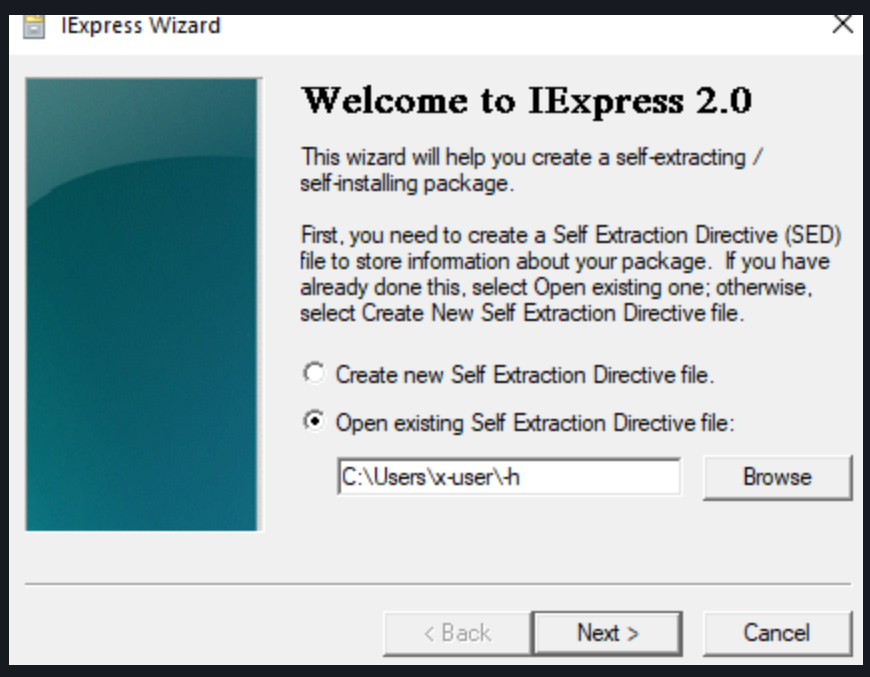
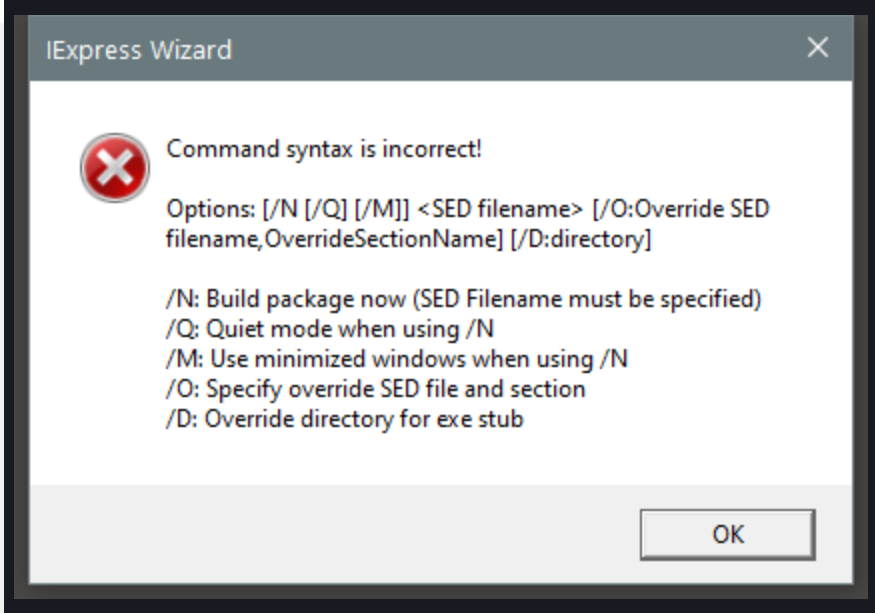
iexpress.exe

