ID: 800687
Sample Name:
FileOpenInstaller.exe
Cookbook: default.jbs
Time: 18:09:40
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

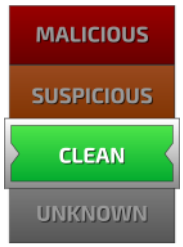
FileOpenInstaller.exe

Overview

General Information

Sample Name:	FileOpenInstaller.exe
Analysis ID:	800687
MD5:	599ebd4af3128..
SHA1:	ee40630abcb1…
SHA256:	f469734bc576a..
Infos:	

Detection

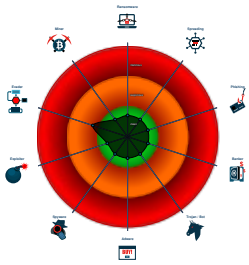


Score:	17
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Obfuscated command line found
- Uses 32bit PE files
- Sample file is different than original …
- Drops PE files
- PE file contains sections with non-s…
- Allocates memory within range whic…
- PE file contains executable resourc…
- Creates a process in suspended mo…

Classification



Analysis Advice

Sample searches for specific file, try point organization specific fake files to the analysis machine
Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Process Tree

- **System is w7x64**
- FileOpenInstaller.exe (PID: 1216 cmdline: C:\Users\user\Desktop\FileOpenInstaller.exe MD5: 599EBD4AF31288DB879786F49BF9487D)
  - FileOpenInstaller.tmp (PID: 1184 cmdline: "C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp" /SL5="$202B6,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" MD5: B7988AC379CEAA456BAA3EF19EB55263)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

