ID: 800687
Sample Name:
FileOpenInstaller.exe
Cookbook: default.jbs
Time: 18:37:52
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

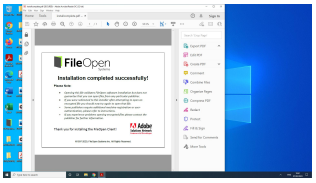
Windows Analysis Report

FileOpenInstaller.exe

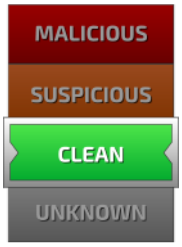
Overview

General Information

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



Detection

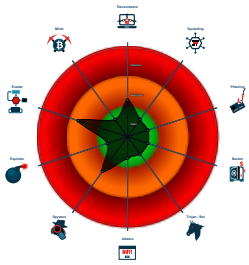


Score:	16
Range:	0 - 100
Whitelisted:	false
Confidence:	20%

Signatures

- Obfuscated command line found
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Sample execution stops while proce…
- JA3 SSL client fingerprint seen in co…
- Contains functionality to call native …

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox
Sample is a service DLL but no service has been registered
Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior
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 w10x64native**
- FileOpenInstaller.exe (PID: 3304 cmdline: C:\Users\user\Desktop\FileOpenInstaller.exe MD5: 599EBD4AF31288DB879786F49BF9487D)
  - FileOpenInstaller.tmp (PID: 6536 cmdline: "C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp" /SL5="$6040A,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" MD5: B7988AC379CEAA456BAA3EF19EB55263)
    - sc.exe (PID: 4948 cmdline: "C:\Windows\system32\sc.exe" create FileOpenManager binpath= "\"C:\Program Files\FileOpen\Services\FileOpenManager64.exe\"" start= auto MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 3300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - sc.exe (PID: 3296 cmdline: "C:\Windows\system32\sc.exe" description FileOpenManager "FileOpen Client Manager" MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 4300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - sc.exe (PID: 2492 cmdline: "C:\Windows\system32\sc.exe" start FileOpenManager MD5: 3FB5CF71F7E7EB49790CB0E663434D80)
      - conhost.exe (PID: 3208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - FileOpenBroker64.exe (PID: 5748 cmdline: C:\Program Files\FileOpen\Services\FileOpenBroker64.exe MD5: DE1A88EBE38A4EB36E2C88B1A69A0251)
    - AcroRd32.exe (PID: 7032 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" installcomplete.pdf MD5: 6791EAE6124B58F201B32F1F6C3EC1B0)
- FileOpenManager64.exe (PID: 5084 cmdline: C:\Program Files\FileOpen\Services\FileOpenManager64.exe MD5: 2ACE6BC0F8B1752879AD54D4EA1938D9)
- FileOpenBroker64.exe (PID: 5344 cmdline: "C:\Program Files\FileOpen\Services\FileOpenBroker64.exe" MD5: DE1A88EBE38A4EB36E2C88B1A69A0251)
- **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

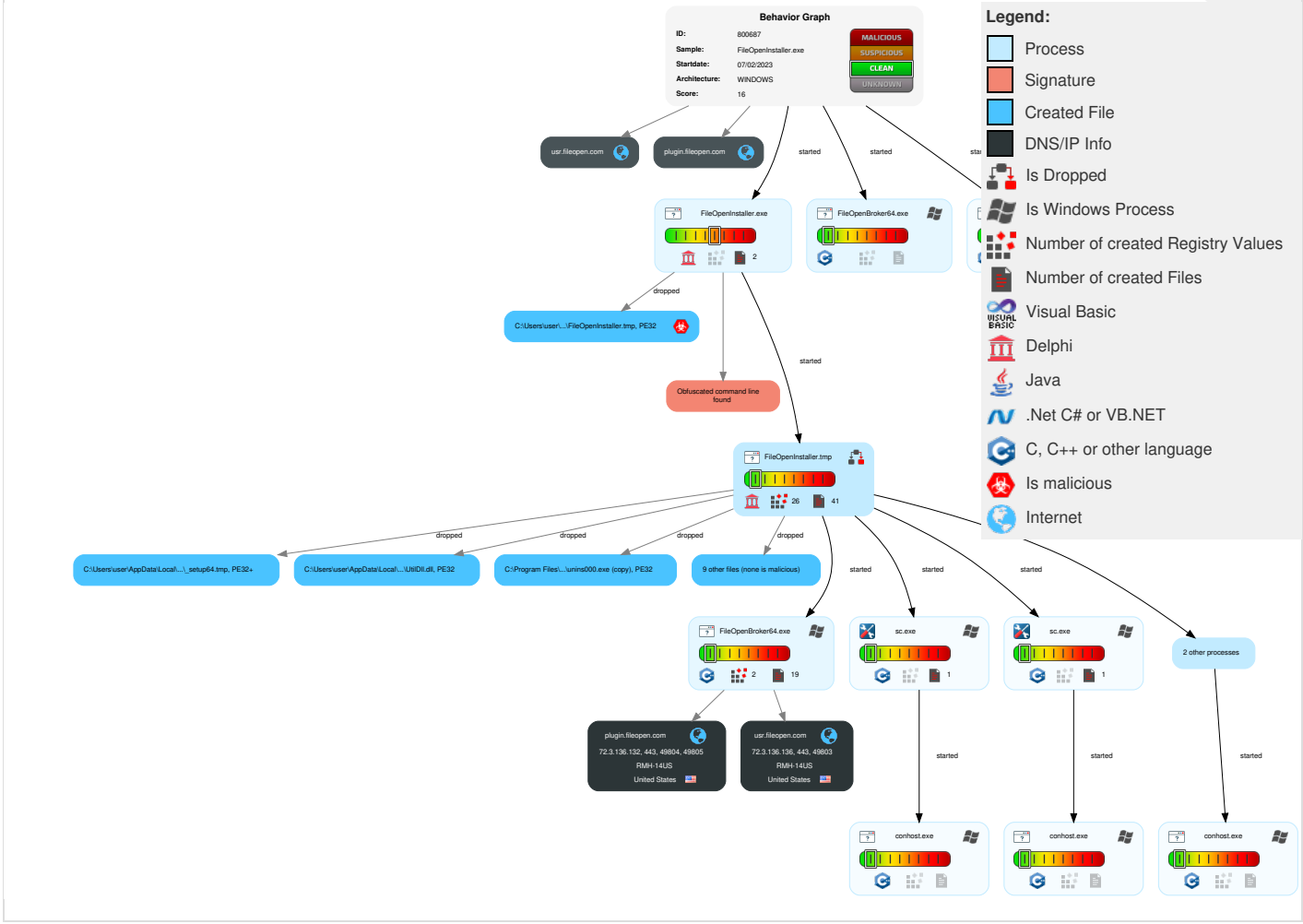
Mitre Att&ck Matrix

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	1 6 Windows Service	1 Access Token Manipulation	3 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 3 Service Execution	1 Registry Run Keys / Startup Folder	1 6 Windows Service	1 Access Token Manipulation	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Native API	1 DLL Side-Loading	1 Process Injection	1 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	NTDS	2 System Owner/User Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 DLL Side-Loading	1 Obfuscated Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph

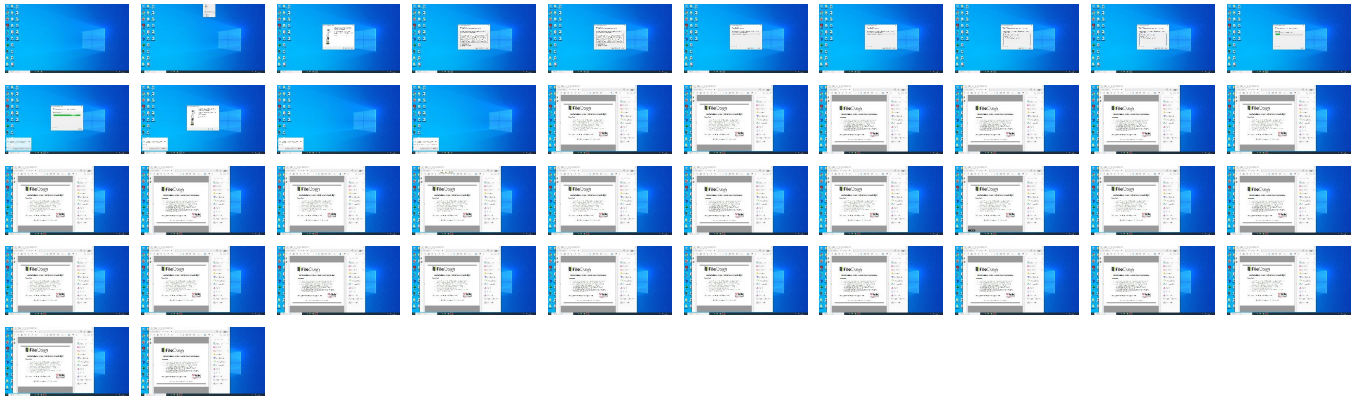
Hide Legend

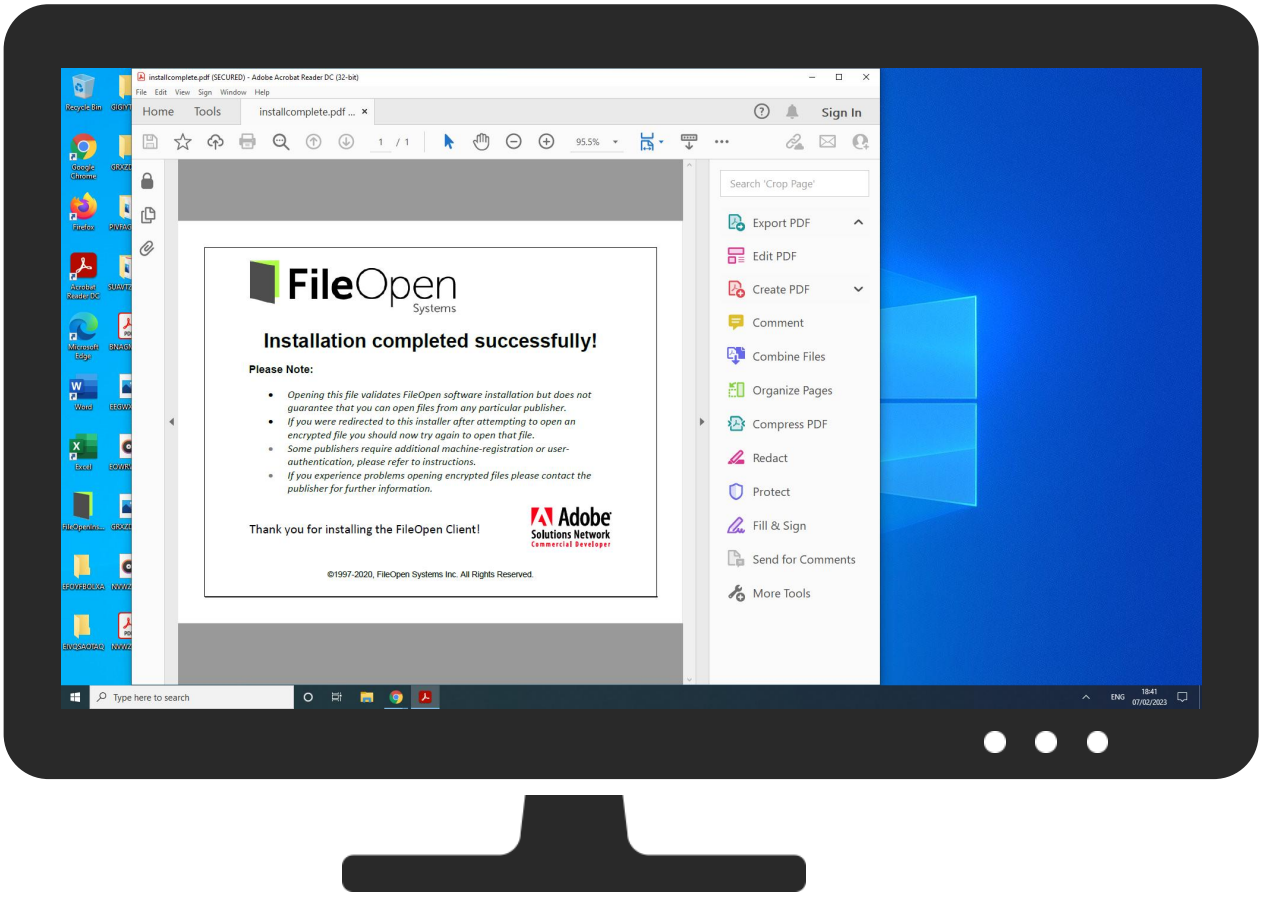


Screenshots

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%	Virustotal		Browse
FileOpenInstaller.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\FileOpen.api (copy)	2%	ReversingLabs		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\FileOpen.api (copy)	0%	Virustotal		Browse
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp	2%	ReversingLabs		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp	0%	Virustotal		Browse
C:\Program Files\FileOpen\Services\FileOpenBroker64.exe (copy)	0%	ReversingLabs		
C:\Program Files\FileOpen\Services\FileOpenManager64.exe (copy)	0%	ReversingLabs		
C:\Program Files\FileOpen\Services\is-FC998.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\Services\is-JKV7N.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\UtilDll.dll (copy)	0%	ReversingLabs		
C:\Program Files\FileOpen\is-9KV5A.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\is-NSHSA.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\unins000.exe (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp\UtilDll.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.remobjects.com/ps	0%	Avira URL Cloud	safe	
http://www.innosetup.com/	0%	Avira URL Cloud	safe	
http://www.innosetup.com/	3%	Virustotal		Browse
http://www.remobjects.com/ps	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
usr.fileopen.com	72.3.136.136	true	false		high
plugin.fileopen.com	72.3.136.132	true	false		high

Contacted URLs

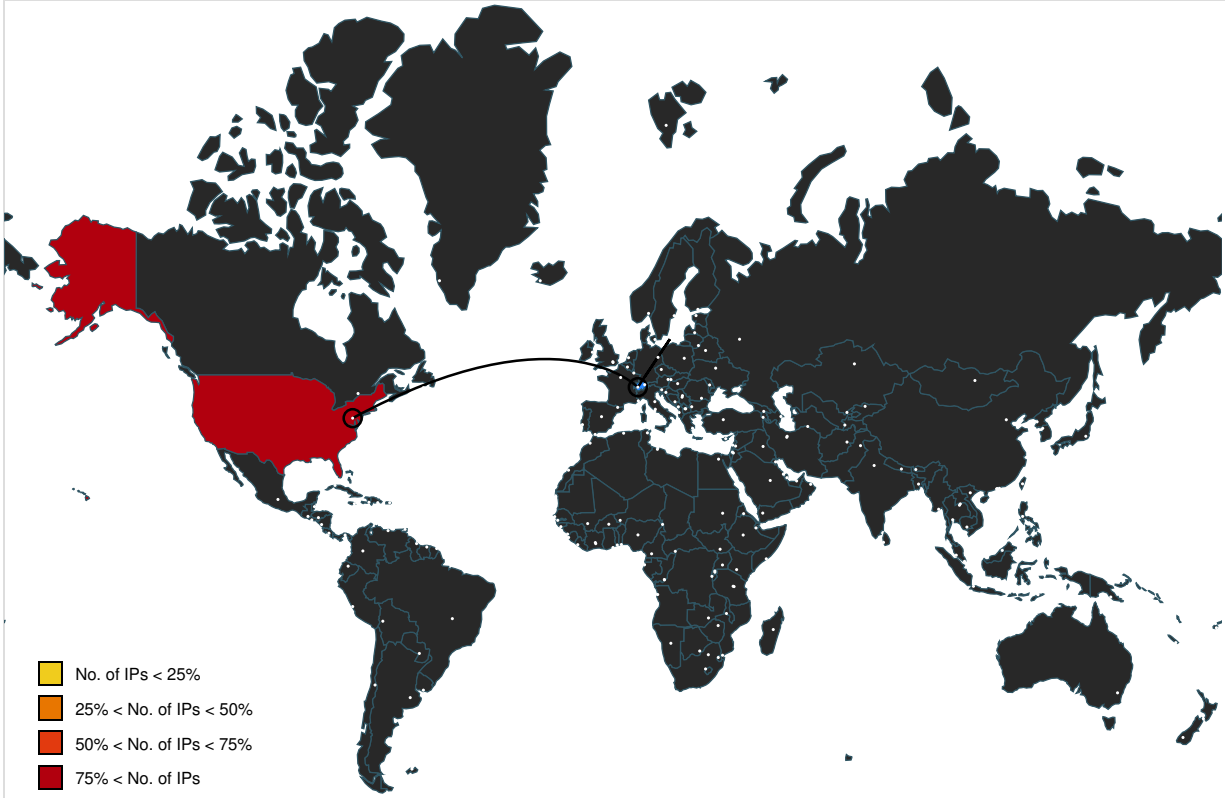
Name	Malicious	Antivirus Detection	Reputation
http://https://usr.fileopen.com/check/usr/ZHAk7YpwDRdZvZq3ePSvK2nhY4hHWUX+9uW5qs0U4Ek=	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	FileOpenInstaller.exe, 00000000.00000003.2487120202.000000007FB50000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.exe, 00000000.00000003.2484508219.0000000002820000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000000.2493227668.0000000000401000.00000020.00000001.01000000.00000005.sdmp, is-NSHSA.tmp.4.dr, FileOpenInstaller.tmp.0.dr	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://fileopen.com/updates	FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003C5E000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003AB5000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003A30000.00000004.00001000.00020000.00000000.sdmp, FileOpenBroker64.exe, 0000000D.00000002.3723165095.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 0000000D.00000000.2735368706.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000010.00000002.2815055164.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000010.00000002.2820538293.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, is-JKV7N.tmp.4.dr, is-GV932.tmp.4.dr	false		high
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	FileOpenInstaller.exe	false		high
http://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000000.00000003.2795690428.000000000243E000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2788287916.00000000025E1000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://usr.fileopen.com/check/usr/ZHAk7YpwDRdZvZq3ePSvK2nhY4hHWUX	FileOpenBroker64.exe, 0000000D.00000002.3718619772.000002253DDD0000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fileopen.com/request-tech-support/Zhttp://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000000.00000003.2483235521.00000000026E0000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2499714116.0000000003650000.00000004.00001000.00020000.00000000.sdmp	false		high
http://fileopen.com	FileOpenBroker64.exe, FileOpenBroker64.exe, 00000010.00000000.2815621930.00007FF668FC8000.00000002.00000001.01000000.00000A.sdmp, is-JKV7N.tmp.4.dr, is-GV932.tmp.4.dr	false		high
http://www.fileopen.com/request-tech-support/q	FileOpenInstaller.tmp, 00000004.00000003.2788287916.00000000025E1000.00000004.00001000.00020000.00000000.sdmp	false		high
http://plugin.fileopen.com/.	FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003C5E000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003AB5000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000003.2775176990.0000000003A30000.00000004.00001000.00020000.00000000.sdmp, FileOpenBroker64.exe, 0000000D.00000002.3723165095.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 0000000D.00000000.2735368706.00007FF668F4B000.00000002.00000001.01000000.00000A.sdmp, FileOpenBroker64.exe, 0000000D.00000002.3718619772.000002253DD40000.00000004.00000020.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000010.00000000.2815055164.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000010.00000002.2817935948.0000021445E97000.00000004.00000020.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000010.00000002.2820538293.00007FF668F4B000.00000002.00000001.01000000.0000000A.sdmp, is-JKV7N.tmp.4.dr, is-GV932.tmp.4.dr	false		high
http://www.fileopen.com/%sPlugin	is-GV932.tmp.4.dr	false		high
http://www.fileopen.com/0	FileOpenInstaller.exe, is-NSHSA.tmp.4.dr, FileOpenInstaller.tmp.0.dr	false		high
http://www.fileopen.com/request-tech-support/0A	FileOpenInstaller.exe, 00000000.00000003.2795690428.000000000243E000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com/installcomplete.ashx?Request=DocPerm&Stamp=1675795218&Mode=CNR&USR=10007	FileOpenBroker64.exe, 0000000D.00000002.3720780457.000002253FA6B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.remobjects.com/ps	FileOpenInstaller.exe, 00000000.00000003.2487120202.000000007FB50000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.exe, 00000000.00000003.2484508219.0000000002820000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000004.00000000.2493227668.0000000000401000.00000020.00000001.01000000.00000005.sdmp, is-NSHSA.tmp.4.dr, FileOpenInstaller.tmp.0.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://plugin.fileopen.com/installcomplete.ashx?Request=Setting&Stamp=1675795217&Mode=CNR&USR=10007	FileOpenBroker64.exe, 0000000D.00000002.3720780457.000002253FA6B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://usr.fileopen.com/_	FileOpenBroker64.exe, 0000000D.00000002.3718619772.000002253DDD0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://usr.fileopen.com/	FileOpenBroker64.exe, 0000000D.00000002.3718619772.000002253DDD0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fileopen.com/%s	is-GV932.tmp.4.dr	false		high
http://plugin.fileopen.com/.n	FileOpenBroker64.exe, 00000010.00000002.2817935948.0000021445E97000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com/	FileOpenBroker64.exe, 0000000D.00000002.3720780457.000002253FA30000.00000004.00000020.00020000.00000000.sdmp, FileOpenBroker64.exe, 0000000D.00000002.3718619772.000002253DDD0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com//&	FileOpenBroker64.exe, 0000000D.00000002.3720780457.000002253FA30000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.3.136.136	usr.fileopen.com	United States		33070	RMH-14US	false
72.3.136.132	plugin.fileopen.com	United States		33070	RMH-14US	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800687
Start date and time:	2023-02-07 18:37:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	19
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:	clean16.winEXE@19/50@2/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 85%) • Quality average: 65.4% • Quality standard deviation: 35.9%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, UsoClient.exe
- Excluded IPs from analysis (whitelisted): 2.19.126.92, 2.19.126.76, 2.21.22.155, 2.21.22.179
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, slscr.update.microsoft.com, acroipm2.adobe.com.edgesuite.net, a122.dscd.akamai.net, ctldl.windowsupdate.com, wdcp.microsoft.com, acroipm2.adobe.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:40:11	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run FileOpenBroker "C:\Program Files\FileOpen\Services\FileOpenBroker64.exe"

