ID: 800687
Sample Name:
FileOpenInstaller.exe
Cookbook: default.jbs
Time: 18:13:58
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

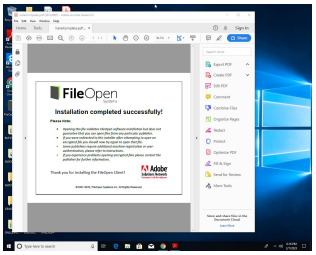
Windows Analysis Report

FileOpenInstaller.exe

Overview

General Information

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



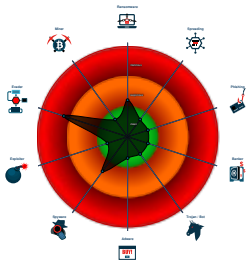
Detection

Score:	26
Range:	0 - 100
Whitelisted:	false
Confidence:	20%

Signatures

- Query firmware table information (lik…
- Changes security center settings (n…
- 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…
- May sleep (evasive loops) to hinder…
- Checks if Antivirus/Antispyware/Fire…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…

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 w10x64**
- FileOpenInstaller.exe (PID: 4844 cmdline: C:\Users\user\Desktop\FileOpenInstaller.exe MD5: 599EBD4AF31288DB879786F49BF9487D)
  - FileOpenInstaller.tmp (PID: 2380 cmdline: "C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp" /SL5="$10404,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" MD5: B7988AC379CEAA456BAA3EF19EB55263)
    - sc.exe (PID: 6164 cmdline: "C:\Windows\system32\sc.exe" create FileOpenManager binpath= "\"C:\Program Files\FileOpen\Services\FileOpenManager64.exe\"" start= auto MD5: D79784553A9410D15E04766AAAB77CD6)
      - conhost.exe (PID: 6172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sc.exe (PID: 6208 cmdline: "C:\Windows\system32\sc.exe" description FileOpenManager "FileOpen Client Manager" MD5: D79784553A9410D15E04766AAAB77CD6)
      - conhost.exe (PID: 6216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sc.exe (PID: 6256 cmdline: "C:\Windows\system32\sc.exe" start FileOpenManager MD5: D79784553A9410D15E04766AAAB77CD6)
      - conhost.exe (PID: 6264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - FileOpenBroker64.exe (PID: 6352 cmdline: C:\Program Files\FileOpen\Services\FileOpenBroker64.exe MD5: DE1A88EBE38A4EB36E2C88B1A69A0251)
    - AcroRd32.exe (PID: 6416 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" installcomplete.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
      - RdrCEF.exe (PID: 6624 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
- svchost.exe (PID: 5916 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4072 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4808 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2840 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4608 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 2376 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 4384 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5444 cmdline: c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3672 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)

- MpCmdRun.exe (PID: 5340 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
  - conhost.exe (PID: 5456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5372 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- FileOpenManager64.exe (PID: 6300 cmdline: C:\Program Files\FileOpen\Services\FileOpenManager64.exe MD5: 2ACE6BC0F8B1752879AD54D4EA1938D9)
- FileOpenBroker64.exe (PID: 6576 cmdline: "C:\Program Files\FileOpen\Services\FileOpenBroker64.exe" MD5: DE1A88EBE38A4EB36E2C88B1A69A0251)
- svchost.exe (PID: 6232 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1128 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **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

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Lowering of HIPS / PFW / Operating System Security Settings