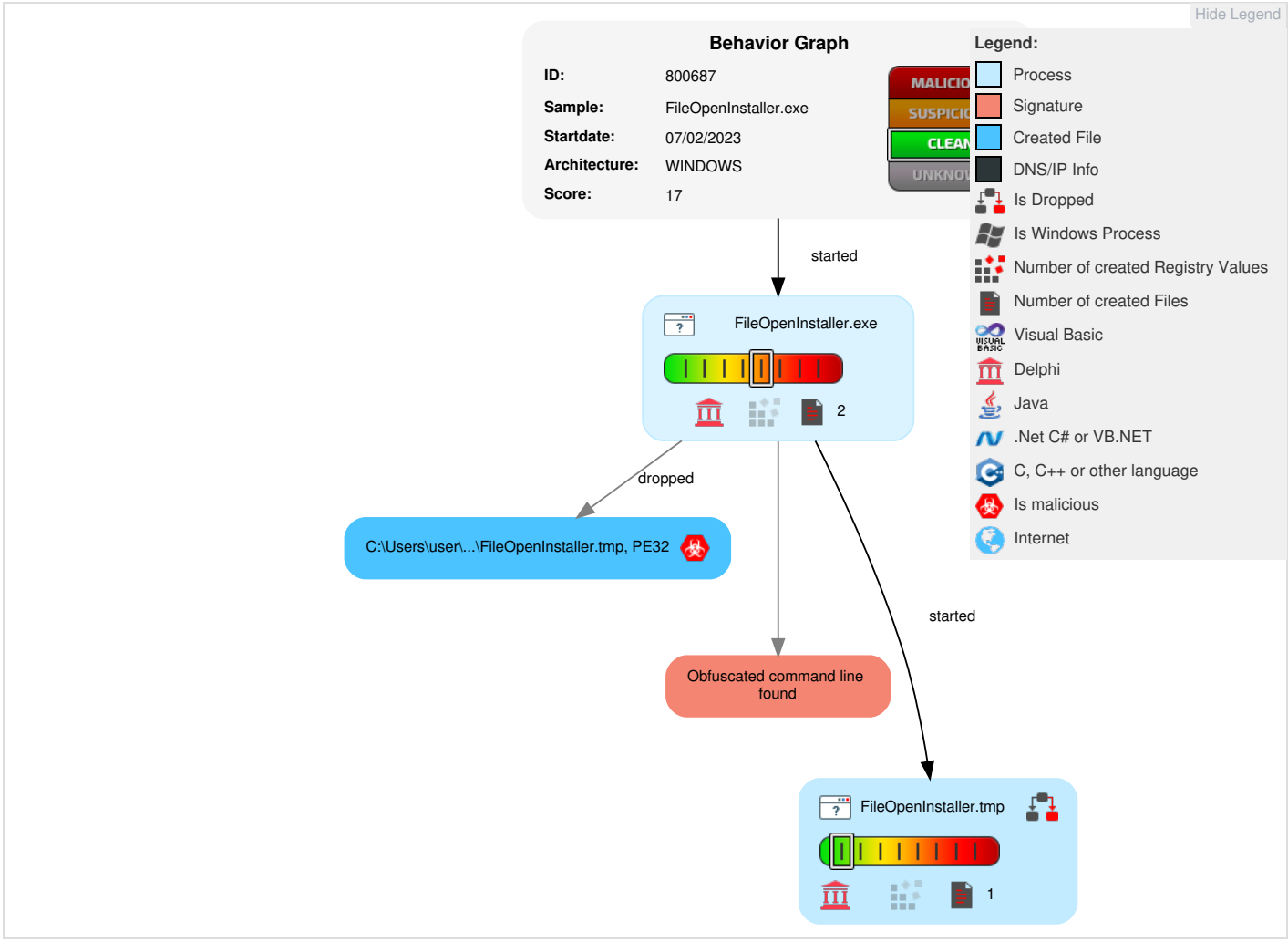
Data Obfuscation

Obfuscated command line found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 1 Process Injection	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

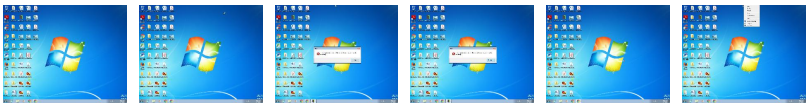
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FileOpenInstaller.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://www.remobjects.com/ps	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	FileOpenInstaller.exe, 00000001.00000003.907181765.0000000002410000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.exe, 00000001.00000003.907784834.000000007ECB0000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000002.00000000.909042225.0000000000401000.00000020.00000001.01000000.00000004.sdmp, FileOpenInstaller.tmp.1.dr	false	• URL Reputation: safe	unknown
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	FileOpenInstaller.exe	false		high
http://www.fileopen.com/0	FileOpenInstaller.exe, FileOpenInstaller.tmp.1.dr	false		high
http://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000001.00000003.917681244.000000000062A000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000002.00000003.916780670.000000000099D000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.remobjects.com/ps	FileOpenInstaller.exe, 00000001.00000003.907181765.0000000002410000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.exe, 00000001.00000003.907784834.000000007ECB0000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000002.00000000.909042225.0000000000401000.00000020.00000001.01000000.00000004.sdmp, FileOpenInstaller.tmp.1.dr	false	• URL Reputation: safe	unknown
http://www.fileopen.com/request-tech-support/Zhttp://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000001.00000003.905803433.00000000022D0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/Q	FileOpenInstaller.exe, 00000001.00000003.917681244.000000000062A000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/q	FileOpenInstaller.tmp, 00000002.00000003.916780670.000000000099D000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800687
Start date and time:	2023-02-07 18:09:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	FileOpenInstaller.exe
Detection:	CLEAN
Classification:	clean17.winEXE@3/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- VT rate limit hit for: FileOpenInstaller.exe

Simulations

Behavior and APIs

Time	Type	Description
18:10:22	API Interceptor	38x Sleep call for process: FileOpenInstaller.tmp modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt

