Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **ZiGuangWC_Setup.exe**
Submission date: **2011-12-06 14:49:11 (UTC)**
Current status: **finished**
Result: **2/ 42 (4.8%)**

VT Community

not reviewed
Safety score: -

Compact Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.12.06.01	2011.12.06	-
AntiVir	7.11.18.253	2011.12.06	TR/Obfuscated.XY.1143
Antiy-AVL	2.0.3.7	2011.12.06	-
Avast	6.0.1289.0	2011.12.06	-
AVG	10.0.0.1190	2011.12.06	-
BitDefender	7.2	2011.12.06	-
ByteHero	1.0.0.1	2011.11.29	-
CAT-QuickHeal	12.00	2011.12.06	-
ClamAV	0.97.3.0	2011.12.06	-
Commtouch	5.3.2.6	2011.12.06	-
Comodo	10859	2011.12.06	-
DrWeb	5.0.2.03300	2011.12.06	-
Emsisoft	5.1.0.11	2011.12.06	-
eSafe	7.0.17.0	2011.12.06	-
eTrust-Vet	37.0.9606	2011.12.06	-
F-Prot	4.6.5.141	2011.11.29	-
F-Secure	9.0.16440.0	2011.12.06	Backdoor.Generic.392289
Fortinet	4.3.388.0	2011.12.06	-
GData	22	2011.12.06	-
Ikarus	T3.1.1.109.0	2011.12.06	-
Jiangmin	13.0.900	2011.12.06	-
K7AntiVirus	9.119.5598	2011.12.05	-
Kaspersky	9.0.0.837	2011.12.06	-
McAfee	5.400.0.1158	2011.12.06	-
McAfee-GW-Edition	2010.1D	2011.12.06	-
Microsoft	1.7903	2011.12.06	-
NOD32	6681	2011.12.04	-

Norman	6.07.13	2011.12.06	-
nProtect	2011-12-06.01	2011.12.06	-
Panda	10.0.3.5	2011.12.06	-
PCTools	8.0.0.5	2011.12.06	-
Prevx	3.0	2011.12.06	-
Rising	23.87.01.02	2011.12.06	-
Sophos	4.71.0	2011.12.06	-
SUPERAntiSpyware	4.40.0.1006	2011.12.06	-
TheHacker	6.7.0.1.352	2011.12.01	-
TrendMicro	9.500.0.1008	2011.12.06	-
TrendMicro-HouseCall	9.500.0.1008	2011.12.06	-
VBA32	3.12.16.4	2011.12.05	-
VIPRE	11207	2011.12.05	-
ViRobot	2011.12.6.4811	2011.12.06	-
VirusBuster	14.1.101.0	2011.12.06	-

Additional information Show all

MD5 : 4c6d89edd14047c9b915c4b6dee679ab

SHA1 : 9fe22d02a6fa7c23f28562544f05dfe5cddc0ace

SHA256: 2594d2e33a8aaa3975b8871e9c58bf7d3bd6c1a42939beeee614fcd9b25102d1

ssdeep: 196608:XdooFbtw6yyGe9u08Nt51Gb8KVOid3ne152EvdMnIrl4O2sze1:No0wyZo04S8aJtne+bIru

File size : 10314104 bytes

First seen: 2011-12-06 14:49:11

Last seen : 2011-12-06 14:49:11

TrID:
Win32 Executable Generic (38.4%)
Win32 Dynamic Link Library (generic) (34.1%)
Win16/32 Executable Delphi generic (9.3%)
Generic Win/DOS Executable (9.0%)
DOS Executable Generic (9.0%)

sigcheck:
publisher....:
copyright....: Copyright _2006 Bai Ping_IT
product.....: _____ 1.1
description..: _____ 1.1 Setup
original name: n/a
internal name: n/a
file version.:
comments.....: This installation was built with Inno Setup.
signers.....: -
signing date.: -
verified.....: Unsigned