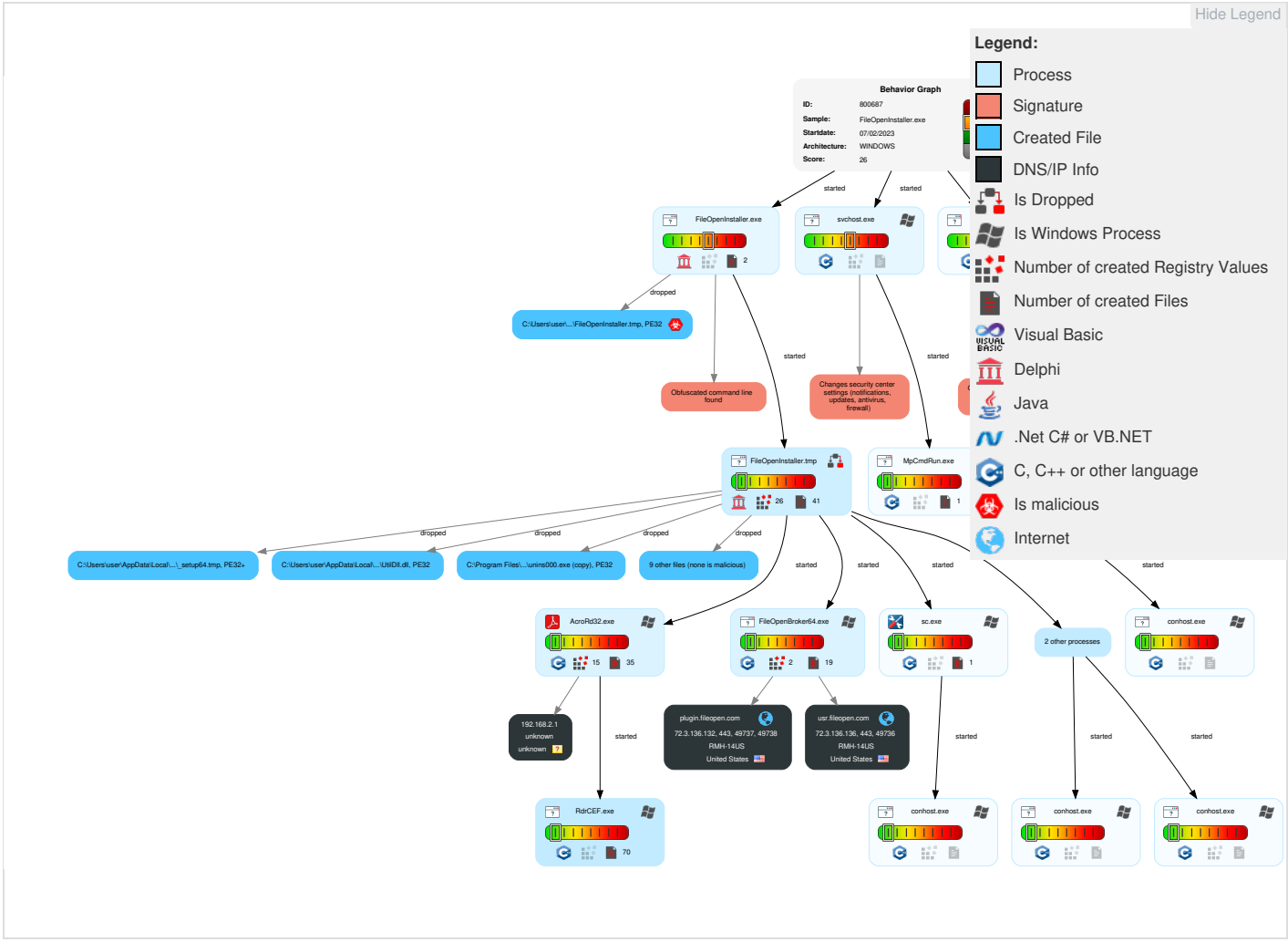
Changes security center settings (notifications, updates, antivirus, firewall)

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

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 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	1 6 Windows Service	1 Access Token Manipulation	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 6 Windows Service	1 Obfuscated Files or Information	Security Account Manager	4 4 System Information 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	1 3 Service Execution	Logon Script (Mac)	1 Process Injection	1 DLL Side-Loading	NTDS	1 5 1 Security Software 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 Registry Run Keys / Startup Folder	3 Masquerading	LSA Secrets	1 2 Virtualization/Sandbox Evasion	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 2 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	2 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

