

SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties ⓘ

MD5
af5938e97b212fcddf228c5ff3a23c53

SHA-1
e41b9488f0c17dce3c902b07e6aa423c9fca8edb

SHA-256
433b44741f07f2ad673eb936511d498c5a6b7f260f98c4d9a6da70c41a56d855

Vhash
086056655d1d55103023z9004fhz32z29fz

Authentihash
cf81e655811fd490b060e0b137988795c62c7f720793655485de2463ce9e9220

Imphash
4204e1fe9e2e0a7f6bec612446ce171b

SSDEEP
196608:pvJqTb9yDDzuFN1Vg2cyV3He9XyGAetMy0nne/3NM0Qoov:NJUba/aVTcyV3Oaq10e/3WH

TLSH
T149963333DBBCAC78F615183AB534DE7D5524FA5302050622EF14E771A88E6096D33EEA

File type
Win32 EXE

Magic
PE32 executable for MS Windows (GUI) Intel 80386 32-bit

TrID
Win32 Executable MS Visual C++ 4.x (52%) | InstallShield setup (16.6%) | Win32 Executable MS Visual C++ (generic) (12%) | Windows screen saver (5%) | Win64 Executable (generic) (4%)

DetectItEasy
PE32 | Installer: InstallShield (2.02.001) | Compiler: EP:Microsoft Visual C/C++ (5.0-6.0 (1720-9049)) [EXE32] | Compiler: Microsoft Visual C/C++ (5.0) | Linker: Microsoft Linker (5.0) [GUI32]

File size
8.52 MB (8935988 bytes)

PEiD packer
Microsoft Visual C++

F-PROT packer
CAB, appended

History ⓘ

Creation Time
1998-03-26 14:31:20 UTC

First Seen In The Wild
2010-10-01 03:13:38 UTC

First Submission
2006-06-02 00:02:30 UTC

Last Submission

2023-03-14 12:06:46 UTC

[Last Analysis](#)

2023-02-22 00:35:07 UTC

Names ⓘ


Borland C++ Compiler.exe
freecommandLinetools.exe
STUB.EXE
STUB32.EXE
freecommandlinetools.exe
freecommandLinetools(Borland C++ 5.5 Compiler).exe
freecommandLinetools(2).exe
freecommandLinetools(1).exe
freecommandLinetools[1].exe
download.php
freecommandLinetools (1).exe
file-2948284_exe
output.20296997.txt
C++ 5.51.exe
vti-rescan
borland_cplpl_compiler_5.5___freecommandLinetools.exe
borlandcpp_builder55_command_line_tools.exe
9_freecommandLine.exe
downloads.sourceforge.net
287272
1567.exe
~vv1.tmp
4qnzjchqyf644peqfmd6nkschsp4vdw3.exe
Borland C Compiler 5.5.exe
filename
FreeCommandLineTools_exe
bcc55compiler.exe
C++ Compiler 5.5 - free command Line tools.exe
Borland C .exe
freecommandLinetools55.exe
FreeCommandLineTools.exe
af5938e97b212fcddf228c5ff3a23c53
sourceforge.net
borland_c_compiler_5_5_1.exe
C 5.51.exe
freecommandLinetoolsBC55.exe

b55.exe
file-45395_exe
__freecommandLinetools.exe
bcc551_freecommandLinetools.exe
BCC55cmd.exe
20296997
Borland-Cpp_v5-5-1.exe
BCC32.exe
freecommandLinetools (2).exe
Borland C++ Compiler 5.5.exe
freecommandLinetools (3).exe
af5938e97b212fcddf228c5ff3a23c53.e41b9488f0c17dce3c902b07e6aa423c9fca8edb



Signature info ⓘ

Signature Verification

 File is not signed

File Version Information

Copyright	Copyright Copyright © 1996 InstallShield Software Corporation
Product	Product PackageForTheWeb Stub
Description	Description PackageForTheWeb Stub
Original Name	Original Name STUB32.EXE
Internal Name	Internal Name STUB.EXE
File Version	File Version 2.02.001

Portable Executable Info ⓘ

Header

[Target Machine](#)
Intel 386 or later processors and compatible processors

[Compilation Timestamp](#)
1998-03-26 14:31:20 UTC

[Entry Point](#)
49424

[Contained Sections](#)
5

Sections

Name	MD5
+ .text	3661b737327af2b4716bc8d6408044c0
+ .rdata	60728361d8e88e954c65497f791555c9
+ .data	f8a2385135919496e047f725021eea9e
+ .idata	6916068ef15055ec5c13a72ba42fd937
+ .rsrc	ad77b58dfeac466d1ca1741e6e99073f

Imports

— ADVAPI32.dll

RegCloseKey
RegOpenKeyExA
RegQueryValueExA

— KERNEL32.dll

CloseHandle
CompareStringA
CreateDirectoryA
CreateFileA
CreateFileMappingA
CreateProcessA
DeleteFileA
DosDateTimeToFileTime
ExitProcess
FindClose
✓

— LZ32.dll

LZClose
LZCopy
LZOpenFileA

— USER32.dll

CharNextA
CreateDialogParamA
CreateWindowExA
DestroyWindow
DialogBoxParamA

DispatchMessageA

EnableWindow

EndDialog

GetClassNameA

GetClientRect



SHELL32.dll

SHBrowseForFolderA

ShellExecuteA

SHGetPathFromIDListA

GDI32.dll

CreateFontIndirectA

DeleteObject

GetDeviceCaps

GetObjectA

GetTextExtentPointA

SelectObject

SetBkMode

SetTextColor

TextOutA

COMCTL32.dll

Ord(17)

PropertySheetA

Contained Resources By Type

RT_STRING

6

RT_DIALOG

6

RT_ICON

5

RT_GROUP_ICON

2

RT_VERSION

1

RT_BITMAP

1

AVI

1

RTF

1

Contained Resources By Language

ENGLISH US

23

Contained Resources

SHA-256

- + 11bd13d42f1f62fdd4bb646455842b5b55b564a7d1c40d4bbb567fb7db437344
- + 0faf5be8726e94f306acdcb387052b1a949fb6639c977d01f957c46608ab37ff
- + 69c6ad296384fe515d9587d9328b2e47e3a12d0c5d54607468ef3802898ea3c4
- + c8a16cb6c6e87f43c7549beb9b46f019b98c424941094d5e4cf1cffee3af7903
- + 000da3f3245370301ebf0768da21e47183e87252045ccd520e3a4e6f1d08f514
- + ebdd41b1f18eccbf540cbaca2706bbab01f644060c857282158a1e1afb5b2a26
- + e43602c81bf8c22ec403f1e859ba1341a667cc1499b0249225dec7721406e523
- + 0a1aaeccc53ede5cdbaf1f5cbd0c83421a2d0902424b955cc2aea98c5d785ef6
- + 98a9b93ecf50ef3be8568126be5de227a76dff99852ab3f36908b31db059dad1
- + ccfc798618c7494bb2c2140eb28e1f472578def8e314ff8b1dfb59f9c9bab925



Overlay

entropy

7.999466896057129

offset

130560

chi2

6650.24

filetype

unknown

md5

69af37a1199c46c75f2cd55647c2ee25

size

8805428

