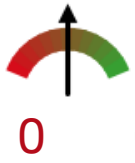
SHA256: 1267b8729bd803b8ade0cb9f5ef78b1f1b344fb7a6815ba27c2ac087dcd0c33f

File name: S7DOS DLL

Detection ratio: 0 / 55

Analysis date: 2015-11-14 21:54:50 UTC (3 months, 2 weeks ago)



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

Authenticode signature block and FileVersionInfo properties

Copyright	Copyright (c) SIEMENS AG 2006-2012
Publisher	Siemens AG
Product	SIMATIC Device Operating System®
Original name	S7OTBLDX.DLL
Internal name	S7DOS DLL
File version	K08.02.06.00_01.03.00.02 release
Description	STEP 7 Block Administration
Signature verification	Signed file, verified signature
Signing date	11:49 AM 6/29/2012
Signers	[+] Siemens AG [+] VeriSign Class 3 Code Signing 2010 CA [+] VeriSign
Counter signers	[+] Symantec Time Stamping Services Signer - G3 [+] VeriSign Time Stamping Services CA [+] Thawte Timestamping CA

PE header basic information

Target machine	Intel 386 or later processors and compatible processors
Compilation timestamp	2012-06-29 10:32:25
Entry Point	0x0009C423
Number of sections	6

PE sections

Name	Virtual address	Virtual size	Raw size	Entropy	MD5
.text	4096	818944	819200	5.79	26824c00b12065791dc39fb423c37a50
.rdata	823296	27520	28672	3.99	d1d9f61beb3fb402e5b517943f890e29
.data	851968	283768	253952	4.88	2e192f6ae87d156639abc377fb32f2c0
.idata	1138688	6002	8192	3.61	4a2879c6a0f40d7ff61706a1d34ba33d

.rsrc	1146880	5289	8192	2.00	2fbfc5be2e64b6abd96787a67823cc2a
.reloc	1155072	56558	57344	6.44	b6d4ffefddd1dca2e5b085a01326a986

☰ Overlays

MD5	812f23aca577ca2ecd5d4e15c87e5040
File type	data
Offset	1179648
Size	7464
Entropy	7.36

🡒 PE imports

[+] ADVAPI32.dll ()

[+] GDI32.dll ()

[+] KERNEL32.dll ()

[+] S7EPAAPI.dll ()

[+] S7ONLINX.dll ()

[+] SHELL32.dll ()

[+] USER32.dll ()

[+] VERSION.dll ()

🡓 PE exports

??4I4link_st@@QAEAAU0@ABU0@@Z

s7H_start_cpu

s7H_stop_cpu

s7H_switch_master_reserve

s7_Simulation_SetMsg

s7_clear_password

s7_conv_errno

s7_conv_ret

s7_event

s7_event_cancel

s7_event_info

s7_get_password

s7_set_password

s7ag_besy_update

s7ag_brcv_create

s7ag_brcv_delete

s7ag_bsnd

s7ag_bub_cycl_read_create

s7ag_bub_cycl_read_delete

s7ag_bub_cycl_read_start

s7ag_bub_cycl_read_stop

s7ag_bub_read_var

s7ag_bub_read_var_seg

s7ag_bub_write_var

s7ag_bub_write_var_seg

s7ag_compress

s7ag_link_in

s7ag_mem_mode

s7ag_msg_mode

s7ag_password

s7ag_pmc_msg_ack

s7ag_pmc_msg_mode

s7ag_pmc_msg_on_off

s7ag_pmc_update

s7ag_read_szl

s7ag_read_time

s7ag_read_time_ex

s7ag_resume

s7ag_start

s7ag_stop

s7ag_test

s7ag_test_delete

s7ag_write_time

s7ag_write_time_ex

s7blk_delete

s7blk_findfirst

s7blk_findnext

s7blk_read

s7blk_write

s7db_close

s7db_copy

s7db_create

s7db_delete

s7db_open

s7dos_release

s7dos_trace

s7dos_version

s7dp_set_slave_address

s7dp_slave_diagnose

s7dpt_read

s7dpt_write

s7epr_image_read

s7epr_image_write

s7epr_kb_memory

s7epr_kennbit

s7epr_physical_rd

s7epr_physical_wr

s7epr_property

s7epr_service

s7ie_CheckIsIPAddressFree

s7ie_CloseServer

s7ie_DeletePGIPAddress

s7ie_GetAdapterInfo

s7ie_GetDataset

s7ie_GetIeParam

s7ie_GetMacAddress

s7ie_GetNetworkParamExt

s7ie_GetPGIPAddressList

s7ie_Identify

s7ie_IdentifyName

s7ie_Identify_Cancel

s7ie_IsReachable

s7ie_SearchAndSetPGIPAddress

s7ie_SearchForFreeIPAddress

s7ie_SetDataset

s7ie_SetIeParam

s7ie_SetNameOfStation

s7ie_SetNetworkParam

s7ie_SetNetworkParamExt

s7ie_ShowLocation

s7l7_dataexchange2

s7l7_download_domain

s7l7_pi_service

s7l7_pi_service_ex

s7l7_upload_domain

s7net_get_baudrate

s7net_get_bus_params

s7net_get_diagnose

s7net_get_direct_plc

s7net_get_life_list

20 more exports

Contract

Number of PE resources by type

RT_VERSION	1

Number of PE resources by language

GERMAN	1

Debug information

Type	Timestamp	Offset	Size
IMAGE_DEBUG_TYPE_CODEVIEW (2) ()	Fri Jun 29 10:32:25 2012	840328	80 Bytes

ExifTool file metadata

SubsystemVersion	4.0
LinkerVersion	8.0

ImageVersion	0.0
FileSubtype	0
FileVersionNumber	802.600.103.2
UninitializedDataSize	0
LanguageCode	English (U.S.)
FileFlagsMask	0x003f
CharacterSet	Unicode
InitializedDataSize	389120
EntryPoint	0x9c423
OriginalFileName	S7OTBLDX.DLL
MIMEType	application/octet-stream
LegalCopyright	Copyright (c) SIEMENS AG 2006-2012
FileVersion	K08.02.06.00_01.03.00.02 release
TimeStamp	2012:06:29 11:32:25+01:00
FileType	Win32 DLL
PEType	PE32
InternalName	<sprachunabhaengig>
ProductVersion	K08.02.06.00_01.03.00.02
FileDescription	<ohne Sprachangabe>
OSVersion	4.0
FileOS	Win32
Subsystem	Windows GUI
MachineType	Intel 386 or later, and compatibles
CompanyName	SIEMENS AG
CodeSize	819200
ProductName	SIMATIC Device Operating System
ProductVersionNumber	802.600.103.2
FileTypeExtension	dll
ObjectFileType	Dynamic link library