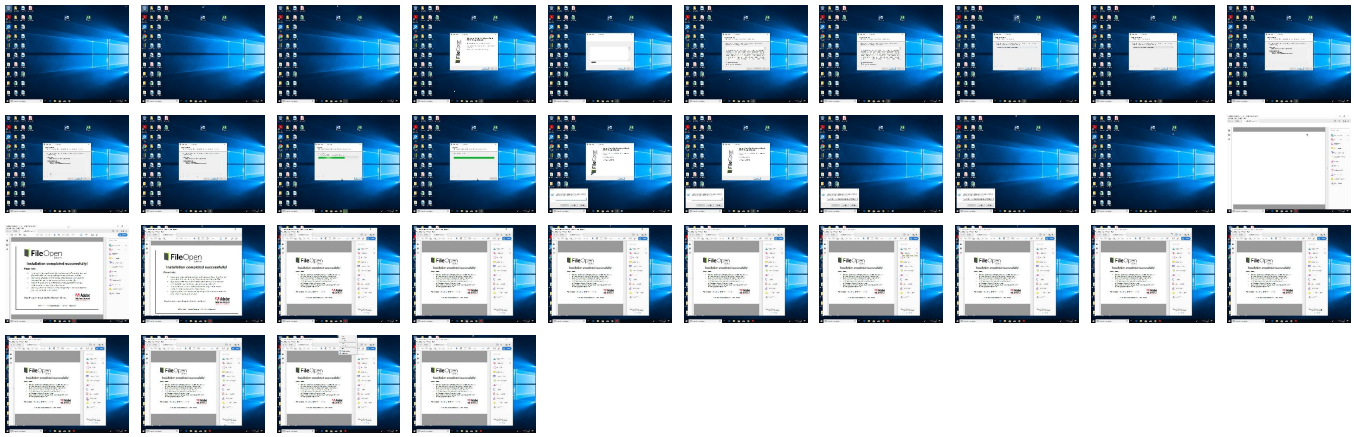
Behavior Graph

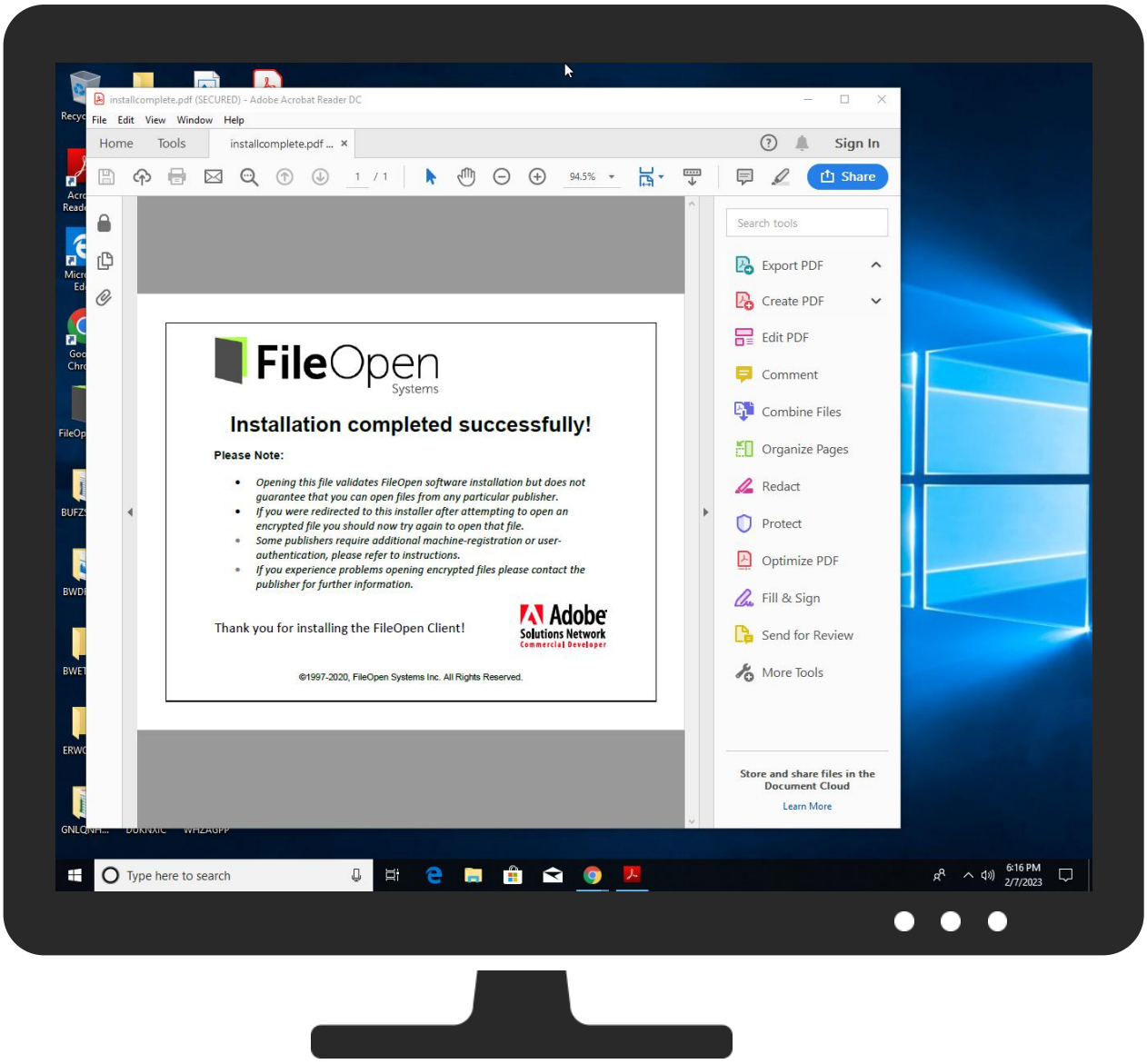


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FileOpenInstaller.exe	0%	ReversingLabs		
FileOpenInstaller.exe	0%	Virustotal		Browse

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\is-U9E22.tmp	2%	ReversingLabs		
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-GL49N.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\Services\is-KGJ5A.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\UtilDll.dll (copy)	0%	ReversingLabs		
C:\Program Files\FileOpen\is-BU7MM.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\is-LL3TI.tmp	0%	ReversingLabs		
C:\Program Files\FileOpen\unins000.exe (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-IORDB.tmp\UtilDll.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-IORDB.tmp_isetup_setup64.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://help.disneyplus.com	0%	Virustotal		Browse
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://disneyplus.com/legal/subscriber-agreement	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://help.disneyplus.com	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://www.remobjects.com/ps	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

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/aZBj6Q+rFX1ikU6tKzx6k1ti|QIahCGjsg4RWrsiwFk=	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	FileOpenInstaller.exe	false		high
http://https://disneyplus.com/legal/subscriber-agreement	svchost.exe, 0000001B.00000003.411594025.000001B6BD59A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411629471.000001B6BD577000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411738099.000001B6BD5A4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411694374.000001B6BD588000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000006.00000002.313394059.0000029DADC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high