Process:	C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp

File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1100
Entropy (8bit):	5.1148711354880705
Encrypted:	false
SSDEEP:	24:21g4XM47BOdXBs9OBOvzuHeWrOMdL7YjNzBEvo:gzXMe2ROOBOa+W6EL7QNlEvo
MD5:	E592A6BBE98B59DCCE026C69E35411D6
SHA1:	7161F1BB99730354B162F183260513543E9261A7
SHA-256:	278DA06FBD78E12DF7F7EA8A2F85F690B9F5B1EA4D07D99017F6ABD7FD874DEF
SHA-512:	FACD18EC182336C4BED89CA5B1408E3D5826072DE4CB5288FE974F6AB4E706E201DAD0A0478B64B80F7851CBC05F4175737C5FA24642FC97125667FE222992C
Malicious:	false
Reputation:	low
Preview:	.2023-02-07 18:10:22.073 Log opened. (Time zone: UTC-08:00)..2023-02-07 18:10:22.073 Setup version: Inno Setup version 6.0.4 (u)..2023-02-07 18:10:22.073 Original Setup EXE: C:\Users\user\Desktop\FileOpenInstaller.exe..2023-02-07 18:10:22.073 Setup command line: /SL5="$202B6,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" ..2023-02-07 18:10:22.073 Windows version: 6.1.7601 SP1 (NT platform: Yes)..2023-02-07 18:10:22.073 64-bit Windows: Yes..2023-02-07 18:10:22.073 Processor architecture: x64..2023-02-07 18:10:22.073 User privileges: Administrative..2023-02-07 18:10:22.416 Administrative install mode: Yes..2023-02-07 18:10:22.416 Install mode root key: HKEY_LOCAL_MACHINE..2023-02-07 18:10:22.416 64-bit install mode: Yes..2023-02-07 18:10:22.416 Message box (OK):.. This program does not support the version of Windows your computer is running...2023-02-07 18:10:24.927 User chose OK...2023-02-07 18:10:24.927 Got EAbort

C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp

Process:	C:\Users\user\Desktop\FileOpenInstaller.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3119936
Entropy (8bit):	6.073128166324036
Encrypted:	false
SSDEEP:	49152:IR/KpmZubPf2S8W2ILeWl+C1p9jWy5Mnd0wigbLNDH:O/jtYLP1Sy5i0qH
MD5:	B7988AC379CEAA456BAA3EF19EB55263
SHA1:	15C13A91E64739C76FF48E20C5BB4182AAD94339
SHA-256:	69383793D354F2A95D88F610B0559F321F37C97197554CD1E9D6D30B038C352D
SHA-512:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7.....PE..L.....m^.....%.....%.....%...@.....`0.....5./...@.....@.....'.....&..5...0'.|+.....z/.@!..... '.....L.&.H.....&.....text.....%.....%..... ..`.itext...&....%..(....%..... ..`.data...dZ....%..\....%.....@....bss.....x...0&.....idata...5....&..6....&.....@....didata.....&.....@&.....@....edata.....'.....J&.....@..@.tls....D.....'.....rdata..].... '.....L&.....@..@.rsrc...|+...0'.,...N&.....@..@.....(.....'.....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.779130580328553
TrID:	• Win32 Executable (generic) a (10002005/4) 98.45% • Inno Setup installer (109748/4) 1.08% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	FileOpenInstaller.exe
File size:	6831336
MD5:	599ebd4af31288db879786f49bf9487d
SHA1:	ee40630abcb1fe05051c3f832c72c2ee99722c35
SHA256:	f469734bc576a00e113bc43b1b1a13de3c74f5370c5b9db8b9289bd9cf8aac31
SHA512:	1f5ab864f07bfc0900eefbc5dbc94ead881156262bf401b46c188a9b51af54247d406eb225f7d7479e75817150313e7ddefadf85ca0edc960f34f4db5d4d3f30
SSDEEP:	98304:ZEVrLQI+bHRk0ryjyKY0hMrF2t2nvuk9orCFrGD4pStQgyCsadx0tJnX1BzNE3:sMdDRk0+WG4QCOugtsa70ttX1da3
TLSH:	6E6602AF73A6902ED86A8AF105BAD3104C776F115C06CCDA13F0E5CCDB369A0FD2A655
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	c0d4d4d4d4d4dc60