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:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\FileOpen.api (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	2241536
Entropy (8bit):	6.648410638768628
Encrypted:	false
SSDEEP:	49152:BusBOEuaRuJCN0900HR88Pix+oiDMpyQmdVqyWy9vSL6TzjolA:BuswEuaRzN090MRnP/fqyWyBS
MD5:	319DDB9C9900DD2BDFE2AF7009BF3A83
SHA1:	B5F8BB5055F944DFBC38720BC30C2747F2989116
SHA-256:	491673ED8FB7AFCF76204DD82079B365F4CD03EBC31452A40D45AA0F952038A5
SHA-512:	DFBBFCF35F39195C326AE7CA2B36224C460B4231AFA042562CE0DA0664316A5068A3BD7544937B53C6167412041DF7D0DB14612FFD11540D097998B52F060E1A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....1.....}.....}... ....}.....}.y.....}.....Rich.....PE..L.....b.....!.....r.....*.....)).....).0.....T..... .....@.....|.....text..... ..`.rdata.....@..@.data.....L.....@....rsrc.....)..... !.....@..@.reloc..0... ..)....2!.....@..B..... .....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2241536
Entropy (8bit):	6.648410638768628
Encrypted:	false
SSDEEP:	49152:BusBOEuaRuJCN0900HR88Pix+oiDMpyQmdVqyWy9vSL6TzjolA:BuswEuaRzN090MRnP/fqyWyBS
MD5:	319DDB9C9900DD2BDFE2AF7009BF3A83
SHA1:	B5F8BB5055F944DFBC38720BC30C2747F2989116
SHA-256:	491673ED8FB7AFCF76204DD82079B365F4CD03EBC31452A40D45AA0F952038A5
SHA-512:	DFBBFCF35F39195C326AE7CA2B36224C460B4231AFA042562CE0DA0664316A5068A3BD7544937B53C6167412041DF7D0DB14612FFD11540D097998B52F060E1A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....1.....}.....}... ....}.....}.y.....}.....Rich.....PE..L.....b.....!.....r.....*.....)).....).0.....T..... .....@.....|.....text..... ..`.rdata.....@..@.data.....L.....@....rsrc.....)..... !.....@..@.reloc..0... ..)....2!.....@..B..... .....

C:\Program Files\FileOpen\Services\FileOpenBroker64.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2089968
Entropy (8bit):	6.41503010887335
Encrypted:	false
SSDEEP:	24576:R+hVl0FSQ2s1dPpvaTRNiNkedM/oyJv0AIOa9IOeBvAUaY0BAARMh8eh+YE7+D:wSFSQ2q9pCeKfv0AhRBvAUYWh8ea7+D
MD5:	DE1A88EBE38A4EB36E2C88B1A69A0251
SHA1:	4C81B58FB221AAC3B36C86A2376A42051F5FB160
SHA-256:	8741A8BB6FBFED7119C1BDECF8EF5C4E5FAEED79208CA1DD78675AC95492B135
SHA-512:	251D051FFEA15C050E61AE4E63F2FCBD50AAAFB92700756D850089D885C203D05AC9B75ABAAB62C767A7A948413D4EB616597BD893C06C557718E731EE52E33 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....g.....L.....t....g.....9.....9. ....9.....9.....9.....Rich.....PE..d.....b....."....D.....@..... !....R. ..`.....c.....c..... .....F...,.....!....xP..T..... .....P..8.....x.....text..... ..`.rdata.....@..@.data.....6...t.....@....pdata...F.....H.....@..@ _RDATA..... .....@..@.rsrc..... .....@..@.reloc.....!.. .....@..B..... .....

C:\Program Files\FileOpen\Services\FileOpenManager64.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	846816
Entropy (8bit):	6.226678050362994
Encrypted:	false
SSDEEP:	12288:lf7ehSp060uzFgjlo85lpywqZdLxCT79mXD4b:lf72Sp0FuzFA6wqZdLxCTJM4b
MD5:	2ACE6BC0F8B1752879AD54D4EA1938D9
SHA1:	C08CAA63D122C0B1DCD6A0855FDD3907905370D8
SHA-256:	D9F13C6BC2F459DAD399BA4E300B054A2205E0D6EFF4353BA7A095F0388258C3
SHA-512:	2B6B4064A66F6482B639E9BC06A6179E649B0F55E57D1CC73647DD5A48010ED3C25E98C25EE4BDB9487DF28B268BDC9EA58455EB924A78B4342296034C884CF7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....%..pK..pK..pK...O..pK...H..pK...N.2pK...O..pK...H..pK...M..p K...N..pK...J..pK..pJ.rpK...6..pK...%..pK...N..pK.....pK..p...pK...I..pK.Rich.pK.....PE..d....b.....".....Z...~.....\.....@..... .....D....`..... .....dJ..x..... ....p...t...z...q.....t...h...T.....8.....p.....text....X.....Z..... ..`.rdata.....p.....^.....@..@.data.....p..... .P.....@....pdata...t...p...v.....@..@_RDATA.....b.....@..@.rsrc... .....d.....@..@.reloc..t.....l.....@..B..... .....

C:\Program Files\FileOpen\Services\is-FC998.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	846816
Entropy (8bit):	6.226678050362994
Encrypted:	false
SSDEEP:	12288:lf7ehSp060uzFgjlo85lpywqZdLxCT79mXD4b:lf72Sp0FuzFA6wqZdLxCTJM4b
MD5:	2ACE6BC0F8B1752879AD54D4EA1938D9
SHA1:	C08CAA63D122C0B1DCD6A0855FDD3907905370D8
SHA-256:	D9F13C6BC2F459DAD399BA4E300B054A2205E0D6EFF4353BA7A095F0388258C3
SHA-512:	2B6B4064A66F6482B639E9BC06A6179E649B0F55E57D1CC73647DD5A48010ED3C25E98C25EE4BDB9487DF28B268BDC9EA58455EB924A78B4342296034C884CF7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....%..pK..pK..pK...O..pK...H..pK...N.2pK...O..pK...H..pK...M..p K...N..pK...J..pK..pJ.rpK...6..pK...%..pK...N..pK.....pK..p...pK...I..pK.Rich.pK.....PE..d....b.....".....Z...~.....\.....@..... .....D....`..... .....dJ..x..... ....p...t...z...q.....t...h...T.....8.....p.....text....X.....Z..... ..`.rdata.....p.....^.....@..@.data.....p..... .P.....@....pdata...t...p...v.....@..@_RDATA.....b.....@..@.rsrc... .....d.....@..@.reloc..t.....l.....@..B..... .....

C:\Program Files\FileOpen\Services\is-JKV7N.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2089968
Entropy (8bit):	6.41503010887335
Encrypted:	false
SSDEEP:	24576:R+hVl0FSQ2s1dPpvaTRNiNkedM/oyJv0AIOa9IOeBvAUaY0BAARMh8eh+YE7+D:wSFSQ2q9pCeKfv0AhRBvAUYWh8ea7+D
MD5:	DE1A88EBE38A4EB36E2C88B1A69A0251
SHA1:	4C81B58FB221AAC3B36C86A2376A42051F5FB160
SHA-256:	8741A8BB6FBFED7119C1BDECF8EF5C4E5FAEED79208CA1DD78675AC95492B135
SHA-512:	251D051FFEA15C050E61AE4E63F2FCBD50AAAFB92700756D850089D885C203D05AC9B75ABAAB62C767A7A948413D4EB616597BD893C06C557718E731EE52E336
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....g.....L.....t....g.....9.....9. .....9.....9.....9.....Rich.....PE..d.....b.....".....D.....@..... !.....R. ..`.....c.....c..... .....F...,.....!....xP..T..... .....P..8.....x.....text..... ..`.rdata.....@..@.data.....6...t.....@....pdata...F.....H.....@..@ _RDATA..... .....@..@.rsrc..... .....@..@.reloc.....!.. .....@..B..... .....

C:\Program Files\FileOpen\UtilDll.dll (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	223744
Entropy (8bit):	6.552035196075477
Encrypted:	false
SSDEEP:	6144:Q4L7/E4GpmEXrLTilLKvMoiLQpQuK2cVAORcC75FI:K4GpmEXrLTiwvlQjuK2arR5FI
MD5:	79F2386CF7296E8661997193CF01BAAD
SHA1:	726FEA5EABC5B38981B1D6CC5B8BE01212C90616
SHA-256:	101EBA215EF5F833EC332DA2C803FBFF060EB55F32A88EC261B5C4192528E6DD
SHA-512:	123F4FFA772FDE8F901ABF12C49B78EB81975E5E5F38A8EF80C10B4CA08DA422C42EE72F51155FC87A6726217A29B0E8BF22CB927347D324D41E87485C5EFF7E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....p...p...p.us...p.uu.n.p.ut...p..mt...p..ms...p..mu..p.uq...p...q..p.Nly...p.Nlp...p.Nl....p.....p.Nlr...p.Rich..p.....PE..L...[F9`.....!.....$...P.....@.....@.....<..l....>..x....p..... ".....p.....@.....@.....@.....text....#.....$..... ..`.rdata.....@.....(.....@..@.data...T....P.....0.....@....rsrc.....p.....@.....@..@.reloc.. ".....$...F.....@..B.....

C:\Program Files\FileOpen\examples\installcomplete.pdf (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PDF document, version 1.6 (zip deflate encoded)
Category:	dropped
Size (bytes):	162991
Entropy (8bit):	**7.995368768567606**
Encrypted:	**true**
SSDEEP:	3072:HAmvwgsSx/UW0CSz15sU1mHNPKYm+HfJkGspEX+OQJv5RComJGD:HbXdECSzvm9KIH7aM+yuD
MD5:	D020B6FF764F08684688E772BCCFFA99
SHA1:	117CCBA4D83B17914F4FF1FFE1996540A041C507
SHA-256:	A6EF65B36F8521FC67269B9FBD024C7E98E0207AE76C8BECA9B289F125F92383
SHA-512:	5C8E7FFD0CBB3205F9164EF83500A9353C3D3F052FA4167AB0F49DE44CA29CF90982CCD767646D339A64A0F26446CEC4BA447D1CFD71388B17DD47F0DFEE358
Malicious:	false
Preview:	%PDF-1.6.%.....38 0 obj<</Linearized 1/L 162991/O 40/E 157459/N 1/T 162689/H [564 199]>>.endobj. ..66 0 obj<</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<FE2312A4B89FD64A94044C8C74BAEF85><7653CFFF47F8504296A48EE78CC73A7D>]/Index[38 50]/Info 37 0 R/Length 128/Prev 162689/Root 39 0 R/Size 88/Type/XRef/W[1 3 1]/Encrypt 87 0 R>>stream..x.cbd`.``b``s....A$.....Dr.....`.).T...`..`R.,..D2>....".?.E.A.....$..7.m...E...m 2#..f,..f..u....K.*..].6...N...&.w 7\b....o..endstream.endobj.startxref..0..%%EOF.. ..86 0 obj<</C 131/Filter/FlateDecode/I 115/Length 113/S 38>>stream..x.c``.b``{.....`.....YL.....,."b..q.rD.m.o...K.....fj...l;..WB..@.OyF..):/...00UYC,`t..L...>.Q.....endstream.endobj. .. ..87 0 obj<</Filter/FOPN_foweb/V 1/Length 40/VEID(9.1)/BUILD(925)/SVID(InstallComplete)/DUID(D-700)/INFO(HgR50GSLkqXShHKestPel17ocyosIBDzOQxbbI1ggGDzJg3a0ibO9nsUYTCH8yDM/ivhsmBnq8p1Au54/T8cq0W8wU5aNOh8aIQgrHDt1oJStrQbMk6GhyM4Cfo

C:\Program Files\FileOpen\examples\is-5NKPI.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PDF document, version 1.6 (zip deflate encoded)
Category:	dropped
Size (bytes):	162991
Entropy (8bit):	**7.995368768567606**
Encrypted:	**true**
SSDEEP:	3072:HAmvwgsSx/UW0CSz15sU1mHNPKYm+HfJkGspEX+OQJv5RComJGD:HbXdECSzvm9KIH7aM+yuD
MD5:	D020B6FF764F08684688E772BCCFFA99
SHA1:	117CCBA4D83B17914F4FF1FFE1996540A041C507
SHA-256:	A6EF65B36F8521FC67269B9FBD024C7E98E0207AE76C8BECA9B289F125F92383
SHA-512:	5C8E7FFD0CBB3205F9164EF83500A9353C3D3F052FA4167AB0F49DE44CA29CF90982CCD767646D339A64A0F26446CEC4BA447D1CFD71388B17DD47F0DFEE358
Malicious:	false
Preview:	%PDF-1.6.%.....38 0 obj<</Linearized 1/L 162991/O 40/E 157459/N 1/T 162689/H [564 199]>>.endobj. ..66 0 obj<</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<FE2312A4B89FD64A94044C8C74BAEF85><7653CFFF47F8504296A48EE78CC73A7D>]/Index[38 50]/Info 37 0 R/Length 128/Prev 162689/Root 39 0 R/Size 88/Type/XRef/W[1 3 1]/Encrypt 87 0 R>>stream..x.cbd`.``b``s....A$.....Dr.....`.).T...`..`R.,..D2>....".?.E.A.....$..7.m...E...m 2#..f,..f..u....K.*..].6...N...&.w 7\b....o..endstream.endobj.startxref..0..%%EOF.. ..86 0 obj<</C 131/Filter/FlateDecode/I 115/Length 113/S 38>>stream..x.c``.b``{.....`.....YL.....,."b..q.rD.m.o...K.....fj...l;..WB..@.OyF..):/...00UYC,`t..L...>.Q.....endstream.endobj. .. ..87 0 obj<</Filter/FOPN_foweb/V 1/Length 40/VEID(9.1)/BUILD(925)/SVID(InstallComplete)/DUID(D-700)/INFO(HgR50GSLkqXShHKestPel17ocyosIBDzOQxbbI1ggGDzJg3a0ibO9nsUYTCH8yDM/ivhsmBnq8p1Au54/T8cq0W8wU5aNOh8aIQgrHDt1oJStrQbMk6GhyM4Cfo

C:\Program Files\FileOpen\is-9KV5A.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	223744
Entropy (8bit):	6.552035196075477
Encrypted:	false
SSDEEP:	6144:Q4L7/E4GpmEXrLTilLKvMoiLQpQuK2cVAORcC75FI:K4GpmEXrLTiwvlQjuK2arR5FI
MD5:	79F2386CF7296E8661997193CF01BAAD
SHA1:	726FEA5EABC5B38981B1D6CC5B8BE01212C90616
SHA-256:	101EBA215EF5F833EC332DA2C803FBFF060EB55F32A88EC261B5C4192528E6DD
SHA-512:	123F4FFA772FDE8F901ABF12C49B78EB81975E5E5F38A8EF80C10B4CA08DA422C42EE72F51155FC87A6726217A29B0E8BF22CB927347D324D41E87485C5EFF7E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....p...p...p.us...p.uu.n.p.ut...p..mt...p..ms...p..mu..p.uq...p...q..p.Nly...p.Nlp...p.Nl....p.....p.Nlr...p.Rich..p.....PE..L...[F9`.....!.....$...P.....@.....@.....<..l....>..x....p..... ".....p.....@.....@.....text....#.....$..... ..`.rdata.....@.....(.....@..@.data...T....P.....0.....@....rsrc.....p.....@.....@..@.reloc.. ".....$...F.....@..B.....