>> File Path: `C:\Windows\SysWOW64\iexpress.exe`

>> Description: Wizard

Screenshot





Hashes

Type	Hash
MD5	`D594B2A33EFAFD0EABF09E3FDC05FCEA`
SHA1	`06845890C783ABB305A8C9BBD119DF5DE0A17E6F`
SHA256	`DD2C185DEAE89D41F42FB9903AA274AE70B103EA2285184C4565F39B69DF945F`
SHA384	`E0AC2315C4E8BBB6DFEB784402F1C35B7DA7B203EF2CBDFFE86AC20843AB5128E74280A6ABDAC0FE4401D0FB24E2EB34`
SHA512	`20E26F7CEB672A4B64CF05CA5595611B9FA561B6C141BD0E9FDC777836AF1E343DFFED81B07D8F3636D1E21A1FE42176C0A090DFB711EACD56006F85551E9A43`
SSDEEP	`3072:KLys2qzK5RnUri12NDnGOb+ahXNqJohePnq45L843H:lqzKDKXNDGOb+asEwv5LD`
IMP	`74C91AAB7B963325BC9BC79D27993FB4`
PESHA1	`A4BFE33FBF848C233DA11B8D3E1D322B4D20AE91`
PE256	`C15CD725091D887C0CB9FF709C53592519CA965006E88CEA1B7A09AF48B183A8`

Runtime Data

Child Processes:

explorer.exe

Window Title:

IExpress Wizard

Open Handles:

Path	Type
(R-D) C:\Windows\Fonts\StaticCache.dat	File

(R-D) C:\Windows\SysWOW64\en-US\iexpress.exe.mui	File
(R-D) C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.19041.1_en-us_a8f1da377db0be9e\comctl32.dll.mui	File
(RW-) C:\Users\user	File
(RW-) C:\Windows	File
(RW-) C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.19041.1_en-us_a8f1da377db0be9e	File
(RW-) C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.19041.488_none_89e6152f0b32762e	File
\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000002.db	Section
\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db	Section
\BaseNamedObjects\C:*ProgramData*Microsoft*Windows*Caches*cversions.2	Section
\BaseNamedObjects\NLS_CodePage_1252_3_2_0_0	Section
\BaseNamedObjects\NLS_CodePage_437_3_2_0_0	Section
\Sessions\1\Windows\Theme1175649999	Section
\Windows\Theme601709542	Section

Loaded Modules:

Path
C:\Windows\SYSTEM32\ntdll.dll
C:\Windows\System32\wow64.dll
C:\Windows\System32\wow64cpu.dll
C:\Windows\System32\wow64win.dll
C:\Windows\SysWOW64\iexpress.exe

Signature

- Status: Signature verified.
- Serial: `3300000266BD1580EFA75CD6D3000000000266`
- Thumbprint: `A4341B9FD50FB9964283220A36A1EF6F6FAA7840`
- Issuer: CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
- Subject: CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

File Metadata

- Original Filename: IEXPRESS.EXE.MUI
- Product Name: Internet Explorer
- Company Name: Microsoft Corporation
- File Version: 11.00.19041.1 (WinBuild.160101.0800)
- Product Version: 11.00.19041.1
- Language: English (United States)
- Legal Copyright: Microsoft Corporation. All rights reserved.
- Machine Type: 32-bit

File Scan

- VirusTotal Detections: 0/75

>> VirusTotal Link:
https://www.virustotal.com/gui/file/dd2c185deae89d41f42fb9903aa274ae70b103ea2285184c4565f39b69df945f/detection

File Similarity (ssdeep match)

File	Score
C:\Windows\system32\cabview.dll	58
C:\Windows\system32\iexpress.exe	61
C:\WINDOWS\system32\iexpress.exe	60
C:\Windows\system32\iexpress.exe	69
C:\windows\system32\iexpress.exe	65
C:\WINDOWS\system32\iexpress.exe	74
C:\Windows\system32\iexpress.exe	72
C:\Windows\SysWOW64\cabview.dll	50
C:\windows\SysWOW64\iexpress.exe	68
C:\WINDOWS\SysWOW64\iexpress.exe	75
C:\Windows\SysWOW64\iexpress.exe	71
C:\WINDOWS\SysWOW64\iexpress.exe	68
C:\Windows\SysWOW64\iexpress.exe	66

MIT License. Copyright (c) 2020-2021 Strontic.

FOLLOW: STRONTIC.COM TWITTER GITHUB INSTAGRAM LINKEDIN FACEBOOK EMAIL FEED

© 2022 STRONTIC. Theme: Jekyll & Minimal Mistakes.