Static PE Info

General

Entrypoint:	0x4b5eec
Entrypoint Section:	.itext
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5E6D1B8D [Sat Mar 14 17:59:41 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	5a594319a0d69dbc452e748bcf05892e

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 3/1/2021 4:00:00 PM 3/1/2023 3:59:59 PM
Subject Chain	• CN=FileOpen Systems Inc., O=FileOpen Systems Inc., L=Santa Cruz, S=California, C=US, SERIALNUMBER=5070649, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization
Version:	3
Thumbprint MD5:	672CE4183DD35C3C4E6ABD4CAF549C09
Thumbprint SHA-1:	42E58D6C0DCC7076DDEB6E71534CB1F0913CD6C9
Thumbprint SHA-256:	BB460A91449CA5F96957CE80966CF8CC861F26A2FAA340DD81D50A41B9885AE8
Serial:	0FDAD5722CB13F7F2013A1CA98D144FE

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax

Instruction
mov eax, 004B10D8h
call 00007F20D8A615B5h
xor eax, eax
push ebp
push 004B65DEh
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp
xor edx, edx
push ebp
push 004B659Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [004BE634h]
call 00007F20D8B03CC7h
call 00007F20D8B0381Eh
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F20D8A77028h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D3Ch
call 00007F20D8A5C1A7h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D3Ch]
mov dl, 01h
mov eax, dword ptr [004237A4h]
call 00007F20D8A7808Fh
mov dword ptr [004C1D40h], eax
xor edx, edx
push ebp
push 004B6546h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007F20D8B03D4Fh
mov dword ptr [004C1D48h], eax
mov eax, dword ptr [004C1D48h]
cmp dword ptr [eax+0Ch], 01h
jne 00007F20D8B0A34Ah
mov eax, dword ptr [004C1D48h]
mov edx, 00000028h
call 00007F20D8A78984h
mov edx, dword ptr [004C1D48h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc4000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2000	0xf36	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc7000	0x88578	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x681ba8	0x2140	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc6000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc22e4	0x244	.idata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xc3000	0x1a4	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb3604	0xb3800	False	0.34484761272632314	data	6.354329115342966	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0xb5000	0x1684	0x1800	False	0.5445963541666666	data	5.970901565517897	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xb7000	0x37a4	0x3800	False	0.36104910714285715	data	5.0421620677813435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0xbb000	0x6da0	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xc2000	0xf36	0x1000	False	0.3681640625	data	4.8987046479600425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didata	0xc3000	0x1a4	0x200	False	0.345703125	data	2.7563628682496506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0xc4000	0x9a	0x200	False	0.2578125	data	1.8722228665884297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0xc5000	0x18	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xc6000	0x5d	0x200	False	0.189453125	data	1.3838943752217987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x88578	0x88600	False	0.05596571379468378	data	3.1574910512692473	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc7798	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144	English	United States
RT_ICON	0x1097c0	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x119fe8	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x123490	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x1276b8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x129c60	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x12ad08	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x12b690	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_ICON	0x12baf8	0x12428	Device independent bitmap graphic, 256 x 512 x 8, image size 65536	English	United States