C:\Program Files\FileOpen\is-NSHSA.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
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:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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&.....@..@..... (.....'.....@..@.....

C:\Program Files\FileOpen\unins000.dat

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	InnoSetup Log 64-bit FileOpen Client B998, version 0x418, 28298 bytes, 724536\37\user\37, C:\Program Files\FileOpen\376\377\377\007
Category:	dropped
Size (bytes):	28298
Entropy (8bit):	3.9283973556016476
Encrypted:	false
SSDEEP:	384:JCEwFsZAIXuAhKCVMneFqf8cGKBUorhr+2NQfiA1kK0bPImRZ8dAHM:JQIRYiBKBUoF62lbbZ4
MD5:	AC044F627C6750CDDEDC6466460B8335
SHA1:	F57FFA62EB27BD8DF86C010885F29A4ED1DE25C7
SHA-256:	16C0FD51135214FCEF99AB370B5D6E91478789115259887E5D6E8A36AE84030C
SHA-512:	60A5845FABA55BB9281D34F1F8AA99972BB33D11E85851E46D30AC7C8C9F3A2C0C484AB42CCE6439717EEA7466316EC9A368B8760FE148E58BA7FDA4CD2D5708
Malicious:	false
Preview:	Inno Setup Uninstall Log (b) 64-bit.....FileOpenClient.....FileOpen Client B998.....n.....w.....d.j.....o.....7.2.4.5.3.6.....A.r.t.h.u.r.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.F.i.l.e.O.p.e.n.....(...}.. .....]....IFPS....'...P.....ANYMETHOD.....BOOLEAN.....TWIZARDFORM....TWIZARDFORM.....TMAINFORM....TMAINFORM.....TUNINSTALLPROGRESSFORM....TUNINSTALLPROGRESSFORM.....

C:\Program Files\FileOpen\unins000.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
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:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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&.....@..@..... ..... (.....:'.....@..@.....

C:\Program Files\FileOpen\unins000.msg

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	InnoSetup messages, version 6.0.0, 243 messages (UTF-16), Cancel installation
Category:	dropped
Size (bytes):	23409
Entropy (8bit):	3.2729698372223375
Encrypted:	false
SSDEEP:	192:M1EXSCkf3STsfr69FTyPanTa1tznL7VF+lqfc51U5YQDztXfbKJg/Bfvo:M196ir64+WX+7Q1U5YQDzt7/B3o
MD5:	DD3DDF5C06B1D597A1D4B0897CEAF095
SHA1:	E6BC22523D9AA34063FE76ED9108376DD35C7DD8
SHA-256:	B3F9AF6EC27F42D6F895794CCF28C4100FEFFDF20505E19C6C37A00826D6B82C
SHA-512:	80D57A14EF8AC41E6A1630C5CA4552421A5A6490BED6318068E5AB34440428DF4D7258199A8B06BF158604E079D4D2525DA5E75A781D0E1F15984208FD68268E
Malicious:	false
Preview:	Inno Setup Messages (6.0.0) (u).....$[...../.1.C.a.n.c.e.l. .i.n.s.t.a.l.l.a.t.i.o.n...S.e.l.e.c.t. .a.c.t.i.o.n...&.l.g.n.o.r.e. .t.h.e. .e.r.r.o.r. .a.n.d. .c.o.n.t.i.n.u.e...& .T.r.y. .a.g.a.i.n...&.A.b.o.u.t. .S.e.t.u.p.....%.1. .v.e.r.s.i.o.n. .%.2.....%.3.....%.1. .h.o.m.e. .p.a.g.e.:.....%.4.....A.b.o.u.t. .S.e.t.u.p...Y.o.u. .m.u.s.t. .b.e. .l.o.g.g.e.d. .i.n. .a.s. .a.n. .a.d.m.i.n.i.s.t.r.a.t.o.r. .w.h.e.n. .i.n.s.t.a.l.l.i.n.g. .t.h.i.s. .p.r.o.g.r.a.m.....T.h.e. .f.o.l.l.o.w.i.n.g. .a.p.p.l.i.c.a.t.i.o.n.s. .a.r.e. .u.s.i.n.g. .f.i.l.e.s. .t.h.a.t. .n.e.e.d. .t.o. .b.e. .u.p.d.a.t.e.d. .b.y. .S.e.t.u.p... .I.t. .i.s. .r.e.c.o.m.m.e.n.d.e.d. .t.h.a.t. .y.o.u. .a.l.l.o.w. .S.e.t.u.p. .t.o. .a.u.t.o.m.a.t.i.c.a.l.l.y. .c.l.o.s.e. .t.h.e.s.e. .a.p.p.l.i.c.a.t.i.o.n.s.....T .h.e. .f.o.l.l.o.w.i.n.g. .a.p.p.l.i.c.a.t.i.o.n.s. .a.r.e. .u.s.i.n.g. .f.i.l.e.s. .t.h.a.t. .n.e.e.d. .t.o. .b.e. .u.p.d.a.t.e.d. .b.y. .S.e.t.u.p... .I.t. .i.s. .r.e.

C:\ProgramData\FileOpen\Updates\L10n\fotk_de.lcd (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (12648), with no line terminators
Category:	dropped
Size (bytes):	12648
Entropy (8bit):	5.997991870273226
Encrypted:	false
SSDEEP:	384:vH6NHxuYvSxaFjN43mKAlz03TuslDR6mZ/juc:yNRuYvSxaFJRIqTvlDR6mZ/l
MD5:	1FF1A88C097A10AF0D2CB463BBB5E4C9
SHA1:	D149B1D0BCD84FAD9A4BD143E7837999BC840141
SHA-256:	3E077B1A201D71636DD045F7B2694AFEE90881DF97704B012DC947C7429492A7
SHA-512:	82AA26F7E0D877A0BEA8D55C57D4D6B98DF283C04360C730E6ED385A589D16438F9BC00B80609B48C33028202661E7343DD4A13A53AE31B6C9A4D8C2E63D102
Malicious:	false
Preview:	lcd&000100000000004400002496000100 72wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zRFBKRDtypz8MHsvOxXIrTq4HwI3gUHxIekwE6otym /yYLUZP7PIEy8O/bpGxW6LzHdWOK3fYHRItpDgBaA5X1AxvY2BO/XOfKySo1Db21+l9H//wtfYGiYOORGAUa1z2iOm5ELO3M+r0ktrNKBZRnxOzECsQsuEa/+1aidVgmCc r5OGJOHDz1NMK0yOvHorXY0IEp0E8UW2oOSovzMqnXNMMwnohZZA/WgMLkGJRbbRp9Qe/tz3PFPaGTc4c9uJpl1CN1n1v3n8ScqDkHNQ72m3NFqoEU0IBA6Z MCFRpB3PAx6VQgER3kQUB75gSOYlRe8OFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQjkOEJyuwk/x+rXId0ne1yi+dcSgih/kSGGEPn ISAxskQFCkrqpWfdTJRMD+7negc2tQRjAdpaFIUKJ3ZmXmCKxTaC1F6Ypjp3YJgAGYhkGRrDT7f7tmBmM3Ow5R/RSlhc8U4Q0Fy8Di3AuIKcZ+nXYkKRyHT1 OkxMuL8xtcwK52NpN6KGl1McXLIYi4k+HzXQmksHytorOvcqNT4YD+NUbyJyyeauJSvGYqPNvlvmsw05oIGDH5KOHUIey+9vGyP9DWqMfxM/i+Z8rZw9WUzh 9qvZukWUF/Kvhnlci82eegqCdG4MGbsflubxfArCfQ65jKl1B+H+h5HWyMslaPrntbQhi4sgM5tYYGqros0o0pzGZFCESgBxPPy/Pe/AorFJsKjzsDfsF/bSeAfJN8lv0S L8JrbukctqROb8gziqsrvHbz1esn4PYRWw3BfHICa8/fiHRQZ7q83b6piRBqYzU91yqG+1ytB7jBh7A7PjNuR7DMMIVdohKwKMjawkIQHxFj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\fotk_fr.lcd (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (12752), with no line terminators
Category:	dropped
Size (bytes):	12752
Entropy (8bit):	5.999182781405648
Encrypted:	false
SSDEEP:	384:b477Sr0GX7TA4Sx6RHk73hrtoueh5Fix0:b477SH/APE2hrto1h5B

MD5:	02D3A1C956563BA31087EE811BCF1F41
SHA1:	6BDDFE58549C328D810B15B37BF93BCFCAB1A14B
SHA-256:	E6DCD083958DB6FB9A3FB75A9ED320638C3CBF97B69AA24AAF68E96FB644F9F1
SHA-512:	A385C69D7CFD88F637D3553BEEFA502563E9620FBA1C502DBCB7CF868383F1CF86D6578FCCCE0EF6B5D0E246E1F94313FF6A3AC01B1529AC78DF5F376B76C3E2
Malicious:	false
Preview:	lcd&0001000000000004400002496000010176wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zShBKRDtypz8MHsvOxXIrTqaHwI3gUHxIekwE6otym/yebUZP7PlEy8O/bpGxW6LzHxWOK3fYHRItpDgBaA5X1A5vY2BO/XOfKySo1Db21+I93//wtfYGiYOORGAUa1z2ham5ELO3M+r0ktrNKBZRnx/zECsQsuEa/+1aidVgmCcs5OGJOHDz1NMK0yOvHorXYoIEp0E8UW2oOSovzMqnXNBMwnohZZA/WgMLkGJRbbRoNQe/tz3PFPaGTc4c9uJplVCN1n1v3n8ScqDkHNQ72mgNFqoEU0IBA6ZMCFRpB3PAx6VQgER3kQUB75gSOYlRcAOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQjIOEJyuwk/x+rXId0ne1yi9dcSgih/kSGGEPnISAxskRlCkrqpWfdTJRMD+7negc2JQRjAdpaFIUKJ3ZmXmCKw8aC1F6Ypjp3YJgAGYhkGR1TT7f7tmBmM3Ow5R/RSlhb4U4Q0Fy8Di3AuIKcZ+nXY3KRyHT1OkxMuL8xtcwK52RpN6KGl1McXLIYi4k+HzXTWksHytorOvcqNT4YD+NUbvJyyeauJSvGYqPNvlvmsw0ZoIGDH5KOHUley+9vGyP8vWqMfxM/i+Z8rZw9WUzh8QvZukWUF/Kvhnlci82eegqSdG4MGbsflubxfArCfQ64TKl1B+H+h5HWyMslaPrntVQhi4sgM5tYYGqros0o0py2ZFCESgBxPPy/Pe/AorFJoKjzsDfsF/bSeAfJN8lv0aL8JrbuktqROb8gziqsrtHbz1esn4PYRWw3BfHICa6PfiHRQZ7q83b6piRBqYzUh1yqG+1ytB7jBh7A7PjNuK7DMMlVdohKwKMjawkIQHw1j/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\fotk_ja.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (15400), with no line terminators
Category:	dropped
Size (bytes):	15400
Entropy (8bit):	5.998963228052221
Encrypted:	false
SSDEEP:	192:sT4SmJg9IPU7nKZ7FknvIyD4s892kYOPM/vUm7Z1pTD/fOa8n9td6XBgD9IEbHxO:+4SuPUmXknvb04kXoMmjpH/GtnOBShK
MD5:	7DD5A9A2ED2E595E660EAB7B06449720
SHA1:	992CAD591FB818A66DFEC96CC32B5B94739692FF
SHA-256:	168ED420AB4AC7C5468362EE5804A1EE1BC2304B3A61884ADF1D9E764E66F889
SHA-512:	2C335278E6E67FD26AF6DCFC50417CB70EA35BDB4ABA5185F023AEC6BA1948F096677B4A6DA3539B746CC79378F6DAB82F386995CD56F3BD9F977815B11FE69
Malicious:	false
Preview:	lcd&0001000000000004400002496000012824wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwI3gUHxIekwE6otym/yHbUZP7PlEy8O/bpGxW6LzHtWOK3fYHRItpDgBaA5X1AXvY2BO/XOfKySo1Db21+Ig3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxIzECsQsuEa/+1aidVgmCc0ZOGJOHDz1NMK0yOvHorXY0IEp0E8UW2oOSovzMqnXNGMwnohZZA/WgMLkGJRbbRrtQe/tz3PFPaGTc4c9uJpm1CN1n1v3n8ScqDkHNQ72mzNFqoEU0IBA6ZMCFRpB3PEx6VQgER3kQUB75gSOYlReMOFEygpaacvJBa+SPwRA0aZu9N3WqHCJ5vks/lgCGrn/fiTl/mokBWgEres7DjQh4OEJyuwk/x+rXId0ne1yihdcSgih/kSGGEPnISAxskQlCkrqpWfdTJRMD+7negcyFQRjAdpaFIUKJ3ZmXmCKwtaC1F6Ypjp3YJgAGYhkGRoDT7f7tmBmM3Ow5R/RSlhbAU4Q0Fy8Di3AuIKcZ+nXZwKRyHT1OkxMuL8xtcwK52OZN6KGl1McXLIYi4k+HzXfOksHytorOvcqNT4YD+NUaPJyyeauJSvGYqPNvlvmswnZoIGDH5KOHUley+9vGyP9vWqMfxM/i+Z8rZw9WUzh92vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMslaPrnszQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFOQKjzsDfsF/bSeAfJN8lv1rL8JrbuktqROb8gziqsr73bz1esn4PYRWw3BfHICa7HfiHRQZ7q83b6piRBqYzUR1yqG+1ytB7jBh7A7PjNuObDMMlVdohKwKMjawkIQHz1j/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\fotk_zh.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (10172), with no line terminators
Category:	dropped
Size (bytes):	10172
Entropy (8bit):	5.999002101128432
Encrypted:	false
SSDEEP:	192:HQzOr83z8zOvnbYPEe5MXjzo2LvLXuqQGgfPuVC9ZMCNVm:HQTz8zO086M42LvcPuVL+Vm
MD5:	03F4D28B17CE89CFE4C288EF7225451F
SHA1:	3470AD6103983DAABEE0D8494E891123BCA9804A
SHA-256:	7C7509711730827DA1A713398845A2E09ADDE8ECFCA07DB04B47F34EECE52493
SHA-512:	50EBDBA872C08D18C54AEBA31C025DE7203C0E1444CDA541857715BB186358C8D8C186F0419EDD9A5C02E03D98D44B95C0EDC4549CF725578CEBD667482A36
Malicious:	false
Preview:	lcd&0001000000000004400002496000007596wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwI3gUHxIekwE6otym/yTbUZP7PlEy8O/bpGxW6LzFxWOK3fYHRItpDgBaA5X1BavY2BO/XOfKySo1Db21+l/X//wtfYGiYOORGAUa1z2gum5ELO3M+r0ktrNKBZRnxxzECsQsuEa/+1aidVgmCcrZOGJOHDz1NMK0yOvHorXbslEp0E8UW2oOSovzMqnXN3MwnohZZA/WgMLkGJRbbRl9Qe/tz3PFPaGTc4c9uJpklCN1n1v3n8ScqDkHNQ72l+NFqoEU0IBA6ZMCFRpB3PcR6VQgER3kQUB75gSOYlRaQOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQiAOEJyuwk/x+rXId0ne1yihdcSgih/kSGGEPnISAxskTVCkrqpWfdTJRMD+7negc5lQRjAdpaFIUKJ3ZmXmCKwKaC1F6Ypjp3YJgAGYhkGRsTT7f7tmBmM3Ow5R/RSlhdYU4Q0Fy8Di3AuIKcZ+nXYxKRyHT1OkxMuL8xtcwK52LJN6KGl1McXLIYi4k+HzXUiksHytorOvcqNT4YD+NUbcJyyeauJSvGYqPNvlvmswz5oIGDH5KOHUley+9vGyP/rWqMfxM/i+Z8rZw9WUzh8MvZukWUF/Kvhnlci82eeglydG4MGbsflydKl65LKl1B+H+h5HWyMslaPrntWQhi4sgM5tYYGqros0o0p0mZFCESgBxPPy/Pe/AorFJAKjzsDfsF/bSeAfJN8lv0KL8JrbuktqROb8gziqsrpXbz1esn4PYRWw3BfHICa87fiHRQZ7q83b6piRBqYzU/1yqG+1ytB7jBh7A7PjNuRrDMMlVdohKwKMjawkIQHxNj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-50LB9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (12752), with no line terminators
Category:	dropped
Size (bytes):	12752