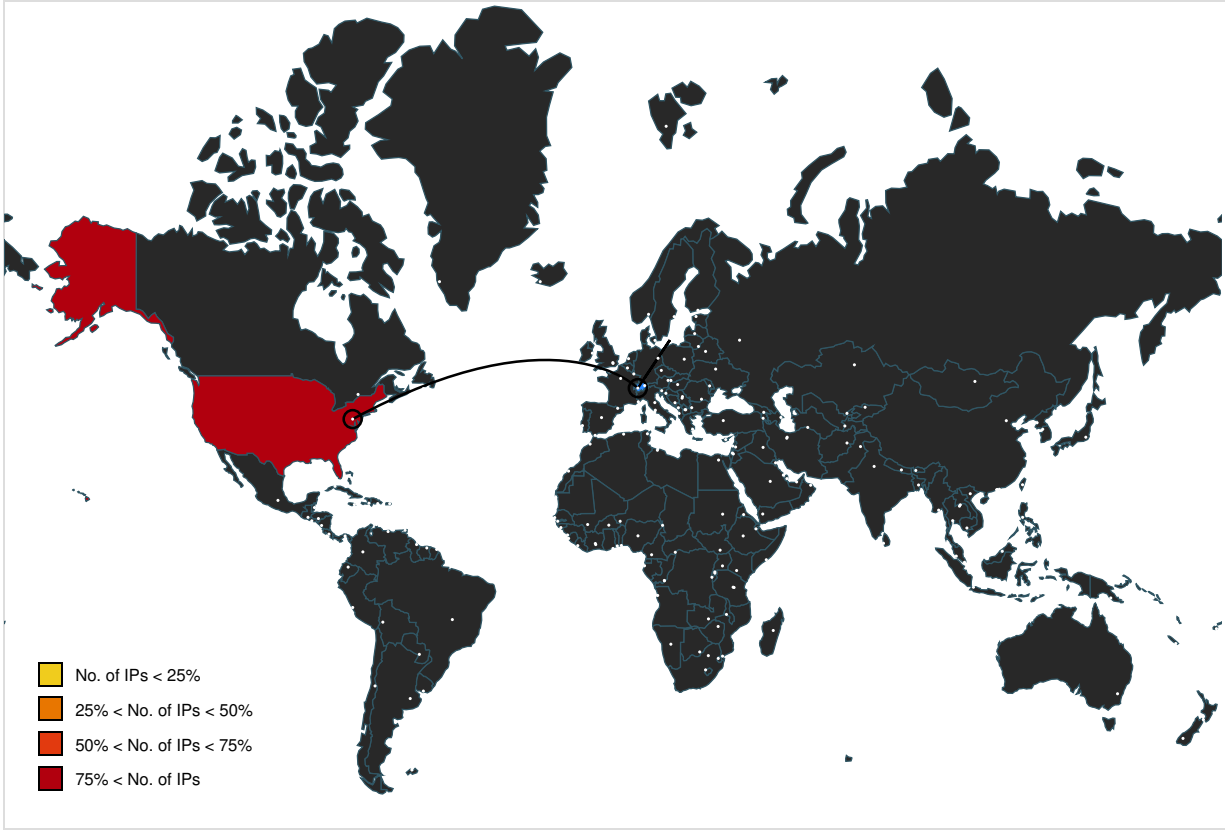
Name	Source	Malicious	Antivirus Detection	Reputation
http://plugin.fileopen.com/.	FileOpenInstaller.tmp, 00000001.00000003.330327512.0000000003855000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000003.330327512.00000000039FE000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000003.330327512.00000000037D0000.00000004.00001000.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000014.00000002.514802671.00007FF72BF0B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000014.00000002.513758365.0000024DCA23C000.00000004.00000020.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000014.00000000.321969420.00007FF72BF0B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000016.00000002.340776018.000001B8CBDC0000.00000004.00000020.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000016.00000002.341394742.00007FF72BF0B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000016.00000000.339698525.00007FF72BF0B000.00000002.00000001.01000000.0000000A.sdmp, is-KGJ5A.tmp.1.dr, is-U9E22.tmp.1.dr	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000006.00000002.313394059.0000029DADC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000006.00000003.312477211.0000029DADC47000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000002.313409269.0000029DADC4D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com/E	FileOpenBroker64.exe, 00000014.00000002.514485574.0000024DCC030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://plugin.fileopen.com/.z&	FileOpenBroker64.exe, 00000014.00000002.513758365.0000024DCA23C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000006.00000003.312972855.0000029DADC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000002.313401443.0000029DADC42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.313036808.0000029DADC41000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://usr.fileopen.com/check/usr/aZBj6Q	FileOpenBroker64.exe, 00000014.00000002.513758365.0000024DCA272000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com/installcomplete.ashx?Request=Setting&Stamp=1675822537&Mode=CNR&USR=10007	FileOpenBroker64.exe, 00000014.00000002.513758365.0000024DCA2E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000006.00000003.312972855.0000029DADC40000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://fileopen.com/updates	FileOpenInstaller.tmp, 00000001.00000003 .330327512.0000000003855000.00000004.000 01000.00020000.00000000.sdmp, FileOpenIn staller.tmp, 00000001.00000003.330327512 .00000000039FE000.00000004.00001000.0002 0000.00000000.sdmp, FileOpenInstaller.tmp, 0000000 1.00000003.330327512.00000000037D0000.00 000004.00001000.00020000.00000000.sdmp, FileOpenBroker64.exe, 00000014.00000002. 514802671.00007FF72BF0B000.00000002.0000 0001.01000000.0000000A.sdmp, FileOpenBro ker64.exe, 00000014.00000000.321969420.0 0007FF72BF0B000.00000002.00000001.010000 00.0000000A.sdmp, FileOpenBroker64.exe, 00000016.00000002.341394742.00007FF72BF0 B000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000016.00000000.339 698525.00007FF72BF0B000.00000002.0000000 1.01000000.0000000A.sdmp, is-KGJ5A.tmp.1.dr, is-U9E22.tmp.1.dr	false		high
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000006.00000003.313036808 .0000029DADC41000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/Zhttp://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000000.00000003 .249527175.0000000002580000.00000004.000 01000.00020000.00000000.sdmp, FileOpenIn staller.tmp, 00000001.00000003.255479179 .00000000033F0000.00000004.00001000.0002 0000.00000000.sdmp	false		high
http://help.disneyplus.com	svchost.exe, 0000001B.00000003.411594025 .000001B6BD59A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.411629471.000001B6BD577000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411738099 .000001B6BD5A4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.411694374.000001B6BD588000.00 000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fileopen.com/0	FileOpenInstaller.exe, FileOpenInstaller.tmp.0.dr	false		high