PEInfo: PE structure information

[[basic data]]
entrypointaddress: 0x9A58
timedatestamp....: 0x2A425E19 (Fri Jun 19 22:22:17 1992)
machinetype.....: 0x14c (I386)

```
[[ 8 section(s) ]]
name, viradd, virsiz, rawdsiz, ntropy, md5
CODE, 0x1000, 0x9174, 0x9200, 6.57, ea92e1415bc80e2738e334267ebbb921
DATA, 0xB000, 0x24C, 0x400, 2.74, f96da19d2571a42bdff1b9e8bd62ec99
BSS, 0xC000, 0xE48, 0x0, 0.00, d41d8cd98f00b204e9800998ecf8427e
.idata, 0xD000, 0x950, 0xA00, 4.43, bb5485bf968b970e5ea81292af2acdba
.tls, 0xE000, 0x8, 0x0, 0.00, d41d8cd98f00b204e9800998ecf8427e
.rdata, 0xF000, 0x18, 0x200, 0.20, 9ba824905bf9c7922b6fc87a38b74366
.reloc, 0x10000, 0x8B4, 0x0, 0.00, d41d8cd98f00b204e9800998ecf8427e
.rsrc, 0x11000, 0x2A00, 0x2A00, 4.50, a94dcd9de77c2865ccb996689ffaeb5e

[[ 8 import(s) ]]
kernel32.dll: DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection,
InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc,
WideCharToMultiByte, TlsSetValue, TlsGetValue, MultiByteToWideChar, GetModuleHandleA,
GetLastError, GetCommandLineA, WriteFile, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile,
RaiseException, GetStdHandle, GetFileSize, GetSystemTime, GetFileType, ExitProcess,
CreateFileA, CloseHandle
user32.dll: MessageBoxA
oleaut32.dll: VariantChangeTypeEx, VariantCopyInd, VariantClear, SysStringLen,
SysAllocStringLen
advapi32.dll: RegQueryValueExA, RegOpenKeyExA, RegCloseKey, OpenProcessToken,
LookupPrivilegeValueA
kernel32.dll: WriteFile, VirtualQuery, VirtualProtect, VirtualFree, VirtualAlloc, Sleep,
SizeofResource, SetLastError, SetFilePointer, SetErrorMode, SetEndOfFile, RemoveDirectoryA,
ReadFile, LockResource, LoadResource, LoadLibraryA, IsDBCSLeadByte, GetWindowsDirectoryA,
GetVersionExA, GetUserDefaultLangID, GetSystemInfo, GetSystemDefaultLCID, GetProcAddress,
GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA,
GetFileSize, GetFileAttributesA, GetExitCodeProcess, GetEnvironmentVariableA,
GetCurrentProcess, GetCommandLineA, GetACP, InterlockedExchange, FormatMessageA,
FindResourceA, DeleteFileA, CreateProcessA, CreateFileA, CreateDirectoryA, CloseHandle
user32.dll: TranslateMessage, SetWindowLongA, PeekMessageA, MsgWaitForMultipleObjects,
MessageBoxA, LoadStringA, ExitWindowsEx, DispatchMessageA, DestroyWindow, CreateWindowExA,
CallWindowProcA, CharPrevA
comctl32.dll: InitCommonControls
advapi32.dll: AdjustTokenPrivileges
```

ExifTool:

```
file metadata
CharacterSet: Unicode
CodeSize: 37376
Comments: This installation was built with Inno Setup.
CompanyName:
EntryPoint: 0x9a58
FileDescription: 1.1 Setup
FileFlagsMask: 0x003f
FileOS: Win32
FileSize: 9.8 MB
FileSubtype: 0
FileType: Win32 EXE
FileVersion:
FileVersionNumber: 0.0.0.0
ImageVersion: 6.0
InitializedDataSize: 17408
LanguageCode: Neutral
LegalCopyright: Copyright ?2006 Bai Ping_IT
LinkerVersion: 2.25
MIMEType: application/octet-stream
MachineType: Intel 386 or later, and compatibles
OSVersion: 1.0
ObjectFileType: Executable application
PEType: PE32
ProductName: 1.1
ProductVersion:
```

```
ProductVersionNumber: 0.0.0.0
Subsystem: Windows GUI
SubsystemVersion: 4.0
TimeStamp: 1992:06:20 00:22:17+02:00
UninitializedDataSize: 0
```

VT Community

This file has never been reviewed by any VT Community member. Be the first one to comment on it!

VirusTotal Team

Add your comment... Remember that when you write comments as an anonymous user they receive the lowest possible reputation. So if you have not signed in yet don't forget to do so. How to markup your comments?

☐ **Goodware** ☐ **Malware** ☐ **Spam attachment/link**
☐ **P2P download** ☐ **Propagating via IM** ☐ **Network worm**
☐ **Drive-by-download**

Preview comment **Post comment**

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*.