Entropy (8bit):	5.999182781405648
Encrypted:	false
SSDEEP:	384:b477Sr0GX7TA4Sx6RHk73hrtoueh5Fix0:b477SH/APE2hrto1h5B
MD5:	02D3A1C956563BA31087EE811BCF1F41
SHA1:	6BDDFE58549C328D810B15B37BF93BCFCAB1A14B
SHA-256:	E6DCD083958DB6FB9A3FB75A9ED320638C3CBF97B69AA24AAF68E96FB644F9F1
SHA-512:	A385C69D7CFD88F637D3553BEEFA502563E9620FBA1C502DBCB7CF868383F1CF86D6578FCCCE0EF6B5D0E246E1F94313FF6A3AC01B1529AC78DF5F376B76C3E2
Malicious:	false
Preview:	lcd&0001000000000044000024960001017 6wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zShBKRDtypz8MHsvOxXIrTqaHwI3gUHxlekwE6otym /yebUZP7PlEy8O/bpGxW6LzHxWOK3fYHRltpDgBaA5X1A5vY2BO/XOfKySo1Db21+l93//wtfYGiYOORGAUa1z2ham5ELO3M+r0ktrNKBZRnx/zECsQsuEa/+1aidVgmCcs5OGJOHDz1NMK0yOvHorXY0lEp0E8UW2oOSovzMqnXNBMwnohZZA/WgMLkGJRbbRoNQe/tz3PFPaGTc4c9uJplVCN1n1v3n8ScqDkHNQ72mgNFqoEU0IBA6Z MCFRpB3PAx6VQgER3kQUB75gSOYlRcAOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTI/mokBWgEres7DjQjlOEJyuwk/x+rXId0ne1yi9dcSgih/kSGGEPn ISAxskRlCkrqpWfdTJRMD+7negc2JQRjAdpaFIUKJ3ZmXmCKw8aC1F6Ypjp3YJgAGYhkGR1TT7f7tmBmM3Ow5R/RSlhb4U4Q0Fy8Di3AuIKcZ+nXY3KRyHT1 OkxMuL8xtcwK52RpN6KGl1McXLIYi4k+HzXTWksHytorOvcqNT4YD+NUbvJyyeauJSvGYqPNvlvmsw0ZoIGDH5KOHUIey+9vGyP8vWqMfxM/i+Z8rZw9WUzh 8QvZukWUF/Kvhnlci82eegqSdG4MGbsflubxfArCfQ64TKl1B+H+h5HWyMslaPrntVQhi4sgM5tYYGqros0o0py2ZFCESgBxPPy/Pe/AorFJoKjzsDfsF/bSeAfJN8lv0a L8JrbukctqROb8gziqsrtHbz1esn4PYRWw3BfHICa6PfiHRQZ7q83b6piRBqYzUh1yqG+1ytB7jBh7A7PjNuK7DMMIVdohKwKMjawkIQHw1j/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-B9C47.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (12648), with no line terminators
Category:	dropped
Size (bytes):	12648
Entropy (8bit):	5.997991870273226
Encrypted:	false
SSDEEP:	384:vH6NHxuYvSxaFjN43mKAIz03TuslDR6mZ/juc:yNRuYvSxaFJRIqTvlDR6mZ/I
MD5:	1FF1A88C097A10AF0D2CB463BBB5E4C9
SHA1:	D149B1D0BCD84FAD9A4BD143E7837999BC840141
SHA-256:	3E077B1A201D71636DD045F7B2694AFEE90881DF97704B012DC947C7429492A7
SHA-512:	82AA26F7E0D877A0BEA8D55C57D4D6B98DF283C04360C730E6ED385A589D16438F9BC00B80609B48C33028202661E7343DD4A13A53AE31B6C9A4D8C2E63D102
Malicious:	false
Preview:	lcd&0001000000000044000024960001007 2wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zRFBKRDtypz8MHsvOxXIrTq4HwI3gUHxlekwE6otym /yYLUZP7PlEy8O/bpGxW6LzHdWOK3fYHRltpDgBaA5X1AxvY2BO/XOfKySo1Db21+l9H//wtfYGiYOORGAUa1z2iOm5ELO3M+r0ktrNKBZRnxOzECsQsuEa/+1aidVgmCcr5OGJOHDz1NMK0yOvHorXY0lEp0E8UW2oOSovzMqnXNMMwnohZZA/WgMLkGJRbbRp9Qe/tz3PFPaGTc4c9uJpl1CN1n1v3n8ScqDkHNQ72m3NFqoEU0IBA6Z MCFRpB3PAx6VQgER3kQUB75gSOYlRe8OFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTI/mokBWgEres7DjQjkOEJyuwk/x+rXId0ne1yi+dcSgih/kSGGEPn ISAxskQFCkrqpWfdTJRMD+7negc2tQRjAdpaFIUKJ3ZmXmCKxTaC1F6Ypjp3YJgAGYhkGRrDT7f7tmBmM3Ow5R/RSlhb8U4Q0Fy8Di3AuIKcZ+nXYkKRyHT1 OkxMuL8xtcwK52NpN6KGl1McXLIYi4k+HzXQmksHytorOvcqNT4YD+NUbvJyyeauJSvGYqPNvlvmsw05oIGDH5KOHUIey+9vGyP9DWqMfxM/i+Z8rZw9WUzh 9qvZukWUF/Kvhnlci82eegqCdG4MGbsflubxfArCfQ65jKl1B+H+h5HWyMslaPrntbQhi4sgM5tYYGqros0o0pzGZFCESgBxPPy/Pe/AorFJsKjzsDfsF/bSeAfJN8lv0S L8JrbukctqROb8gziqsrvHbz1esn4PYRWw3BfHICa8/fiHRQZ7q83b6piRBqYzU91yqG+1ytB7jBh7A7PjNuR7DMMIVdohKwKMjawkIQHxFj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-BQIFQ.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (15400), with no line terminators
Category:	dropped
Size (bytes):	15400
Entropy (8bit):	5.998963228052221
Encrypted:	false
SSDEEP:	192:sT4SmJg9IPU7nKZ7FknvIyD4s892kYOPM/vUm7Z1pTD/fOa8n9td6XBgD9IEbHxO:+4SuPUmXknvb04kXoMmjpH/GtnOBShK
MD5:	7DD5A9A2ED2E595E660EAB7B06449720
SHA1:	992CAD591FB818A66DFEC96CC32B5B94739692FF
SHA-256:	168ED420AB4AC7C5468362EE5804A1EE1BC2304B3A61884ADF1D9E764E66F889
SHA-512:	2C335278E6E67FD26AF6DCFC50417CB70EA35BDB4ABA5185F023AEC6BA1948F096677B4A6DA3539B746CC79378F6DAB82F386995CD56F3BD9F977815B11FE69
Malicious:	false
Preview:	lcd&0001000000000044000024960001282 4wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwI3gUHxlekwE6otym /yHbUZP7PlEy8O/bpGxW6LzHtWOK3fYHRltpDgBaA5X1AXvY2BO/XOfKySo1Db21+lg3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxlzECsQsuEa/+1aidVgmCc 0ZOGJOHDz1NMK0yOvHorXY0lEp0E8UW2oOSovzMqnXNGMwnohZZA/WgMLkGJRbbRrtQe/tz3PFPaGTc4c9uJpm1CN1n1v3n8ScqDkHNQ72mzNFqoEU0IBA6Z MCFRpB3PEx6VQgER3kQUB75gSOYlREMOFEygpaacvJBa+SPwRA0aZu9N3WqHCJ5vks/lgCGrn/fiTI/mokBWgEres7DjQh4OEJyuwk/x+rXId0ne1yihdcSgih/kSGGEPn ISAxskQlCkrqpWfdTJRMD+7negcyFQRjAdpaFIUKJ3ZmXmCKwtaC1F6Ypjp3YJgAGYhkGRoDT7f7tmBmM3Ow5R/RSlhbAU4Q0Fy8Di3AuIKcZ+nXZwKRyHT1 OkxMuL8xtcwK52OZN6KGl1McXLIYi4k+HzXfOksHytorOvcqNT4YD+NUaPJyyeauJSvGYqPNvlvmswnZoIGDH5KOHUIey+9vGyP9vWqMfxM/i+Z8rZw9WUzh 92vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMslaPrnszQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFOQKjzsDfsF/bSeAfJN8lv1r L8JrbukctqROb8gziqsr73bz1esn4PYRWw3BfHICa7HfiHRQZ7q83b6piRBqYzUR1yqG+1ytB7jBh7A7PjNuObDMMIVdohKwKMjawkIQHz1j/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-H0NCM.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (10172), with no line terminators

Category:	dropped
Size (bytes):	10172
Entropy (8bit):	5.999002101128432
Encrypted:	false
SSDEEP:	192:HQzOr83z8zOvnbYPEe5MXjzo2LvLXuqQGgfPuVC9ZMCNVm:HQTz8zO086M42LvcPuVL+Vm
MD5:	03F4D28B17CE89CFE4C288EF7225451F
SHA1:	3470AD6103983DAABEE0D8494E891123BCA9804A
SHA-256:	7C7509711730827DA1A713398845A2E09ADDE8ECFCA07DB04B47F34EECE52493
SHA-512:	50EBDBA872C08D18C54AEBA31C025DE7203C0E1444CDA541857715BB186358C8D8C186F0419EDD9A5C02E03D98D44B95C0EDC4549CF725578CEBD667482A3 6
Malicious:	false
Preview:	lcd&0001000000000004400002496000075 96wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwI3gUHxIekwE6otym /yTbUZP7PIEy8O/bpGxW6LzFxWOK3fYHRItpDgBaA5X1BavY2BO/XOfKySo1Db21+l/X//wtfYGiYOORGAUa1z2gum5ELO3M+r0ktrNKBZRnxxzECsQsuEa/+1aidVgmCc rZOGJOHDz1NMK0yOvHorXbslEp0E8UW2oOSovzMqnXN3MwnohZZA/WgMLkGJRbbRl9Qe/tz3PFPaGTc4c9uJpkICN1n1v3n8ScqDkHNQ72l+NFqoEU0IBA6Z MCFRpB3PcR6VQgER3kQUB75gSOYlRaQOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQiAOEJyuwk/x+rXId0ne1yihdcSgih/kSGGEPn ISAxskTVCkrqpWfdTJRMD+7negc5lQRjAdpaFIUKJ3ZmXmCKwKaC1F6Ypjp3YJgAGYhkGRsTT7f7tmBmM3Ow5R/RSlhdYU4Q0Fy8Di3AuIKcZ+nXYxKRyHT1 OkxMuL8xtcwK52LJN6KGI1McXLIYi4k+HzXUiksHytorOvcqNT4YD+NUbcJyyeauJSvGYqPNvlvmswz5oIGDH5KOHUIey+9vGyP/rWqMfxM/i+Z8rZw9WUzh8MvZukWUF/ Kvhnlci82eeglydG4MGbsfIubxfArCfQ65LKl1B+H+h5HWyMsIaPrntWQhi4sgM5tYYGqros0o0p0mZFCESgBxPPy/Pe/AorFJAKjzsDfsF/bSeAfJN8lv0KL8Jrbukctq ROb8gziqsrpXbz1esn4PYRWw3BfHICa87fiHRQZ7q83b6piRBqYzU/1yqG+1ytB7jBh7A7PjNuRrDMMIVdohKwKMjawkIQHxNj/E9kwja6IUI7

C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (7568), with no line terminators
Category:	dropped
Size (bytes):	7568
Entropy (8bit):	5.994994247200588
Encrypted:	false
SSDEEP:	192:by7MRsGZtKD5PXgQn2aZgqi3ycNBiEd5vtgZ86VVV0Kq:uIRsgg5P12aiqI5v63GKq
MD5:	8C21D08BA2B447A7C85FA5575A3E57EE
SHA1:	A07E68F1613AD29A8274A07B6EC03B6266C06F15
SHA-256:	BB6DFD0A1F9FA1658FA75BDC117F601398D9D132453EE7A7D1B858AED29E42F9
SHA-512:	0AB5767C4EE3D0CFBA28174C8A3FB6BB9326E1BF66554AEFD4549C41FA096DEEFE76A6150DA3C577E6C99B40EFD3151C0A96D6460F3DD266F5928156D58CF5 6A
Malicious:	false
Preview:	lcd&0001000000000044000074880000000 0wfNamjzkzT1BNRD8ypz8XHsvOxLIrTqsHwI36UHxId8=wfNamzz0zTYLRniD6tiTVXsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3jLSxC9j+TIGikgTu62WV+0XP8o3YGiYOORGAV61z2kWm5Dev3M+r00trNKdZRnwrzECsQsuEa/ +1aiddgmCcgJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/Wg+HnC0aIboouUpqu3BBmbuIwclJduJpg1CN1n1v3n8ScqD5RdQ72kHNF qoEU0IBA6ZMCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjMXSfbnLk3B7snKKkIbZcVk0IKz0wk/x+rXId1re1yiwdcTV Fh/kSGCEPnIGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3CT5g0zm4vN8l1lk0/frX6DG4GYV+ nXYaKRyHT1OkxMuL826DwK52AJN6KGI1McXLIYi4iOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TkmPbHHsiH Svvul/ui9CoVh6uUA0F/KvhnlcIc2eegiSdGlTibsflvbxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKMKjzsDfsF/bR WwTYBRpsQNHvU/X98mg5B0X/hPiqsrj3bz1esn4PYRWw20oXICa+HfiHRQZ7q83b6piThqYzV41yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUI7

C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	80
Entropy (8bit):	4.142037796599528
Encrypted:	false
SSDEEP:	3:5VvXjyoyRd2tUquhItSjt/n:5k7KUquhItSt/n
MD5:	CA943A39A4F5DD13E54089690FEC080A
SHA1:	0DC95BE92BF165A841D1881BC2A14212C31F4792
SHA-256:	FDF6D2CBF65EDCF9E84B66D484BA0FD18FAD427E3EB1BF332C94CADDF1D7EC63
SHA-512:	EE0051B72252A61399E53288CD23EEE59CA4A7139E941A07B750281CFCB77BFD143453BF86F54C03CAD39CABECA7CEC2C5E4D1DC1B8A41E16FB174FA13196 FE
Malicious:	false
Preview:	lcd&0001000000000044000000000000000 0wfNamjzkzT1BNRD8ypz8XHsvOxzIrTqtHwI3gUHxIek=

C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (7248), with no line terminators
Category:	dropped
Size (bytes):	7248

Entropy (8bit):	5.997073501805218
Encrypted:	false
SSDEEP:	192:bfzTsUutE1urhpa053dRffUnm309gNCSBgEYpKn2qV/2:bfzTsVEwrTV3zHIUYJpjz
MD5:	30FE73410C791D4BF1D7A1FDCEA9E54A
SHA1:	ED3EB0A5F503D1B7F84D19592249E0E7409E31EB
SHA-256:	366C3AA0A8F734B055D685D1B4783C95B2E1830B7F25319B3577FFA3E66AA2B5
SHA-512:	DD76385E04704077E0972DB4BB58629538884A316F8B8EC5C75B7597B66D80A5C20C243A6BA70F67F4492C95BB86D04053E8F7D7DFD8CFF5BC803B286C52FF2
Malicious:	false
Preview:	lcd&0001000000000004400007168000000000wfNamjzkzT1BNRD8ypz8XHsvOxbIrTqsHwI3AUHxIcM=kbcczG69mWVBKRDtypz8MHsvOxTlrTqtHwI3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//lLmEWxmCc gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSXN+NJ+Jpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvNEetnG1FF49Zu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPn IGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3ekoep1HY1scU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHytorOvcuIXqM+qAUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUley+6PGyP+TWqMfxM/i+Z8rZw8qUzh 8hvZukWUF/Kvg3xovOkLf0vCdG4MGbsflubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPireXi14eFKMKjzsDfsF/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3lCa+DfiHRQZ7q83e76ymojM2FN1yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6lUl7

C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (720), with no line terminators
Category:	dropped
Size (bytes):	720
Entropy (8bit):	5.900569033555435
Encrypted:	false
SSDEEP:	12:4lHoMwA+gmo1buxC1iXXTpNsoUSFLuQPC+ZkGVg0J3DAiWNOcoJAAijBuDotI:/HoMwAyoMCkXXlWo1LE+2GK0Jal6
MD5:	55D02DA6997B22D40AC0BBD083D0D79E
SHA1:	5802069EBC18E6B83EF9974E1E88A5DC9AEF3F16
SHA-256:	323CA3057BBCD45288E40132953CD66B7F2AA1A403FA3D336F7E395FB51F94C3
SHA-512:	4B78F7B57FD666ADA151CFEF2ABAB34A09B5270BE7F7651AEF0AAA1263512C8B35DCB09B70481F010D10417F9D71D13B86A6A51DC77C0FDCA6D50BC5561D6 A5
Malicious:	false
Preview:	lcd&0001000000000044000006400000000wfNamjzkzT1BNRD8ypz8XHsvOxPIrTqsHwI3+UHxIe0=pZZamzz0zTdBKRDtypz8MB1AT3+XyV+tHwI3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1Dc6W+U/1LP9frqI3l/DCuxZZdD6h+m5ELO3M+r0ktrNKdZRnwrqjKsQsuEa/+1aiddgmCc gPXpUlqcqSFMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n3jUnNfeezp1Ni1j01BmCaIXc4NFSZ MCFfpB3PSh6VQgER3kQUfdZgR+YlRZgOFEygpaacvPY1jVivPmUJZu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPn IEMSsVYX2UlodmS4D4cvrOy02QQ6VQRjAdpaFIUKJ3ZnPmCKwRAkxF6Ypjp3YJgAGPhkGRllKUC9A5bAI3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHyvkIOeRI5j2LHOAxL2ERavWdhijDwqPNv4vmsw6JoIGDH5KOHU

C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (1104), with no line terminators
Category:	dropped
Size (bytes):	1104
Entropy (8bit):	5.9577061260906765
Encrypted:	false
SSDEEP:	24:q7VsiyT/NCkWaPIHxby827qIIU7gXcwl9ji5JMvX:uwjNFIRmPVU8qO/
MD5:	DE68D51F9BFED85374972FC4B778C7FE
SHA1:	70CF0EB0A85E503F56D91404E3C25D140FA462F4
SHA-256:	3115D9807B7F4558FA79D09F3DDEBCFD41AF2FA4761B006F108F9817165F0665
SHA-512:	37FE62C56CDC889B321C650D87554715113710E081BAE7B35F7C8D52DEF73A7C3E28FDDACD3BBF48270BCBFAEA27DFDA49E0D5E6DEC1A9EF9E8A1B88085E F53A
Malicious:	false
Preview:	lcd&0001000000000004400001024000000000wfNamjzkzT1BNRD8ypz8XHsvOxXlrTqsHwI34UHxIeE=wfNamnCHuURBKRDthvWPRAgvOxTlrTqtHwI3gUHxIekwE6ovym /yVrUZP7ODfFtlsckytW6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfK2VR1Da20mlyn//wjnYGiYOORGAUOEdvTam5ELOkK7FtT4KU8IqRnwrzECsQsuEa/+1aiddgmCc gJOGJOGloCcnZyLpxnorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WkLzkGLRbvRkdQe/gv3PFPaGTc4d5jnwH5CN1n1/BaSL6Pk5QwxmwBrWimoEU0IBA6Z MCFfpB3PSh6VQgF3sTB/RNAGNOYIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ9oTM/9gCirhvfiTF3mokBWgEreo+CHMAMOEJyukj2YlMGtBR6svl7VB7eg ih/kSGGEPnIGAxskVVCkrqowEqCiALKN+3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3cOZAGLhleRljT7f2dmBmM3Ow5R5kT46oAU4Q0Fm7KLsn/tW48R 7wJpKRyHT1OkxMuL8xtGwK52AZN6KGJTXrGgcfrLiOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGct3NvzvmAw75oIGOv5KOHUley+7KPWU4jWqMfxYZ3U Aqmtpq7QonNSvZukWUF/Kvhnlcic2eegiSdG4MH93oZFPXOzjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYcBdLoD0oAp62ZFCI+gBxPPy/Pe3UREfc0KjzsDMK42A0 3lH8IV+ZNTL8JrbukctqROb8gViqsrj3bz1etBj4J6FWSyW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB7nGWbAUPjFuerDMMFZdohKwKMja7gBlbCZj/E9kgFfUTywf