RT_ICON	0x13df20	0x4c28	Device independent bitmap graphic, 128 x 256 x 8, image size 16384	English	United States
RT_ICON	0x142b48	0x2ca8	Device independent bitmap graphic, 96 x 192 x 8, image size 9216	English	United States
RT_ICON	0x1457f0	0x1628	Device independent bitmap graphic, 64 x 128 x 8, image size 4096	English	United States
RT_ICON	0x146e18	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x147cc0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x148568	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x148c30	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x149198	0x2868	Device independent bitmap graphic, 128 x 256 x 4, image size 8192	English	United States
RT_ICON	0x14ba00	0xa68	Device independent bitmap graphic, 64 x 128 x 4, image size 2048	English	United States
RT_ICON	0x14c468	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	English	United States
RT_STRING	0x14c650	0x360	data		
RT_STRING	0x14c9b0	0x260	data		
RT_STRING	0x14cc10	0x45c	data		
RT_STRING	0x14d06c	0x40c	data		
RT_STRING	0x14d478	0x2d4	data		
RT_STRING	0x14d74c	0xb8	data		
RT_STRING	0x14d804	0x9c	data		
RT_STRING	0x14d8a0	0x374	data		
RT_STRING	0x14dc14	0x398	data		
RT_STRING	0x14dfac	0x368	data		
RT_STRING	0x14e314	0x2a4	data		
RT_RCDATA	0x14e5b8	0x10	data		
RT_RCDATA	0x14e5c8	0x2c4	data		
RT_RCDATA	0x14e88c	0x2c	data		
RT_GROUP_ICON	0x14e8b8	0x110	data	English	United States
RT_VERSION	0x14e9c8	0x584	data	English	United States
RT_MANIFEST	0x14ef4c	0x62c	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetACP, GetExitCodeProcess, LocalFree, CloseHandle, SizeofResource, VirtualProtect, VirtualFree, GetFullPathNameW, ExitProcess, HeapAlloc, GetCPInfoExW, RtlUnwind, GetCPInfo, GetStdHandle, GetModuleHandleW, FreeLibrary, HeapDestroy, ReadFile, CreateProcessW, GetLastError, GetModuleFileNameW, SetLastError, FindResourceW, CreateThread, CompareStringW, LoadLibraryA, ResetEvent, GetVersion, RaiseException, FormatMessageW, SwitchToThread, GetExitCodeThread, GetCurrentThread, LoadLibraryExW, LockResource, GetCurrentThreadId, UnhandledExceptionFilter, VirtualQuery, VirtualQueryEx, Sleep, EnterCriticalSection, SetFilePointer, LoadResource, SuspendThread, GetTickCount, GetFileSize, GetStartupInfoW, GetFileAttributesW, InitializeCriticalSection, GetThreadPriority, SetThreadPriority, GetCurrentProcess, VirtualAlloc, GetSystemInfo, GetCommandLineW, LeaveCriticalSection, GetProcAddress, ResumeThread, GetVersionExW, VerifyVersionInfoW, HeapCreate, GetWindowsDirectoryW, VerSetConditionMask, GetDiskFreeSpaceW, FindFirstFileW, GetUserDefaultUILanguage, lstrlenW, QueryPerformanceCounter, SetEndOfFile, HeapFree, WideCharToMultiByte, FindClose, MultiByteToWideChar, LoadLibraryW, SetEvent, CreateFileW, GetLocaleInfoW, GetSystemDirectoryW, DeleteFileW, GetLocalTime, GetEnvironmentVariableW, WaitForSingleObject, WriteFile, ExitThread, DeleteCriticalSection, TlsGetValue, GetDateFormatW, SetErrorMode, IsValidLocale, TlsSetValue, CreateDirectoryW, GetSystemDefaultUILanguage, EnumCalendarInfoW, LocalAlloc, GetUserDefaultLangID, RemoveDirectoryW, CreateEventW, SetThreadLocale, GetThreadLocale
comctl32.dll	InitCommonControls
version.dll	GetFileVersionInfoSizeW, VerQueryValueW, GetFileVersionInfoW
user32.dll	CreateWindowExW, TranslateMessage, CharLowerBuffW, CallWindowProcW, CharUpperW, PeekMessageW, GetSystemMetrics, SetWindowLongW, MessageBoxW, DestroyWindow, CharUpperBuffW, CharNextW, MsgWaitForMultipleObjects, LoadStringW, ExitWindowsEx, DispatchMessageW
oleaut32.dll	SysAllocStringLen, SafeArrayPtrOfIndex, VariantCopy, SafeArrayGetLBound, SafeArrayGetUBound, VariantInit, VariantClear, SysFreeString, SysReAllocStringLen, VariantChangeType, SafeArrayCreate
netapi32.dll	NetWkstaGetInfo, NetApiBufferFree
advapi32.dll	RegQueryValueExW, AdjustTokenPrivileges, LookupPrivilegeValueW, RegCloseKey, OpenProcessToken, RegOpenKeyExW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x454058
__dbk_fcall_wrapper	2	0x40d0a0
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