http://www.bingmapsportal.com	svchost.exe, 00000006.00000002.313352938 .0000029DADC13000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000006.00000002.313394059 .0000029DADC3D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/Q/3	FileOpenInstaller.exe, 00000000.00000003 .339885366.0000000002331000.00000004.000 01000.00020000.00000000.sdmp	false		high
http://https://plugin.fileopen.com/	FileOpenBroker64.exe, 00000014.00000002. 514485574.0000024DCC030000.00000004.0000 0020.00020000.00000000.sdmp	false		high
http://www.innosetup.com/	FileOpenInstaller.exe, 00000000.00000003 .249970577.00000000026C0000.00000004.000 01000.00020000.00000000.sdmp, FileOpenIn staller.exe, 00000000.00000003.250333831 .000000007FBB0000.00000004.00001000.0002 0000.00000000.sdmp, FileOpenInstaller.tmp, 0000000 1.00000000.252856251.0000000000401000.00 000020.00000001.01000000.00000004.sdmp, FileOpenInstaller.tmp.0.dr	false	• URL Reputation: safe	unknown
http:// https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000006.00000003.312665346 .0000029DADC61000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001B.00000003.411594025 .000001B6BD59A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.411629471.000001B6BD577000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411738099 .000001B6BD5A4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.411694374.000001B6BD588000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000006.00000003.312991453 .0000029DADC56000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/qM	FileOpenInstaller.tmp, 00000001.00000003 .335133861.0000000000D14000.00000004.000 01000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000006.00000002.313394059.0000029DADC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000006.00000003.312972855.0000029DADC40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312972855.0000029DADC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001B.00000003.413351324.000001B6BD585000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413374045.000001B6BD5A7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413365349.000001B6BD596000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413397653.000001B6BDA18000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413430330.000001B6BD585000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413413969.000001B6BDA02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.413383708.000001B6BDA18000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000006.00000002.313394059.0000029DADC3D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000002.313352938.0000029DADC13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000004.00000002.513825993.0000023F6823E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000006.00000003.312477211.0000029DADC47000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000002.313409269.0000029DADC4D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000006.00000003.312972855.0000029DADC40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://usr.fileopen.com/	FileOpenBroker64.exe, 00000014.00000002.513758365.0000024DCA2A1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001B.00000003.411594025.000001B6BD59A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411629471.000001B6BD577000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411738099.000001B6BD5A4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.411694374.000001B6BD588000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://plugin.fileopen.com/installcomplete.ashx?Request=DocPerm&Stamp=1675822538&Mode=CNR&USR=10007	FileOpenBroker64.exe, 00000014.00000002.514485574.0000024DCC030000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fileopen.com/request-tech-support/	FileOpenInstaller.exe, 00000000.00000003.339885366.0000000002331000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000003.335133861.0000000000D14000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000006.00000002.313430643.0000029DADC65000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fileopen.com	FileOpenInstaller.tmp, 00000001.00000003.330327512.0000000003855000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000003.330327512.00000000039FE000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000003.330327512.0000000003C10000.00000004.00001000.00020000.00000000.sdmp, FileOpenBroker64.exe, FileOpenBroker64.exe, 00000014.00000000.323167265.00007FF72BF88000.00000002.00000001.01000000.0000000A.sdmp, FileOpenBroker64.exe, 00000016.00000002.341623060.00007FF72BF88000.00000002.00000001.01000000.0000000A.sdmp, is-KGJ5A.tmp.1.dr, is-U9E22.tmp.1.dr	false		high