C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd (copy)

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (2640), with no line terminators
Category:	dropped

Size (bytes):	2640
Entropy (8bit):	5.987942858685715
Encrypted:	false
SSDEEP:	48:jDSdbGs0gEvopAOW+ChoamiiaAlptDCHdWdy5jqbx3saHOHz8:Sd10PAXnCuamiivAHkdaqb298
MD5:	7F9D763543F94CA15B7158ADA872C7E4
SHA1:	9661F3C85A6E583EB455E50488530D40B5FD6C56
SHA-256:	6E3C654DA94BF2DAB61704FA4787747DA578DF0EA8A7B808A7943E1D506FB373
SHA-512:	0F2ACD1B623362B15C1D634B6E18E14452EAE3BA6F984EEEF2496094EBB258B62EDA2CE607FC99F571EEF54E92507650BB83BA2EBBEAAC223D2346D343DEA871
Malicious:	false
Preview:	lcd&0001000000000004400002560000000000wfNamjzkzT1BNRD8ypz8XHsvOxHlrTqsHwl3AUHxIeY=hIsq91OGqEVBKRDtypz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItvWYdchWLTUFk+j5XvXOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//6H1Mx7Q/3 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPadkJME7TmzSMnTzz1v3n8ScqDkH5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvNE5i1ySJXkpNIosuQ/1CJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXId1re1yiwdcSgih/kSGHFXQ BpUX8XZ37B1s9WfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3em0jinbp8fIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHytorOvcuIwk/OcVDLpQlT7auJSvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh 8hvZukWUF/Kvgm9rrzu4bUqWU0j6r+w/lubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPqpCst2hZe8hv/RVmBqR/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3lCa+DfiHRQZ7q83f/K+1clAkFYlln1ki/ZZta1h7ASPjNuaLDMMIVdohKwKMja6ElQH1Rj/E9kwja6lUl7

C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (2960), with no line terminators
Category:	dropped
Size (bytes):	2960
Entropy (8bit):	5.986739218510661
Encrypted:	false
SSDEEP:	48:3jiESWGhYjEvKaAZ/m7g5Tk0oqmiia4k7qYebCuFbx3JnFpOHdxK/xB:3WYQyPukGNqmii27qYsFbAK/xB
MD5:	DD46349E256F66DA49E6ED04DAD039DE
SHA1:	32929544444286C63FA674F56BD19171EB851AAB
SHA-256:	D658B0AA15C2E36AD2C4C08BCED8693E525387822A1604DAA26D81BBFB6DF6B1
SHA-512:	29E9BDCBE21D95DF93FABAF280B90C7FF860B64D692F2492ED642479C0306118F2032EDB6E7FA216687EFB963E71C4F691BAA301060BAE838916047B2AE782EF
Malicious:	false
Preview:	lcd&0001000000000044000028800000000wfNamjzkzT1BNRD8ypz8XHsvOxfIrTqsHwl3yUHxIfc=wfNamzz0zTlHYFyo8Jz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKje5hGajxDqhyz/wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa/+1aiddgmCc gJOGJOHDz1NMK0yOtXorXaNjQs8x8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBAjO eW8Z5UXPSh6VQgER3kQUB75gR+YlRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQm1Kde/FtiCB+rXId1re1yiwdcSgih/kSGGEPn IGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3BazkDIzxWRljT7f7tmBmM3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtG wK52AZN6KGl1McXLIYi4iOHzXW/i/D3+6uPuluYB08ysfAiTYn7OJbAGvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh8hvZukWUF/KvM30Y6xga TI6EkhhcGbsfIubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKBfy3gDfsF/bSeAfLZ8lv0gL8JrbukctqROb8gViqsr j3bz1esn4PYRWw3BW3lCa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB72H1+AhBDNuaLDMMIVdohKwKMja6ElQH1Rj/E9kwja6lUl7

C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (424), with no line terminators
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.806054763135282
Encrypted:	false
SSDEEP:	6:5uRL07KUqCkuYOH6jZPTxDtoIbL6zn9qjAWQbiyT8/KjXPlvNsKOioDUX0bOWxTh:wWIdo6lPTvnFTx/KTpNsoR0yWx5LT
MD5:	BABA88923DACAC1B9FFCCD1CAA783903
SHA1:	BD9C1D4176B709671310EB31C197E54311DF2E09
SHA-256:	06793859377ADE0F42F713178559A3189B9118884CC9D783E98C36820BEAB899
SHA-512:	C834660D40616847458D21287692BB809101653EE8A29EB24AAC7D7AC6D9967BD78866081216848E073D50ED2E30EF4219CC13BB494A5F6C0201B27CEA5D0ED
Malicious:	false
Preview:	lcd&0001000000000044000003440000000wfNamjzkzT1BNRD8ypz8XHsvOxDIrTqsHwl3AUHxIes=kbccyFKVplJvaECkypz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItsCkQ/dXPjsSvY2BO/XOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//EAxVz4xD1 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSH5sOoTY02Q2UhCYzxaPlKTkon5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvA==

C:\ProgramData\FileOpen\Updates\Lists\is-9F2R0.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (1104), with no line terminators
Category:	dropped
Size (bytes):	1104

Entropy (8bit):	5.9577061260906765
Encrypted:	false
SSDEEP:	24:q7VsiyT/NCkWaPIHxby827qIlU7gXcwl9ji5JMvX:uwjNFIRmPVU8qO/
MD5:	DE68D51F9BFED85374972FC4B778C7FE
SHA1:	70CF0EB0A85E503F56D91404E3C25D140FA462F4
SHA-256:	3115D9807B7F4558FA79D09F3DDEBCFD41AF2FA4761B006F108F9817165F0665
SHA-512:	37FE62C56CDC889B321C650D87554715113710E081BAE7B35F7C8D52DEF73A7C3E28FDDACD3BBF48270BCBFAEA27DFDA49E0D5E6DEC1A9EF9E8A1B88085EF53A
Malicious:	false
Preview:	lcd&0001000000000004400001024000000000wfNamjzkzT1BNRD8ypz8XHsvOxXIrTqsHwl34UHxIeE=wfNamnCHuURBKRDthvWPRAgvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7ODfFtlsckytW6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfK2VR1Da20mlyn//wjnYGiYOORGAUOEdvTam5ELOkK7FtT4KU8IqRnwrzECsQsuEa/+1aiddgmCc gJOGJOGloCcnZyLpxnorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WkLzkGLRbvRkdQe/gv3PFPaGTc4d5jnwH5CN1n1/BaSL6Pk5QwxmwBrWimoEU0IBA6Z MCFfpB3PSh6VQgF3sTB/RNAGNOYIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ9oTM/9gCirhvfiTF3mokBWgEreo+CHMAMOEJyukj2YlMGtBR6svl7VB7eg ih/kSGGEPnIGAxskVVCkrqowEqCiALKN+3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3cOZAGLhleRljT7f2dmBmM3Ow5R5kT46oAU4Q0Fm7KLsn/tW48R 7wJpKRyHT1OkxMuL8xtGwK52AZN6KGJTXrGgcfrLiOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGct3NvzvmAw75oIGOv5KOHUley+7KPWU4jWqMfxYZ3U Aqmtpq7QonNSvZukWUF/KvhnIcic2eegiSdG4MH93oZFPXOzjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYcBdLoD0oAp62ZFCl+gBxPPy/Pe3UREfc0KjzsDMK42A0 3lH8IV+ZNTL8JrbukctqROb8gViqsrj3bz1etBj4J6FWSyW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB7nGWbAUPjFuerDMMFZdohKwKMja7gBlbCZj/E9kgFfUTywf

C:\ProgramData\FileOpen\Updates\Lists\is-CKRT4.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (424), with no line terminators
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.806054763135282
Encrypted:	false
SSDEEP:	6:5uRL07KUqCkuYOH6jZPTxDtoIbL6zn9qjAWQbiyT8/KjXPlvNsKOioDUX0bOWxTh:wWIdo6lPTvnFTx/KTpNsoR0yWx5LT
MD5:	BABA88923DACAC1B9FFCCD1CAA783903
SHA1:	BD9C1D4176B709671310EB31C197E54311DF2E09
SHA-256:	06793859377ADE0F42F713178559A3189B9118884CC9D783E98C36820BEAB899
SHA-512:	C834660D40616847458D21287692BB809101653EE8A29EB24AAC7D7AC6D9967BD78866081216848E073D50ED2E30EF4219CC13BB494A5F6C0201B27CEA5D0ED
Malicious:	false
Preview:	lcd&0001000000000044000003440000000wfNamjzkzT1BNRD8ypz8XHsvOxDIrTqsHwl3AUHxIes=kbccyFKVplJvaECkypz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItsCkQ/dXPjsSvY2BO/XOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//EAxVz4xD1 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSH5sOoTY02Q2UhCYzxaPIKTkon5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvA==

C:\ProgramData\FileOpen\Updates\Lists\is-DNLJ4.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (2640), with no line terminators
Category:	dropped
Size (bytes):	2640
Entropy (8bit):	5.987942858685715
Encrypted:	false
SSDEEP:	48:jDSdbGs0gEvopAOW+ChoamiiaAlptDCHdWdy5jqbx3saHOHz8:Sd10PAXnCuamiivAHkdaqb298
MD5:	7F9D763543F94CA15B7158ADA872C7E4
SHA1:	9661F3C85A6E583EB455E50488530D40B5FD6C56
SHA-256:	6E3C654DA94BF2DAB61704FA4787747DA578DF0EA8A7B808A7943E1D506FB373
SHA-512:	0F2ACD1B623362B15C1D634B6E18E14452EAE3BA6F984EEEF2496094EBB258B62EDA2CE607FC99F571EEF54E92507650BB83BA2EBBEAAC223D2346D343DEA871
Malicious:	false
Preview:	lcd&0001000000000044000025600000000wfNamjzkzT1BNRD8ypz8XHsvOxHIrTqsHwl3AUHxIeY=hIsq91OGqEVBKRDtypz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItvWYdchWLTUFk+j5XvXOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//6H1Mx7Q/3 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPadkJME7TmzSMnTzz1v3n8ScqDkH5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvNE5i1ySJXkpNIosuQ/1CJ5vks/0gCGrjPfiTI/mokBWgEreobDjQmoOEJyuwk/x+rXId1re1yiwdcSgih/kSGHFXQ BpUX8XZ37B1s9WfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3em0jinbp8fIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHytorOvcuIwk/OcVDLpQIT7auJSvGYqPNv4vmsw6JoIGDH5KOHUley+6PGyP+TWqMfxM/i+Z8rZw8qUzh 8hvZukWUF/Kvgm9rrzu4bUqWU0j6r+w/IubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPqpCst2hZe8hv/RVmBqR/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3lCa+DfiHRQZ7q83f/K+1cIAkFYlln1ki/ZZta1h7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6lUl7

C:\ProgramData\FileOpen\Updates\Lists\is-KNQ1D.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (720), with no line terminators
Category:	dropped
Size (bytes):	720
Entropy (8bit):	5.900569033555435

Encrypted:	false
SSDEEP:	12:4IHoMwA+gmo1buxC1iXXTpNsoUSFLuQPC+ZkGVg0J3DAiWNOcoJAAijBuDotI:/HoMwAyoMCkXXlWo1LE+2GK0Jal6
MD5:	55D02DA6997B22D40AC0BBD083D0D79E
SHA1:	5802069EBC18E6B83EF9974E1E88A5DC9AEF3F16
SHA-256:	323CA3057BBCD45288E40132953CD66B7F2AA1A403FA3D336F7E395FB51F94C3
SHA-512:	4B78F7B57FD666ADA151CFEF2ABAB34A09B5270BE7F7651AEF0AAA1263512C8B35DCB09B70481F010D10417F9D71D13B86A6A51DC77C0FDCA6D50BC5561D65A5
Malicious:	false
Preview:	lcd&0001000000000044000006400000000wfNamjzkzT1BNRD8ypz8XHsvOxPIrTqsHwI3+UHxIe0=pZZamzz0zTdBKRDtypz8MB1AT3+XyV+tHwI3gUHxIekwE6ovym/yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1Dc6W+U/1LP9frqI3I/DCuxZZdD6h+m5ELO3M+r0ktrNKdZRnwrqjKsQsuEa/+1aiddgmCcgPXpUlqcqSFMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n3jUnNfeezp1Ni1j01BmCaIXc4NFSZMCFfpB3PSh6VQgER3kQUfdZgR+YIRZgOFEygpaacvPY1jVivPmUJZu9N3WqHCJ5vks/0gCGrjPfiTI/mokBWgEreobDjQmoOEJyuwk/x+rXId1re1yiwdcSgih/kSGGEPnIEMSsVYX2UlodmS4D4cvrOy02QQ6VQRjAdpaFIUKJ3ZnPmCKwRAkxF6Ypjp3YJgAGPhkGRllKUC9A5bAl3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHyvkIOeRI5j2LHOAxL2ERavWdhijDwqPNv4vmsw6JoIGDH5KOHU

C:\ProgramData\FileOpen\Updates\Lists\is-L7T53.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (2960), with no line terminators
Category:	dropped
Size (bytes):	2960
Entropy (8bit):	5.986739218510661
Encrypted:	false
SSDEEP:	48:3jiESWGhYjEvKaAZ/m7g5Tk0oqmiia4k7qYebCuFbx3JnFpOHdxK/xB:3WYQyPukGNqmii27qYsFbAK/xB
MD5:	DD46349E256F66DA49E6ED04DAD039DE
SHA1:	32929544444286C63FA674F56BD19171EB851AAB
SHA-256:	D658B0AA15C2E36AD2C4C08BCED8693E525387822A1604DAA26D81BBFB6DF6B1
SHA-512:	29E9BDCBE21D95DF93FABAF280B90C7FF860B64D692F2492ED642479C0306118F2032EDB6E7FA216687EFB963E71C4F691BAA301060BAE838916047B2AE782EF
Malicious:	false
Preview:	lcd&0001000000000044000028800000000wfNamjzkzT1BNRD8ypz8XHsvOxfIrTqsHwI3yUHxIfc=wfNamzz0zTIHYFyo8Jz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym/yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKje5hGajxDqhyz/wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa/+1aiddgmCcgJOGJOHDz1NMK0yOtXorXaNjQs8x8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBAjOeW8Z5UXPSh6VQgER3kQUB75gR+YIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjPfiTI/mokBWgEreobDjQm1Kde/FtiCB+rXId1re1yiwdcSgih/kSGGEPnIGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3BazkDIzxWRIjT7f7tmBmM3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXW/i/D3+6uPuIuYB08ysfAiTYn7OJbAGvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh8hvZukWUF/KvM30Y6xgaTI6EkhhcGbsfIubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKBfy3gDfsF/bSeAfLZ8lv0gL8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB72H1+AhBDNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\Lists\is-O4NSE.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (7568), with no line terminators
Category:	dropped
Size (bytes):	7568
Entropy (8bit):	5.994994247200588
Encrypted:	false
SSDEEP:	192:by7MRsGZtKD5PXgQn2aZgqi3ycNBiEd5vtgZ86VVV0Kq:uIRsgg5P12aiqI5v63GKq
MD5:	8C21D08BA2B447A7C85FA5575A3E57EE
SHA1:	A07E68F1613AD29A8274A07B6EC03B6266C06F15
SHA-256:	BB6DFD0A1F9FA1658FA75BDC117F601398D9D132453EE7A7D1B858AED29E42F9
SHA-512:	0AB5767C4EE3D0CFBA28174C8A3FB6BB9326E1BF66554AEFD4549C41FA096DEEFE76A6150DA3C577E6C99B40EFD3151C0A96D6460F3DD266F5928156D58CF56A
Malicious:	false
Preview:	lcd&0001000000000044000074880000000wfNamjzkzT1BNRD8ypz8XHsvOxLIrTqsHwI36UHxId8=wfNamzz0zTYLRniD6tiTVXsvOxTIrTqtHwI3gUHxIekwE6ovym/yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3jLSxC9j+TIGikgTu62WV+0XP8o3YGiYOORGAV61z2kWm5Dev3M+r00trNKdZRnwrzECsQsuEa/+1aiddgmCcgJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/Wg+HnC0aIboouUpqu3BBmbuIwclJduJpg1CN1n1v3n8ScqD5RdQ72kHNFqoEU0IBA6ZMCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjMXSfbnLk3B7snKKkIbZcVk0IKz0wk/x+rXId1re1yiwdcTVFh/kSGCEPnIGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3CT5g0zm4vN8l1lk0/frX6DG4GYV+nXYaKRyHT1OkxMuL826DwK52AJN6KGl1McXLIYi4iOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TkmPbHHsiHSvvul/ui9CoVh6uUA0F/KvhnlcIc2eegiSdGlTibsfIvbxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKMKjzsDfsF/bRWwTYBRpsQNHvU/X98mg5B0X/hPiqsrj3bz1esn4PYRWw20oXICa+HfiHRQZ7q83b6piThqYzV41yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\Lists\is-OQA7C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	80

Entropy (8bit):	4.142037796599528
Encrypted:	false
SSDEEP:	3:5VvXjyoyRd2tUquhItSjt/n:5k7KUquhItSt/n
MD5:	CA943A39A4F5DD13E54089690FEC080A
SHA1:	0DC95BE92BF165A841D1881BC2A14212C31F4792
SHA-256:	FDF6D2CBF65EDCF9E84B66D484BA0FD18FAD427E3EB1BF332C94CADDF1D7EC63
SHA-512:	EE0051B72252A61399E53288CD23EEE59CA4A7139E941A07B750281CFCB77BFD143453BF86F54C03CAD39CABECA7CEC2C5E4D1DC1B8A41E16FB174FA13196FE
Malicious:	false
Preview:	lcd&0001000000000004400000000000000000wfNamjzkzT1BNRD8ypz8XHsvOxzIrTqtHwl3gUHxIek=