Language of compilation system	Country where language is spoken	Map

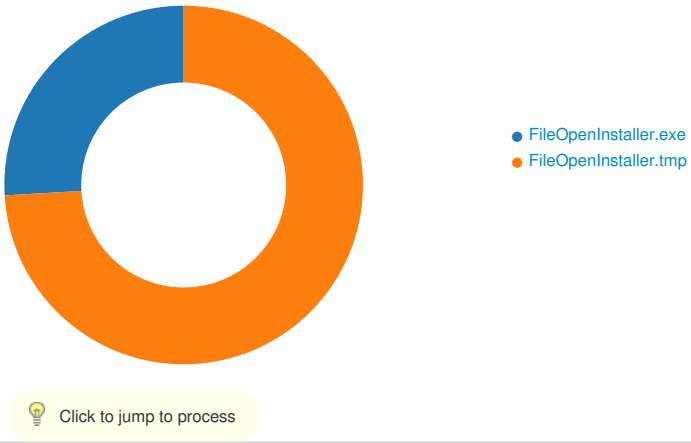
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: FileOpenInstaller.exe PID: **1216**, Parent PID: **1860**

General

Target ID:	1
Start time:	18:10:19
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\FileOpenInstaller.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FileOpenInstaller.exe
Imagebase:	0x400000
File size:	6831336 bytes
MD5 hash:	599EBD4AF31288DB879786F49BF9487D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4AF029	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	423DEA	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp	success or wait	1	427188	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp	0	3119936	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 6e 55 6e 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@InUn!L!This program must be run under Win32$7	success or wait	1	423F10	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	64	success or wait	1	423E74	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	2	423E74	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	2	423E74	ReadFile

Analysis Process: FileOpenInstaller.tmp PID: **1184**, Parent PID: **1216**

General

Target ID:	2
Start time:	18:10:21
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-IK3FC.tmp\FileOpenInstaller.tmp" /SL5="$202B6,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe"
Imagebase:	0x400000
File size:	3119936 bytes
MD5 hash:	B7988AC379CEAA456BAA3EF19EB55263
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	0	3	ff		success or wait	4	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	65	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	136	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	228	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	351	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	428	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	475	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	530	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 30 37 33 20 20 20	2023-02-07 18:10:22.073	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	589	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 34 31 36 20 20 20	2023-02-07 18:10:22.416	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	649	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 34 31 36 20 20 20	2023-02-07 18:10:22.416	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	718	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 34 31 36 20 20 20	2023-02-07 18:10:22.416	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	770	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 32 2e 34 31 36 20 20 20	2023-02-07 18:10:22.416	success or wait	5	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	921	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 34 2e 39 32 37 20 20 20	2023-02-07 18:10:24.927	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	963	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 34 2e 39 32 37 20 20 20	2023-02-07 18:10:24.927	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1012	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 34 2e 39 32 37 20 20 20	2023-02-07 18:10:24.927	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1061	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 30 3a 32 34 2e 39 32 37 20 20 20	2023-02-07 18:10:24.927	success or wait	3	5B6D0C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	64	success or wait	1	5B6C3C	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	2	5B6C3C	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	2	5B6C3C	ReadFile

Disassembly

No disassembly