



SHA256: a888d8d51ab2d34af0fbfb4f60a2f1149c1e6245aec38b4051634c09f37ebce6

File name: Runtime.exe

Detection ratio: 0 / 55

Analysis date: 2016-03-01 21:56:24 UTC (1 minute ago)



- Analysis
- File detail
- Additional information
- Comments
- Votes

The file being studied is a **Portable Executable file**! More specifically, it is a Win32 EXE file for the Windows GUI subsystem.

FileVersionInfo properties

Copyright	Copyright © 2014 Everest Software LLC. All Rights Reserved.
Internal name	Runtime
File version	0.0.0.0

Packers identified

PEiD BobSoft Mini Delphi -> BoB / BobSoft

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2015-04-07 11:13:18
Entry Point	0x01060714
Number of sections	11

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	17146428	17146880	6.40	db846da1f683d506c3a72d3fe8e77e71
.itext	17154048	18516	18944	6.39	3805758147af298196ed91d034e53504
.data	17174528	518756	519168	5.18	36b2ccd6f362ce19616fb68feb109377
.bss	17694720	326952	0	0.00	d41d8cd98f00b204e9800998ecf8427e
.idata	18022400	36930	37376	5.40	1fbbac366dad0e95ef1add8b8ee216d1
.didata	18063360	3506	3584	4.87	3daacad3d665f95c6933b0ccf8143bda
.edata	18067456	78	512	0.92	4c051e1227cd932f2c969913b28fc5ab
.tls	18071552	856	0	0.00	d41d8cd98f00b204e9800998ecf8427e
.rdata	18075648	24	512	0.28	11068f5849dfb5c3f534affe78bfa5c0
.reloc	18079744	1148992	1149440	6.75	e035407ef5321b44a764ad0ca05e3849

Show all

PE imports

[+] AVICAP32.DLL ()

[+] IMAGEHLP.DLL ()

[+] MsVfw32.dll ()

[+] advapi32.dll ()

[+] comctl32.dll ()

[+] comdlg32.dll ()

[+] gdi32.dll ()

[+] gdiplus.dll ()

[+] iphlapi.dll ()

[+] kernel32.dll ()

[+] mpr.dll ()

[+] msimg32.dll ()

[+] ole32.dll ()

[+] oleaut32.dll ()

[+] olepro32.dll ()

[+] shell32.dll ()

[+] user32.dll ()

[+] usp10.dll ()

[+] version.dll ()

[+] wininet.dll ()

[+] winmm.dll ()

[+] winspool.drv ()

[+] wsock32.dll ()

➡ PE exports

madTraceProcess

🔍 Number of PE resources by type

RT_RCDATA	301
RT_BITMAP	264
RT_STRING	102
RT_GROUP_CURSOR	29
RT_CURSOR	29
RT_ICON	10
RT_GROUP_ICON	10
RT_MANIFEST	3
RT_DIALOG	2
MAD	2
TYPELIB	1
RT_VERSION	1

🚩 Number of PE resources by language

NEUTRAL	504
ENGLISH US	153
DUTCH BELGIAN	92

DUTCH	3
RUSSIAN	1
SPANISH URUGUAY	1

👁 ExifTool file metadata	
UninitializedDataSize	0
LinkerVersion	2.25
ImageVersion	0.0
FileVersionNumber	0.0.0.0
LanguageCode	English (U.S.)
FileFlagsMask	0x003f
CharacterSet	Windows, Latin1
InitializedDataSize	3899392
EntryPoint	0x1060714
MIMEType	application/octet-stream
Subsystem	Windows GUI
FileVersion	0.0.0.0
TimeStamp	2015:04:07 12:13:18+01:00
FileType	Win32 EXE
PEType	PE32
InternalName	Runtime
ProductVersion	0
SubsystemVersion	5.0
OSVersion	5.0
FileOS	Win32
LegalCopyright	Copyright 2014 Everest Software LLC. All Rights Reserved.
MachineType	Intel 386 or later, and compatibles
CodeSize	17165824
FileSubtype	0
ProductVersionNumber	0.0.0.0
FileTypeExtension	exe
ObjectFileType	Executable application