C:\ProgramData\FileOpen\Updates\Lists\is-THTBB.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with very long lines (7248), with no line terminators
Category:	dropped
Size (bytes):	7248
Entropy (8bit):	5.997073501805218
Encrypted:	false
SSDEEP:	192:bfzTsUutE1urhpa053dRffUnm309gNCSBgEYpKn2qV/2:bfzTsVEwrTV3zHIUYJpjz
MD5:	30FE73410C791D4BF1D7A1FDCEA9E54A
SHA1:	ED3EB0A5F503D1B7F84D19592249E0E7409E31EB
SHA-256:	366C3AA0A8F734B055D685D1B4783C95B2E1830B7F25319B3577FFA3E66AA2B5
SHA-512:	DD76385E04704077E0972DB4BB58629538884A316F8B8EC5C75B7597B66D80A5C20C243A6BA70F67F4492C95BB86D04053E8F7D7DFD8CFF5BC803B286C52FF2
Malicious:	false
Preview:	lcd&0001000000000004400007168000000000wfNamjzkzT1BNRD8ypz8XHsvOxbIrTqsHwl3AUHxIcM=kbcczG69mWVBKRDtypz8MHsvOxTIrTqtHwl3gUHxIekwE6ovym/yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//lLmEWxmCcgJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSXN+NJ+Jpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBA6ZMCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvNEetnG1FF49Zu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPnIGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3ekoep1HY1scU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHytorOvcuIXqM+qAUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUley+6PGyP+TWqMfxM/i+Z8rZw8qUzh8hvZukWUF/Kvg3xovOkLf0vCdG4MGbsfIubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPireXi14eFKMKjzsDfsF/bSeAfLZ8Iv0gL8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83e76ymojM2FN1yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035004, file counter 22, database pages 16, 1st free page 12, free pages 2, cookie 0x5, schema 4, UTF-8, version-valid-for 22
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.151918324786366
Encrypted:	false
SSDEEP:	384:vedThotEL38KXlOmrhSZsLRGlMapvC+8ZsLTT1SwIvV:JK+ZsL7ZsLP1iV
MD5:	D058D6CD99A7455EEBBF633D891E4B5E
SHA1:	70F65A4153CE5926CA34B09AFCAE78046F7925DE
SHA-256:	9F762476756F2A65B023D16D651F6BC63ACF9C59D19A86EF70A19D2702545A0C
SHA-512:	31C9FCED9D45CF69D376A00578B5B1B6D2D05A7C2E2A6B65F18EE761BA5AAA7B81B8901E134DA1644F86726CDEC2F6C8BFA711A684D873CC4DF114BC75D99CC
Malicious:	false
Preview:	SQLite format 3.....@ .....O|.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.2041765369956123
Encrypted:	false
SSDEEP:	48:7MWECioIVaioldol1Nol1Aiol1RROiol1+EMol1C0f5ol15iolBxqumFTIF3XmHd:7F9paSMm0SjG9IVXEBodRBkD
MD5:	D2B7CE307691325B4E04CF50EEAD8E30
SHA1:	3FD1DB1CC08735BF7D7387426266B34F0573CEA4

SHA-256:	3E45607EED54B74890CC34DA0B7C58CD3D983BA4489523E1BC1A53C6F6CC1FD9
SHA-512:	D73A637025FEFAF0D8EF27FD52509BFDE0F55A3194328D9F6C13A0D9FD248D5DAB3F2C65D08DA76C2A4D8819003A5B030FD5A8E6D09266CE2224472F9E5454 4
Malicious:	false
Preview:	.... .c.....Z\.E..... .....X.... ./.y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt22.lst.1460

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	110694
Entropy (8bit):	5.190261286653695
Encrypted:	false
SSDEEP:	1536:JgN4DipADWp1ttawvayjLgs1RY4V9gMRpF6j37cNp3yrjDlro/qu9rp:WaDls1RY4V9gMRpF6j37cNp3yrjA
MD5:	F94C322499A42D2F2D40561BB14B8397
SHA1:	526645D16C28BF57406A8B96AB27A97C8AFD21F6
SHA-256:	A3A862B90DE7C071196DD65C81C6E6DAAB486537FF4CABF5003D2411B2CE9B42
SHA-512:	1E31084AC3D1484E88970026FF7BAD1F6C4E5CC5B09A53B20A49833878A0A983E1E7778CE8B74C2CAC24F1F77DBA372771D761A7D06C031C504596BF17A29E3 A
Malicious:	false
Preview:	%!Adobe-FontList 1.22.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Ar ial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.hasSVG:no.VariableFontType:NonVariableFont.WinName:Arial. FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType .FontName:Arial-Black.FamilyName:Arial.StyleName:Black.MenuName:Arial Black.StyleBits:0.WeightClass:900.WidthClass:5.AngleClass:0.FullName:Arial Black .WritingScript:Roman.hasSVG:no.VariableFontType:NonVariableFont.WinName:Arial Black.FileLength:167592.NameArray:0,Win,1,Arial Black.NameArray:0,Mac,4,Arial Black.NameArray:0,Win,1,Arial Black.NameArray:0,Win,16,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.F amilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	110694
Entropy (8bit):	5.190261286653695
Encrypted:	false
SSDEEP:	1536:JgN4DipADWp1ttawvayjLgs1RY4V9gMRpF6j37cNp3yrjDlro/qu9rp:WaDls1RY4V9gMRpF6j37cNp3yrjA
MD5:	F94C322499A42D2F2D40561BB14B8397
SHA1:	526645D16C28BF57406A8B96AB27A97C8AFD21F6
SHA-256:	A3A862B90DE7C071196DD65C81C6E6DAAB486537FF4CABF5003D2411B2CE9B42
SHA-512:	1E31084AC3D1484E88970026FF7BAD1F6C4E5CC5B09A53B20A49833878A0A983E1E7778CE8B74C2CAC24F1F77DBA372771D761A7D06C031C504596BF17A29E3 A
Malicious:	false
Preview:	%!Adobe-FontList 1.22.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Ar ial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.hasSVG:no.VariableFontType:NonVariableFont.WinName:Arial. FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType .FontName:Arial-Black.FamilyName:Arial.StyleName:Black.MenuName:Arial Black.StyleBits:0.WeightClass:900.WidthClass:5.AngleClass:0.FullName:Arial Black .WritingScript:Roman.hasSVG:no.VariableFontType:NonVariableFont.WinName:Arial Black.FileLength:167592.NameArray:0,Win,1,Arial Black.NameArray:0,Mac,4,Arial Black.NameArray:0,Win,1,Arial Black.NameArray:0,Win,16,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.F amilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:e:e
MD5:	DC84B0D741E5BEAE8070013ADDCC8C28
SHA1:	802F4A6A20CBF157AAF6C4E07E4301578D5936A2
SHA-256:	81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06

SHA-512:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB1
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	945
Entropy (8bit):	5.084822438547672
Encrypted:	false
SSDEEP:	24:YFubaRCzi56W9fg56Uxvj56R2clx2LSC56+Xma560OG:YgY8i56W9o56+56RdxY56+Xma56w
MD5:	9B25B5445ECA39016DC30DE44FD9539A
SHA1:	520C63BEBDC323CC349C6DAA1C8EA30886A18DE3
SHA-256:	DB65364D109DCB21B7A0E8B8C3889BAD6AFAFAA63D2A85871FF5081AAD3611D1
SHA-512:	17751C25AFBF562BE4BD4E57E0B27BF5CBFD6ABA95B3DCD807F9AF25E75EA560839F1BCDBB053FAC73FAD32581E7D4CFBE8FFA7D9C1AAEE2BC619AFE01D37E4C
Malicious:	false
Preview:	{"all":[{"id":"TESTING","info":{"dg":"DG","sid":"TESTING"},"mimeType":"file","size":4,"ts":1675795219000},{"id":"Edit_InApp_Aug2020","info":{"dg":"2646f0f0f5dd62f2d56ca1c033033c58","sid":"Edit_InApp_Aug2020"},"mimeType":"file","size":782,"ts":1642668697000},{"id":"DC_Reader_RHP_Banner","info":{"dg":"6b5098d964b65c5397b668715cc670a2","sid":"DC_Reader_RHP_Banner"},"mimeType":"file","size":1393,"ts":1642668697000},{"id":"DC_Reader_Upsell_Cards","info":{"dg":"0e188ce3b10d082e729bd3a233cfaf51","sid":"DC_Reader_Upsell_Cards"},"mimeType":"file","size":286,"ts":1642668697000},{"id":"DC_FirstMile_Right_Sec_Surface","info":{"dg":"74af15052665af89ad7102a0cb63a33a","sid":"DC_FirstMile_Right_Sec_Surface"},"mimeType":"file","size":294,"ts":1642668697000},{"id":"DC_Reader_RHP_Retention","info":{"dg":"38b4eab1fcf9ab6a31440a452fcbde2b","sid":"DC_Reader_RHP_Retention"},"mimeType":"file","size":287,"ts":1642668697000}],"g_info":{"Version":"0.0.0.1"}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	40393
Entropy (8bit):	5.517981962339109
Encrypted:	false
SSDEEP:	384:K7X4oyVFMqnBkPa2wy+QZ0KEJrgL1KsYNg7y:KT4oyVFMQBoaLy+QZ0KEJ6Yyu
MD5:	E8E7E38218B5033FEEF933576AD02510
SHA1:	38BF9C8E07B2164CA4547D1AC742E503A0D3410C
SHA-256:	CA3F67BA69A8BA7848B5D832709B04C180655E7FEE7A7B566B32B5AA1C5CC4C8
SHA-512:	896BC5A6E217D7B2A896F465D5CDF21CF5A7DF96B9389E2BF70D3AD0C5F36C9B45E4A1F32D571349E4C7E9C2B881FD934A1C449C7108621D36D9981A6C8409E
Malicious:	false
Preview:	4.241.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-BoldItalicMT.P:Arial Bold Italic.L:$....."F:Arial.#.91.FID.2:o:.....:F:Arial-Black.P:Arial Black.L:-....."F:Arial Black.#.103.FID.2:o:.....:F:Bahnschrift.P:Bahnschrift Light.L:&.....,.....,....."F:Bahnschrift Light.#.

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

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	21453
Entropy (8bit):	5.12277210742906
Encrypted:	false
SSDEEP:	384:hwZpMJvlfGLekAD6BFxie6vjphYjSYfJ00c:h+8mjlfJ00c
MD5:	74BEFA61F838AD6178FD091F41640A01
SHA1:	4F01B78C105F010882965AA1703DE7364BFD4785
SHA-256:	1A4F9AE259E6008493B0C11CC8E9C22D856A95337213382FEA2B5ACFBD1A7737
SHA-512:	600D99672AB1B074A590A31A7BD547F79EF1894FBB377DEDBDA2702586AFE8B509D962133DF40910A261B73B7A31C227BA512FBD13AACE3B1BE4707738463E89
Malicious:	false

Preview:	.2023-02-07 18:39:47.989 Log opened. (Time zone: UTC+00:00)..2023-02-07 18:39:47.989 Setup version: Inno Setup version 6.0.4 (u)..2023-02-07 18:39:47.989 Original Setup EXE: C:\Users\user\Desktop\FileOpenInstaller.exe..2023-02-07 18:39:47.989 Setup command line: /SL5="$6040A,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" ..2023-02-07 18:39:47.989 Windows version: 10.0.19042 (NT platform: Yes)..2023-02-07 18:39:47.989 64-bit Windows: Yes..2023-02-07 18:39:47.989 Processor architecture: x64..2023-02-07 18:39:47.989 User privileges: Administrative..2023-02-07 18:39:48.333 Administrative install mode: Yes..2023-02-07 18:39:48.333 Install mode root key: HKEY_LOCAL_MACHINE..2023-02-07 18:39:48.333 64-bit install mode: Yes..2023-02-07 18:39:48.333 Created temporary directory: C:\Users\user\AppData\Local\Temp\is-K56MV.tmp..2023-02-07 18:39:48.380 -- DLL function import --..2023-02-07 18:39:48.380 Function name: OpenSCManagerW..2023-02-07 18:39

C:\Users\user\AppData\Local\Temp\is-K56MV.tmp\UtilDll.dll

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	223744
Entropy (8bit):	6.552035196075477
Encrypted:	false
SSDEEP:	6144:Q4L7/E4GpmEXrLTilLKvMoiLQpQuK2cVAORcC75FI:K4GpmEXrLTiwvlQjuK2arR5FI
MD5:	79F2386CF7296E8661997193CF01BAAD
SHA1:	726FEA5EABC5B38981B1D6CC5B8BE01212C90616
SHA-256:	101EBA215EF5F833EC332DA2C803FBFF060EB55F32A88EC261B5C4192528E6DD
SHA-512:	123F4FFA772FDE8F901ABF12C49B78EB81975E5E5F38A8EF80C10B4CA08DA422C42EE72F51155FC87A6726217A29B0E8BF22CB927347D324D41E87485C5EFF7E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....p...p...p.us...p.uu.n.p.ut...p..mt...p..ms...p..mu..p.uq...p...q..p.Nly...p.Nlp...p.Nl....p.....p.Nlr...p.Rich..p.....PE..L...[F9`.....!....$...P.....@.....@.....<..l....>..x....p..... "....p.....@.....@.....text....#.....$..... ..`.rdata.....@.....(.....@..@.data...T....P.....0.....@....rsrc.....p.....@.....@..@.reloc.. ".....$...F.....@..B.....

C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE..d.....R.....#.....@.....`.....<!.....P..H....@..0..... .....text..... ..`.rdata..|.... .....@..@.data....,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@.....

C:\Users\user\AppData\Local\Temp\is-RJIJI.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:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

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&.....@..@..... ..... (.....'.....@..@.....

C:\Users\user\AppData\Roaming\FileOpen\Fowpmadi.txt	
Process:	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe
File Type:	data
Category:	dropped
Size (bytes):	60
Entropy (8bit):	5.52764247057246
Encrypted:	false
SSDEEP:	3:39+/34y9q4LlIUBncPA5Vw+en:tRl4F15q
MD5:	61010E7699F30FEED1B3E7C73AC21C8C
SHA1:	5F237B4BD6FD54912ECFACADCE758288EAD907AE
SHA-256:	964A8D039AB66591B3562204CB488DC12B43D262484D6D005895ADB64EED9F5B
SHA-512:	B71C82D414DB61DCA65894BF8A911EDF6B5DBEDEAD5B4F0A25A41F6721A13AC53C32E82E58A5ED58B781BD49B51696349EF6A1CB4AFE87B502DCCFDCBF9E1F3C
Malicious:	false
Preview:	..*.I%.1./....]...p.S.f....).-7..d}.5..*7i%.\7K2...)m...

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	• 02/03/2021 00:00:00 01/03/2023 23:59:59
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
mov eax, 004B10D8h
call 00007FF854A91215h
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 00007FF854B33927h
call 00007FF854B3347Eh
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007FF854AA6C88h

Instruction
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D3Ch
call 00007FF854A8BE07h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D3Ch]
mov dl, 01h
mov eax, dword ptr [004237A4h]
call 00007FF854AA7CEFh
mov dword ptr [004C1D40h], eax
xor edx, edx
push ebp
push 004B6546h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007FF854B339AFh
mov dword ptr [004C1D48h], eax
mov eax, dword ptr [004C1D48h]
cmp dword ptr [eax+0Ch], 01h
jne 00007FF854B39FAAh
mov eax, dword ptr [004C1D48h]
mov edx, 00000028h
call 00007FF854AA85E4h
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
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
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		

Name	RVA	Size	Type	Language	Country
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

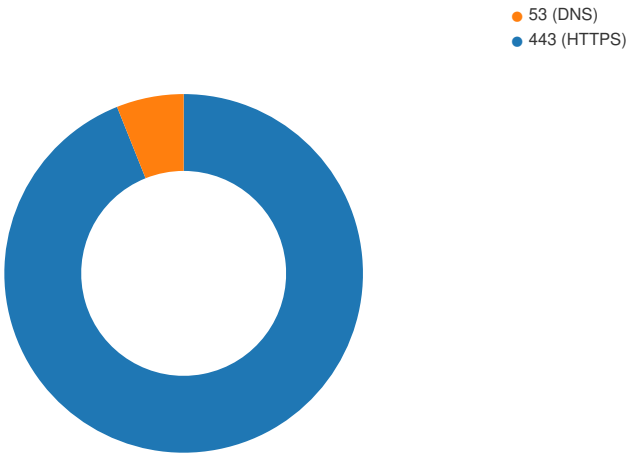
Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 33



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:40:17.564126968 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:17.564145088 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:17.564351082 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:17.576366901 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:17.576374054 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:17.973437071 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:17.973717928 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.059180975 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.059195995 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.059534073 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.059776068 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.061364889 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.061364889 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.061387062 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.417651892 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.417804956 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.417831898 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.417990923 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.418032885 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.418131113 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.419624090 CET	49803	443	192.168.11.20	72.3.136.136
Feb 7, 2023 18:40:18.419634104 CET	443	49803	72.3.136.136	192.168.11.20
Feb 7, 2023 18:40:18.786721945 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:18.786739111 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:18.786868095 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:18.787334919 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:18.787343979 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.192358017 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.192694902 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.194992065 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.195024967 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.195450068 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.195997000 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.196116924 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.236479044 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.328406096 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.328579903 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.328623056 CET	443	49804	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.328874111 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.329595089 CET	49804	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.329643965 CET	443	49804	72.3.136.132	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:40:19.331896067 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.331989050 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.332298040 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.332508087 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.332551956 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.605200052 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.605422020 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.607630014 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.607639074 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.608886003 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.608921051 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.911317110 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.911520004 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.911544085 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.911575079 CET	443	49805	72.3.136.132	192.168.11.20
Feb 7, 2023 18:40:19.911669970 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.914753914 CET	49805	443	192.168.11.20	72.3.136.132
Feb 7, 2023 18:40:19.914788008 CET	443	49805	72.3.136.132	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:40:17.513036966 CET	54958	53	192.168.11.20	1.1.1.1
Feb 7, 2023 18:40:17.554100037 CET	53	54958	1.1.1.1	192.168.11.20
Feb 7, 2023 18:40:18.452562094 CET	64384	53	192.168.11.20	1.1.1.1
Feb 7, 2023 18:40:18.785670996 CET	53	64384	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:40:17.513036966 CET	192.168.11.20	1.1.1.1	0xc93	Standard query (0)	usr.fileopen.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:40:18.452562094 CET	192.168.11.20	1.1.1.1	0x7553	Standard query (0)	plugin.fileopen.com	A (IP address)	IN (0x0001)	false

