): PE-Crypt.XorPE, PE-Crypt.XorPE, UPX, UPX
packers (F-Prot): RAR, XORCrypt, UPX
RDS    : NSRL Reference Data Set
-
```

**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