DNS Answers

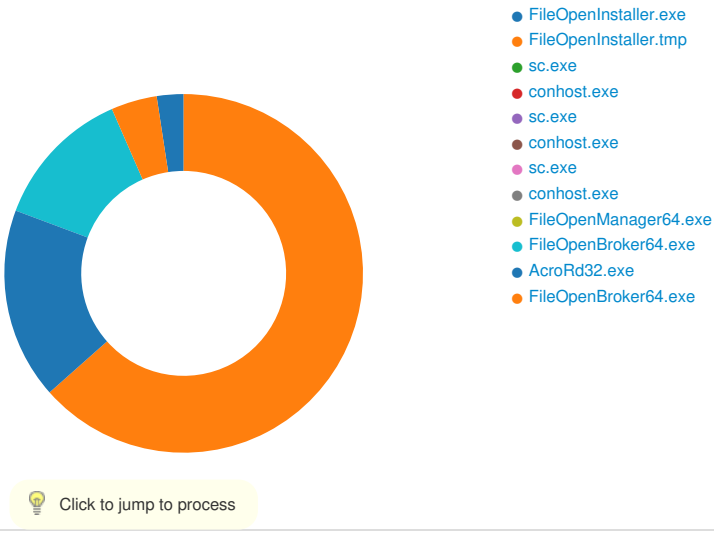
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:40:17.554100037 CET	1.1.1.1	192.168.11.20	0xc93	No error (0)	usr.fileopen.com		72.3.136.136	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:40:18.785670996 CET	1.1.1.1	192.168.11.20	0x7553	No error (0)	plugin.fileopen.com		72.3.136.132	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- usr.fileopen.com
- plugin.fileopen.com

Statistics

Behavior



System Behavior

Analysis Process: FileOpenInstaller.exe PID: **3304**, Parent PID: **4844**

General

Target ID:	0
Start time:	18:39:46
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

Analysis Process: FileOpenInstaller.tmp PID: **6536**, Parent PID: **3304**

General

Target ID:	4
Start time:	18:39:47
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp" /SL5="$6040A,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	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F8BC5	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	64452C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	420D96	CreateFileW
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp\UtilDll.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\Program Files\FileOpen\unins000.dat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	62B65A	CreateFileW
C:\Program Files\FileOpen\is-NSHSA.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen\is-9KV5A.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen\examples	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\Program Files\FileOpen\examples\is-5NKPI.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen\Services	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\Program Files\FileOpen\Services\is-JKV7N.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen\Services\is-FC998.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\ProgramData\FileOpen\Updates\L10n	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\ProgramData\FileOpen\Updates\L10n\is-B9C47.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\L10n\is-50LB9.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\L10n\is-BQIFQ.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\L10n\is-H0NCM.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F765A	CreateDirectoryW
C:\ProgramData\FileOpen\Updates\Lists\is-O4NSE.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-OQA7C.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-THTBB.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-KNQ1D.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-9F2R0.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-DNLJ4.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-L7T53.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\ProgramData\FileOpen\Updates\Lists\is-CKRT4.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW
C:\Program Files\FileOpen\unins000.msg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp\UtilDll.dll	success or wait	1	5F77F0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup_setup64.tmp	success or wait	1	5F77F0	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files\FileOpen\is-NSHSA.tmp	C:\Program Files\FileOpen\unins000.exe	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\is-9KV5A.tmp	C:\Program Files\FileOpen\UtilDll.dll	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\examples\is-5NKPI.tmp	C:\Program Files\FileOpen\examples\installcomplete.pdf	success or wait	1	5F7B77	MoveFileW
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\FileOpen.api	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\Services\is-JKV7N.tmp	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\Services\is-FC998.tmp	C:\Program Files\FileOpen\Services\FileOpenManager64.exe	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-B9C47.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_de.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-50LB9.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_fr.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-BQIFQ.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_ja.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-H0NCM.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_zh.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-O4NSE.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-OQA7C.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-THTBB.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-KNQ1D.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-9F2R0.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-DNLJ4.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-L7T53.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-CKRT4.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd	success or wait	1	5F7B77	MoveFileW

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 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	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 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	229	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	353	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	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 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	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 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	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 33 39 3a 34 37 2e 39 38 39 20 20 20	2023-02-07 18:39:47.989	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 33 39 3a 34 38 2e 33 33 33 20 20 20	2023-02-07 18:39:48.333	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 33 39 3a 34 38 2e 33 33 33 20 20 20	2023-02-07 18:39:48.333	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 33 39 3a 34 38 2e 33 33 33 20 20 20	2023-02-07 18:39:48.333	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 33 39 3a 34 38 2e 33 33 33 20 20 20	2023-02-07 18:39:48.333	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp_isetup_setup64.tmp	0	6144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd fd 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 50 45 00 00 64 fd 05 00 60 1c 52 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^l=\=\=\RichPE dR#	success or wait	1	420DE1	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	874	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	144	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	927	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	72	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	984	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	72	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1034	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	63	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1144	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	63	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	4587	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 33 38 30 20 20 20	2023-02-07 18:39:48.380	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-K56MV.tmp\UtilDll.dll	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 7c 1e fd fd 1d 70 fd fd 1d 70 fd fd 1d 70 2d 75 73 fd fd 1d 70 2d 75 75 fd 6e 1d 70 2d 75 74 fd fd 1d 70 fd 0e 6d 74 fd fd 1d 70 fd 0e 6d 73 fd fd 1d 70 fd 0e 6d 75 7e 1d 70 2d 75 71 fd fd 1d 70 fd fd 1d 71 03 1d 70 fd 4e 6c 79 fd fd 1d 70 fd 4e 6c 70 fd fd 1d 70 fd 4e 6c fd fd fd 1d 70 fd fd 1d fd fd fd 1d 70 fd 4e 6c 72 fd fd 1d 70 fd 52 69 63 68 fd 1d 70	MZ@!L!This program cannot be run in DOS mode.$|pppuspuunputp mtpmspmupuqpqpNlypNl ppNlppNlrpRichp	success or wait	4	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	9722	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 33 39 3a 34 38 2e 34 32 36 20 20 20	2023-02-07 18:39:48.426	success or wait	27	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10352	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 38 2e 38 37 35 20 20 20	2023-02-07 18:40:08.875	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10408	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 38 2e 39 38 34 20 20 20	2023-02-07 18:40:08.984	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10451	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 38 2e 39 38 34 20 20 20	2023-02-07 18:40:08.984	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10949	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 30 33 31 20 20 20	2023-02-07 18:40:09.031	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11024	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 30 33 31 20 20 20	2023-02-07 18:40:09.031	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11087	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 30 37 38 20 20 20	2023-02-07 18:40:09.078	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11147	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 30 37 38 20 20 20	2023-02-07 18:40:09.078	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11235	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11297	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11730	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11803	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11887	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11981	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12025	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12106	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12161	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12236	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 31 32 35 20 20 20	2023-02-07 18:40:09.125	success or wait	3	5B6D0C	WriteFile
C:\Program Files\FileOpen\is-NSHSA.tmp	0	16384	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 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	191	5B6D0C	WriteFile
C:\Program Files\FileOpen\is-NSHSA.tmp	48	4	49 6e 55 6e	InUn	success or wait	1	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12284	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 32 38 20 20 20	2023-02-07 18:40:09.328	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12344	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 32 38 20 20 20	2023-02-07 18:40:09.328	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12388	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 32 38 20 20 20	2023-02-07 18:40:09.328	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12468	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 32 38 20 20 20	2023-02-07 18:40:09.328	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12543	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 32 38 20 20 20	2023-02-07 18:40:09.328	success or wait	51	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\FileOpen\is-9KV5A.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 7c 1e fd fd 1d 70 fd fd 1d 70 fd fd 1d 70 2d 75 73 fd fd 1d 70 2d 75 75 fd 6e 1d 70 2d 75 74 fd fd 1d 70 fd 0e 6d 74 fd fd 1d 70 fd 0e 6d 73 fd fd 1d 70 fd 0e 6d 75 7e 1d 70 2d 75 71 fd fd 1d 70 fd fd 1d 71 03 1d 70 fd 4e 6c 79 fd fd 1d 70 fd 4e 6c 70 fd fd 1d 70 fd 4e 6c fd fd fd 1d 70 fd fd 1d fd fd fd 1d 70 fd 4e 6c 72 fd fd 1d 70 fd 52 69 63 68 fd 1d 70	MZ@!L!This program cannot be run in DOS mode.$|pppuspuunputp mtpmspmupuqpqpNlypNlppNlppNlrpRichp	success or wait	4	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12591	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 37 35 20 20 20	2023-02-07 18:40:09.375	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12915	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 33 37 35 20 20 20	2023-02-07 18:40:09.375	success or wait	12	5B6D0C	WriteFile
C:\Program Files\FileOpen\examples\is-5NKPI.tmp	0	65536	25 50 44 46 2d 31 2e 36 0d 25 fd fd fd fd 0d 0a 33 38 20 30 20 6f 62 6a 3c 3c 2f 4c 69 6e 65 61 72 69 7a 65 64 20 31 2f 4c 20 31 36 32 39 39 31 2f 4f 20 34 30 2f 45 20 31 35 37 34 35 39 2f 4e 20 31 2f 54 20 31 36 32 36 38 39 2f 48 20 5b 20 35 36 34 20 31 39 39 5d 3e 3e 0d 65 6e 64 6f 62 6a 0d 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 36 36 20 30 20 6f 62 6a 3c 3c 2f 44 65 63 6f 64 65 50 61 72 6d 73 3c 3c 2f 43 6f 6c 75 6d 6e 73 20 35 2f 50 72 65 64 69 63 74 6f 72 20 31 32 3e 3e 2f 46 69 6c 74 65 72 2f 46 6c 61 74 65 44 65 63 6f 64 65 2f 49 44 5b 3c 46 45 32 33 31 32 41 34 42 38 39 46 44 36 34 41 39 34 30 34 34 43 38 43 37 34 42 41 45 46 38 35 3e 3c 37 36 35 33 43 46 46 46 34 37 46 38 35 30 34 32 39 36 41 34 38 45 45 37	%PDF-1.6%38 0 obj<</Linearized 1/L 162991/O 40/E 157459/N 1/T 162689/H [564 199]>>endobj 66 0 obj<</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<FE2312A4B89FD64A94044C8C74BAEF85><7653CFFF47F8504296A48EE7	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13057	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 34 33 37 20 20 20	2023-02-07 18:40:09.437	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13144	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 30 39 2e 34 33 37 20 20 20	2023-02-07 18:40:09.437	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\is-GV932.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 28 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 5c fd fd fd fd fd fd 5c fd fd 15 fd fd fd 5c fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 5c fd fd fd fd fd fd fd fd fd fd fd fd fd fd 31 fd fd fd fd fd 5c fd fd fd fd fd fd fd fd fd fd fd fd fd 7d fd fd fd fd fd fd fd 7d fd fd fd fd fd fd fd 7d fd fd fd fd fd fd fd 7d fd 79 fd fd fd fd	MZ@(!L!This program cannot be run in DOS mode.$1}}}}y	success or wait	35	5B6D0C	WriteFile
C:\Program Files\FileOpen\Services\is-JKV7N.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 67 fd fd fd 09 c5 fd 09 c5 fd 09 d1 fd 0d 96 fd 09 d1 fd 0a 8a fd 09 d1 fd 0c fd 4c fd 09 fd e7 0d 96 fd 09 fd e7 0a 8f fd 09 d1 fd 0f 84 fd 09 fd e7 0c fd fd fd 09 e2 14 74 c7 fd 09 e2 14 67 d0 fd 09 d1 fd 08 9c fd 09 c5 fd 08 fd fd fd 09 fd 39 fd 0d 84 fd 09 fd 39 fd 0c af fd 09 fd 39 fd 09 84 fd 09	MZ@(!L!This program cannot be run in DOS mode.$gLtg999	success or wait	32	5B6D0C	WriteFile
C:\Program Files\FileOpen\Services\is-FC998.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 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 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 11 25 fd fd 70 4b fd fd 70 4b fd fd 70 4b fd fd 1b 4f fd fd 70 4b fd fd 1b 48 fd fd 70 4b fd fd 1b 4e fd 32 70 4b fd fd 05 4f fd fd 70 4b fd fd 05 48 fd fd 70 4b fd fd 1b 4d fd fd 70 4b fd fd 05 4e fd fd 70 4b fd fd 1b 4a fd fd 70 4b fd fd 70 4a fd 72 70 4b fd fd fd 36 fd fd 70 4b fd fd fd 25 fd fd 70 4b fd 1b 05 4e fd fd 70 4b fd 1b 05 fd fd fd 70 4b fd fd 70 fd fd fd 70 4b	MZ@ !L!This program cannot be run in DOS mode.$%pKpKpKOpKHpK N2pKOpKHpKMpKNpKJ pKpJrpK6pK%pK NpKpKppK	success or wait	13	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	14934	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 30 37 38 20 20 20	2023-02-07 18:40:10.078	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	15005	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 30 37 38 20 20 20	2023-02-07 18:40:10.078	success or wait	3	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\L10n\is-B9C47.tmp	0	12648	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 32 34 39 36 30 30 30 31 30 30 37 32 77 66 4e 61 6d 69 7a 30 78 7a 64 64 4b 51 48 74 79 70 7a 38 58 48 73 76 4f 78 50 49 72 54 71 73 48 77 49 33 6b 55 48 78 49 5a 77 3d 77 66 4e 61 6d 7a 7a 30 7a 52 46 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 58 49 72 54 71 34 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 74 79 6d 2f 79 59 4c 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 57 36 4c 7a 48 64 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 41 35 58 31 41 78 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 62 32 31 2b 6c 39 48 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 55 61 31 7a 32 69 4f 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 42 5a 52 6e 78 4f 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000249600010072wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zRFBKRDtypz8MHsvOxXIrTq4HwI3gUHxIekwE6otym/yYLUZP7PIEy8O/bpGxW6LzHdWOK3fYHRItpDgBaA5X1AxvY2BO/XOfKySo1Db21+l9H//wtfYGiYOORGAUa1z2iOm5ELO3M+r0ktrNKBZRnxOzECsQsuEa/+1aid
C:\ProgramData\FileOpen\Updates\L10n\is-50LB9.tmp	0	12752	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 32 34 39 36 30 30 30 31 30 30 31 37 36 77 66 4e 61 6d 69 7a 30 78 7a 64 64 4b 51 48 74 79 70 7a 38 58 48 73 76 4f 78 50 49 72 54 71 73 48 77 49 33 6b 55 48 78 49 5a 77 3d 77 66 4e 61 6d 7a 7a 30 7a 53 68 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 58 49 72 54 71 61 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 74 79 6d 2f 79 65 62 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 57 36 4c 7a 48 78 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 41 35 58 31 41 35 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 62 32 31 2b 6c 39 33 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 55 61 31 7a 32 68 61 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 42 5a 52 6e 78 2f 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000249600010176wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zShBKRDtypz8MHsvOxXIrTqaHwI3gUHxIekwE6otym/yebUZP7PIEy8O/bpGxW6LzHxWOK3fYHRItpDgBaA5X1A5vY2BO/XOfKySo1Db21+l93//wtfYGiYOORGAUa1z2ham5ELO3M+r0ktrNKBZRnx/zECsQsuEa/+1aid

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\L10n\is-BQIFQ.tmp	0	15400	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 32 34 39 36 30 30 30 31 32 38 32 34 77 66 4e 61 6d 69 7a 30 78 7a 64 64 4b 51 48 74 79 70 7a 38 58 48 73 76 4f 78 50 49 72 54 71 73 48 77 49 33 6b 55 48 78 49 5a 77 3d 77 66 4e 61 6d 7a 7a 30 7a 51 46 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 58 49 72 54 72 76 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 74 79 6d 2f 79 48 62 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 57 36 4c 7a 48 74 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 41 35 58 31 41 58 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 62 32 31 2b 6c 67 33 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 55 61 31 7a 32 69 61 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 42 5a 52 6e 78 49 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000249600012824wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwl3kUHxlZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwl3gUHxIekwE6otym/yHbUZP7PlEy8O/bpGxW6LzHtWOK3fYHRItpDgBaA5X1AXvY2BO/XOfKySo1Db21+lg3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxIzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\L10n\is-H0NCM.tmp	0	10172	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 32 34 39 36 30 30 30 30 30 37 35 39 36 77 66 4e 61 6d 69 7a 30 78 7a 64 64 4b 51 48 74 79 70 7a 38 58 48 73 76 4f 78 50 49 72 54 71 73 48 77 49 33 6b 55 48 78 49 5a 77 3d 77 66 4e 61 6d 7a 7a 30 7a 53 39 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 58 49 72 54 71 4d 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 74 79 6d 2f 79 54 62 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 57 36 4c 7a 46 78 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 41 35 58 31 42 61 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 62 32 31 2b 6c 2f 58 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 55 61 31 7a 32 67 75 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 42 5a 52 6e 78 78 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000249600007596wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwl3kUHxlZw=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwl3gUHxIekwE6otym/yTbUZP7PlEy8O/bpGxW6LzFxWOK3fYHRItpDgBaA5X1BavY2BO/XOfKySo1Db21+l/X//wtfYGiYOORGAUa1z2gum5ELO3M+r0ktrNKBZRnxxzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\is-O4NSE.tmp	0	7568	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 37 34 38 38 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 4c 49 72 54 71 73 48 77 49 33 36 55 48 78 49 64 38 3d 77 66 4e 61 6d 7a 7a 30 7a 54 59 4c 52 6e 69 44 36 74 69 54 56 58 73 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 51 35 58 31 42 33 6a 4c 53 78 43 39 6a 2b 54 49 47 69 6b 67 54 75 36 32 57 56 2b 30 58 50 38 6f 33 59 47 69 59 4f 4f 52 47 41 56 36 31 7a 32 6b 57 6d 35 44 65 76 33 4d 2b 72 30 30 74 72 4e 4b 64 5a 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000044000748800000000wfNamjzkzT1BNRD8ypz8XHsvOxLIrTqsHwl36UHxId8=wfNamzz0zTYLRniD6tiTVXsvOxTIrTqtHwl3gUHxIekwE6ovym/yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3jLSxC9j+TlGikgTu62WV+0XP8o3YGiYOORGAV61z2kWm5Dev3M+r00trNKdZRnwrzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\Lists\is-OQA7C.tmp	0	80	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 7a 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 3d	lcd&00010000000000044000000000000000wfNamjzkzT1BNRD8ypz8XHsvOxzIrTqtHwl3gUHxIek=	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\Lists\is-THTBB.tmp	0	7248	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 37 31 36 38 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 62 49 72 54 71 73 48 77 49 33 41 55 48 78 49 63 4d 3d 6b 62 63 63 7a 47 36 39 6d 57 56 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 51 35 58 31 42 33 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 65 32 31 2b 6c 79 33 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 56 36 31 7a 32 6b 57 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 64 5a 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2f 6c 4c 6d 45	lcd&00010000000000044000716800000000wfNamjzkzT1BNRD8ypz8XHsvOxbIrTqsHwl3AUHxIcM=kbcczG69mWVBKRDtypz8MHsvOxTIrTqtHwl3gUHxIekwE6ovym/yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//lLmE	success or wait	1	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\is-KNQ1D.tmp	0	720	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 30 30 36 34 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 50 49 72 54 71 73 48 77 49 33 2b 55 48 78 49 65 30 3d 70 5a 5a 61 6d 7a 7a 30 7a 54 64 42 4b 52 44 74 79 70 7a 38 4d 42 31 41 54 33 2b 58 79 56 2b 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 51 35 58 31 42 33 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 63 36 57 2b 55 2f 31 4c 50 39 66 72 71 49 33 49 2f 44 43 75 78 5a 5a 64 44 36 68 2b 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 64 5a 52 6e 77 72 71 6a 4b 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000064000000000wfNamjzkzT1BNRD8ypz8XHsvOxPIrTqsHwl3+UHxIe0=pZZamzz0zTdBKRDtypz8MB1AT3+XyV+tHwl3gUHxIekwE6ovym/yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRltpDgBaQ5X1B3vY2BO/XOfKySo1Dc6W+U/1LP9frql3I/DCuxZZdD6h+m5ELO3M+r0ktrNKdZRnwrqjKsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\Lists\is-9F2R0.tmp	0	1104	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 30 31 30 32 34 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 58 49 72 54 71 73 48 77 49 33 34 55 48 78 49 65 45 3d 77 66 4e 61 6d 6e 43 48 75 55 52 42 4b 52 44 74 68 76 57 50 52 41 67 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 4f 44 66 46 74 6c 73 63 6b 79 74 57 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 51 35 58 31 42 33 76 59 32 42 4f 2f 58 4f 66 4b 32 56 52 31 44 61 32 30 6d 6c 79 6e 2f 2f 77 6a 6e 59 47 69 59 4f 4f 52 47 41 55 4f 45 64 76 54 61 6d 35 45 4c 4f 6b 4b 37 46 74 54 34 4b 55 38 49 71 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000102400000000wfNamjzkzT1BNRD8ypz8XHsvOxXIrTqsHwl34UHxIeE=wfNamnCHuURBKRDthvWPRAgvOxTIrTqtHwl3gUHxIekwE6ovym/yVrUZP7ODfFtlsckytW6LzApWOK3fYHRltpDgBaQ5X1B3vY2BO/XOfK2VR1Da20mlyn//wjnYGiYOORGAUOEdvTam5ELOkK7FtT4KU8IqRnwrzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\is-DNLJ4.tmp	0	2640	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 32 35 36 30 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 48 49 72 54 71 73 48 77 49 33 41 55 48 78 49 65 59 3d 68 49 73 71 39 31 4f 47 71 45 56 42 4b 52 44 74 79 70 7a 38 4d 48 73 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 76 57 59 64 63 68 57 4c 54 55 46 6b 2b 6a 35 58 76 58 4f 66 4b 79 53 6f 31 44 65 32 31 2b 6c 79 33 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 56 36 31 7a 32 6b 57 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 64 5a 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2f 36 48 31 4d	lcd&00010000000000440000256000000000wfNamjzkzT1BNRD8ypz8XHsvOxHlrTqsHwl3AUHxIeY=hIsq91OGqEVBKRDtypz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym/yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRltvWYdchWLTUFk+j5XvXOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//6H1M	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\Lists\is-L7T53.tmp	0	2960	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 32 38 38 30 30 30 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 66 49 72 54 71 73 48 77 49 33 79 55 48 78 49 66 63 3d 77 66 4e 61 6d 7a 7a 30 7a 54 49 48 59 46 79 6f 38 4a 7a 38 4d 48 73 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 70 44 67 42 61 51 35 58 31 42 33 76 59 32 42 4f 2f 58 4f 66 4b 6a 65 35 68 47 61 6a 78 44 71 68 79 7a 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 56 36 31 7a 32 6b 57 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 64 5a 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2b 31 61 69 64	lcd&00010000000000440000288000000000wfNamjzkzT1BNRD8ypz8XHsvOxflrTqsHwl3yUHxIfc=wfNamzz0zTIHYFyo8Jz8MHsvOxTlrTqtHwl3gUHxIekwE6ovym/yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRltpDgBaQ5X1B3vY2BO/XOfKje5hGajxDqhyz/wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\is-CKRT4.tmp	0	424	6c 63 64 26 30 30 30 31 30 30 30 30 30 30 30 30 30 34 34 30 30 30 30 30 30 33 34 34 30 30 30 30 30 30 30 77 66 4e 61 6d 6a 7a 6b 7a 54 31 42 4e 52 44 38 79 70 7a 38 58 48 73 76 4f 78 44 49 72 54 71 73 48 77 49 33 41 55 48 78 49 65 73 3d 6b 62 63 63 79 46 4b 56 70 6c 4a 76 61 45 43 6b 79 70 7a 38 4d 48 73 76 4f 78 54 49 72 54 71 74 48 77 49 33 67 55 48 78 49 65 6b 77 45 36 6f 76 79 6d 2f 79 56 72 55 5a 50 37 50 6c 45 79 38 4f 2f 62 70 47 78 6d 36 4c 7a 41 70 57 4f 4b 33 66 59 48 52 49 74 73 43 6b 51 2f 64 58 50 6a 73 53 76 59 32 42 4f 2f 58 4f 66 4b 79 53 6f 31 44 65 32 31 2b 6c 79 33 2f 2f 77 74 66 59 47 69 59 4f 4f 52 47 41 56 36 31 7a 32 6b 57 6d 35 45 4c 4f 33 4d 2b 72 30 6b 74 72 4e 4b 64 5a 52 6e 77 72 7a 45 43 73 51 73 75 45 61 2f 2f 45 41 78 56	lcd&00010000000000440000034400000000wfNamjzkzT1BNRD8ypz8XHsvOxDIrTqsHwl3AUHxIes=kbccyFKVplJvaECkypz8MHsvOxTIrTqtHwl3gUHxIekwE6ovym/yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItsCkQ/dXPjsSvY2BO/XOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//EAxV	success or wait	1	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	18822	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	18870	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	18967	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19021	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19077	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19135	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19201	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19258	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\FileOpen\unins000.msg	0	23332	49 6e 6e 6f 20 53 65 74 75 70 20 4d 65 73 73 61 67 65 73 20 28 36 2e 30 2e 30 29 20 28 75 29 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 fd 00 00 00 24 5b 00 00 e4 fd fd 2f 1d 31 fd 43 00 61 00 6e 00 63 00 65 00 6c 00 20 00 69 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 53 00 65 00 6c 00 65 00 63 00 74 00 20 00 61 00 63 00 74 00 69 00 6f 00 6e 00 00 00 26 00 49 00 67 00 6e 00 6f 00 72 00 65 00 20 00 74 00 68 00 65 00 20 00 65 00 72 00 72 00 6f 00 72 00 20 00 61 00 6e 00 64 00 20 00 63 00 6f 00 6e 00 74 00 69 00 6e 00 75 00 65 00 00 00 26 00 54 00 72 00 79 00 20 00 61 00 67 00 61 00 69 00 6e 00 00 00 26 00 41 00 62 00 6f 00 75 00 74 00 20 00 53 00 65 00 74 00 75 00 70	Inno Setup Messages (6.0.0) (u)$[/1Cancel installationSelect action&Ignore the error and continue&Try again&About Setup	success or wait	2	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19354	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19499	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19556	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19632	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 33 37 34 20 20 20	2023-02-07 18:40:10.374	success or wait	3	5B6D0C	WriteFile
C:\Program Files\FileOpen\unins000.dat	0	448	49 6e 6e 6f 20 53 65 74 75 70 20 55 6e 69 6e 73 74 61 6c 6c 20 4c 6f 67 20 28 62 29 20 36 34 2d 62 69 74 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 46 69 6c 65 4f 70 65 6e 43 6c 69 65 6e 74 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 46 69 6c 65 4f 70 65 6e 20 43 6c 69 65 6e 74 20 42 39 39 38 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	Inno Setup Uninstall Log (b) 64-bitFileOpenClientFileOpen Client B998	success or wait	2	5B6D0C	WriteFile
C:\Program Files\FileOpen\unins000.dat	448	12	00 10 00 00 fd fd fd fd 64 10 6a	dj	success or wait	12	5B6D0C	WriteFile
C:\Program Files\FileOpen\unins000.dat	25096	12	76 0c 00 00 fd fd fd fd c3 fd 0a	v	success or wait	2	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19711	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19770	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19813	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19861	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19899	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19963	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 34 33 37 20 20 20	2023-02-07 18:40:10.437	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20109	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 30 2e 37 33 34 20 20 20	2023-02-07 18:40:10.734	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20837	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 31 2e 34 33 37 20 20 20	2023-02-07 18:40:11.437	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21017	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 31 2e 37 38 30 20 20 20	2023-02-07 18:40:11.780	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21072	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 34 33 36 20 20 20	2023-02-07 18:40:15.436	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21115	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 34 33 36 20 20 20	2023-02-07 18:40:15.436	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21164	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 34 33 36 20 20 20	2023-02-07 18:40:15.436	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21202	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 34 33 36 20 20 20	2023-02-07 18:40:15.436	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21306	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 34 33 36 20 20 20	2023-02-07 18:40:15.436	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21365	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 35 2e 36 33 39 20 20 20	2023-02-07 18:40:15.639	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21414	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 34 30 3a 31 36 2e 37 38 33 20 20 20	2023-02-07 18:40:16.783	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
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	1	5B6C3C	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	1	success or wait	3	5B6C3C	ReadFile
C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp	unknown	16384	success or wait	1	5B6C3C	ReadFile
C:\Users\user\AppData\Local\Temp\is-RJIJI.tmp\FileOpenInstaller.tmp	unknown	16384	success or wait	190	5B6C3C	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	4	success or wait	1	5B6C3C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	1	success or wait	23	5B6C3C	ReadFile
C:\Users\user\Desktop\FileOpenInstaller.exe	unknown	65536	success or wait	51	5B6C3C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	success or wait	1	5B0F75	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	FileOpenBroker	unicode	"C:\Program Files\FileOpen\Services\FileOpenBroker64.exe"	success or wait	1	6295B1	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Setup Version	unicode	6.0.4 (u)	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: App Path	unicode	C:\Program Files\FileOpen	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	InstallLocation	unicode	C:\Program Files\FileOpen\	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Icon Group	unicode	FileOpen	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: User	unicode	Arthur	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Setup Type	unicode	standard	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Selected Components	unicode	pdf,pdf\dist	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Deselected Components	unicode	pdf\trace	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Inno Setup: Language	unicode	en	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	DisplayName	unicode	FileOpen Client B998	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	UninstallString	unicode	"C:\Program Files\FileOpen\unins000.exe"	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	QuietUninstallString	unicode	"C:\Program Files\FileOpen\unins000.exe" /SILENT	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	DisplayVersion	unicode	B998	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	Publisher	unicode	FileOpen Systems Inc.	success or wait	1	622A39	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	URLInfoAbout	unicode	http://www.fileopen.com/request-tech-support/	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	HelpLink	unicode	http://www.fileopen.com/request-tech-support/	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	NoModify	dword	1	success or wait	1	622A98	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	NoRepair	dword	1	success or wait	1	622A98	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	InstallDate	unicode	20230207	success or wait	1	622A39	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FileOpenClient_is1	EstimatedSize	dword	8553	success or wait	1	622A98	RegSetValueExW

Analysis Process: sc.exe PID: **4948**, Parent PID: **6536**

General

Target ID:	6
Start time:	18:40:10
Start date:	07/02/2023
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\sc.exe" create FileOpenManager binpath= "\"C:\Program Files\FileOpen\Services\FileOpenManager64.exe\"" start= auto
Imagebase:	0x7ff767990000
File size:	72192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3300**, Parent PID: **4948**

General

Target ID:	7
Start time:	18:40:10
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70dd20000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: 3296, Parent PID: 6536

General

Target ID:	8
Start time:	18:40:10
Start date:	07/02/2023
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\sc.exe" description FileOpenManager "FileOpen Client Manager"
Imagebase:	0x7ff767990000
File size:	72192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4300, Parent PID: 3296

General

Target ID:	9
Start time:	18:40:10
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70dd20000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: 2492, Parent PID: 6536

General

Target ID:	10

Start time:	18:40:11
Start date:	07/02/2023
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\sc.exe" start FileOpenManager
Imagebase:	0x7ff767990000
File size:	72192 bytes
MD5 hash:	3FB5CF71F7E7EB49790CB0E663434D80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3208, Parent PID: 2492

General

Target ID:	11
Start time:	18:40:11
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70dd20000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: FileOpenManager64.exe PID: 5084, Parent PID: 896

General

Target ID:	12
Start time:	18:40:11
Start date:	07/02/2023
Path:	C:\Program Files\FileOpen\Services\FileOpenManager64.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\FileOpen\Services\FileOpenManager64.exe
Imagebase:	0x7ff600a70000
File size:	846816 bytes
MD5 hash:	2ACE6BC0F8B1752879AD54D4EA1938D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: FileOpenBroker64.exe PID: 5748, Parent PID: 6536

General

Target ID:	13
Start time:	18:40:11
Start date:	07/02/2023
Path:	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe
Imagebase:	0x7ff668dd0000
File size:	2089968 bytes
MD5 hash:	DE1A88EBE38A4EB36E2C88B1A69A0251
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FileOpen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF668F32040	CreateDirectoryW
C:\ProgramData\FileOpen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668F32040	CreateDirectoryW
C:\ProgramData\FileOpen\Updates	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668F32040	CreateDirectoryW
C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\FileOpen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF668F32040	CreateDirectoryW
C:\Users\user\AppData\Roaming\FileOpen\Fowpmadi.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF668F43344	CreateFileW
C:\Users\user\AppData\Roaming\FileOpen\WebPublisherDemo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF668F32040	CreateDirectoryW
C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\FileOpen\WebPublisherDemo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF668F32040	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF668E98343	HttpSendRequestA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FileOpen\Fowpmadi.txt	0	60	fd fd 2a 19 49 25 fd 31 1a 2f 1b fd fd fd 5d 17 fd dd 70 fd 53 97 66 fd fd fd 07 29 fd 2d 37 fd fd 64 7d 0f 35 fd fd 2a 37 69 25 fd 5c 37 4b 32 fd fd fd 29 6d fd fd fd	*I%1/]pSf)-7d}5*7i%\7K2)m	success or wait	1	7FF668F34074	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\FileOpen	success or wait	1	7FF668E95DE9	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\FileOpen	success or wait	1	7FF668E95E49	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\FileOpen\FileOpenClient	success or wait	1	7FF668E95E49	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\FileOpen	Fowp3Uuid	binary	F2 A1 F9 2A 19 49 25 AB 31 1A 2F 1B BD B7 92 5D 17 D8 CF 9D 70 85 53 DE 97 66 9D 92 8E 07 29 A4 2D 37 90 E6 64 7D 0F 35	success or wait	1	7FF668E97964	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\FileOpen	Fowp3Madi	binary	F2 A1 F9 2A 37 69 25 98 5C 37 4B 32 D5 EE E9 29 6D C1 BC EE	success or wait	1	7FF668E97992	RegSetValueExA

Analysis Process: AcroRd32.exe PID: **7032**, Parent PID: **6536**

General

Target ID:	15
Start time:	18:40:15
Start date:	07/02/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" installcomplete.pdf
Imagebase:	0x650000
File size:	3014368 bytes
MD5 hash:	6791EAE6124B58F201B32F1F6C3EC1B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67DC4F	CreateDirectoryExW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt22.lst.1460	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C905A	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock7032.1.2496545763.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	6FBBC2	CreateFileW
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A95of2mf_yg8e71_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	748DE8	HttpSendRequestA
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	6BAC25	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9ax1nej_yg8e72_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9z5v46e_yg8e73_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A96il8kd_yg8e74_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A997yjmq_yg8e75_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91pk4u3f_yg8e76_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A97pebsj_yg8e77_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91fwov6u_yg8e78_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A91waesx5_yg8e79_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9t0trxz_yg8e7a_14k.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	6BAC25	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt22.lst.1460	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst	success or wait	1	707157	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	6BB769	RegCreateKeyW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	65DE03	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	65DE03	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	65DE03	RegCreateKeyExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFolders	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFolders\c1	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\DetectSign	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\ToolsSearch	success or wait	1	6BBCED	NtCreateKey
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVConnector\cIconCache	success or wait	1	6BBCED	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Program Files/FileOpen/examples/installcomplete.pdf	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	installcomplete.pdf	success or wait	1	6CCCA7	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	6CCCC9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 50 72 6F 67 72 61 6D 20 46 69 6C 65 73 2F 46 69 6C 65 4F 70 65 6E 2F 65 78 61 6D 70 6C 65 73 2F 69 6E 73 74 61 6C 6C 63 6F 6D 70 6C 65 74 65 2E 70 64 66 00	success or wait	1	6CCCC9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 33 30 32 30 37 31 38 34 30 32 30 5A 00	success or wait	1	6CCCC9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	162991	success or wait	1	6CCCE9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	6CCCE9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	6CCCA7	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	6CCCC9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	6CCCC9	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 32 31 30 38 31 38 31 32 31 36 35 38 2B 30 31 27 30 30 27 00	success or wait	1	6CCCC9	RegSetValueExW

Analysis Process: FileOpenBroker64.exe PID: **5344**, Parent PID: **4844**

General

Target ID:	16
Start time:	18:40:19
Start date:	07/02/2023
Path:	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\FileOpen\Services\FileOpenBroker64.exe"
Imagebase:	0x7ff668dd0000
File size:	2089968 bytes
MD5 hash:	DE1A88EBE38A4EB36E2C88B1A69A0251
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF668F32CF1	ReadFile

Disassembly

No disassembly