http://www.fileopen.com/%sPlugin	is-U9E22.tmp.1.dr	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000006.00000003.290703561.0000029DADC32000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000002.313374724.0000029DADC3B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.remobjects.com/ps	FileOpenInstaller.exe, 00000000.00000003.249970577.00000000026C0000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.exe, 00000000.00000003.250333831.000000007FBB0000.00000004.00001000.00020000.00000000.sdmp, FileOpenInstaller.tmp, 00000001.00000000.252856251.0000000000401000.00000020.00000001.01000000.00000004.sdmp, FileOpenInstaller.tmp.0.dr	false	• URL Reputation: safe	unknown
http://https://activity.windows.com	svchost.exe, 00000004.00000002.513825993.0000023F6823E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000006.00000003.312665346.0000029DADC61000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fileopen.com/%s	is-U9E22.tmp.1.dr	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000004.00000002.513825993.0000023F6823E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000006.00000002.313417322.0000029DADC5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000006.00000003.312883589.0000029DADC5A000.00000004.00000020.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800687
Start date and time:	2023-02-07 18:13:58 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	33
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:	SUS
Classification:	sus26.evad.winEXE@40/98@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 81.8%) • Quality average: 61.9% • Quality standard deviation: 38.1%
HCA Information:	• Successful, ratio: 71% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.250, 2.21.22.179, 2.21.22.155, 20.82.228.9, 20.82.154.241
- Excluded domains from analysis (whitelisted): fs.microsoft.com, eudb.ris.api.iris.microsoft.com, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.net, ctldl.windowsupdate.com, arc.msn.com, acroipm2.adobe.com, neus1c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, armmf.adobe.com, a122.dscd.akamai.net, neus2c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:15:28	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run FileOpenBroker "C:\Program Files\FileOpen\Services\FileOpenBroker64.exe"
18:15:39	API Interceptor	1x Sleep call for process: RdrCEF.exe modified
18:16:10	API Interceptor	8x Sleep call for process: svchost.exe modified
18:16:16	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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%
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-U9E22.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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%
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-0FUR6.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-0FUR6.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-GL49N.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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-KGJ5A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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-0FUR6.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-0FUR6.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-SJIP9.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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-BU7MM.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA6
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\is-LL3TI.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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\unins000.dat

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp
File Type:	InnoSetup Log 64-bit FileOpen Client B998, version 0x418, 28302 bytes, 585948\37\user\, C:\Program Files\FileOpen\376\377\377\007
Category:	dropped
Size (bytes):	28302
Entropy (8bit):	3.929149512869022
Encrypted:	false
SSDEEP:	384:PCEwFsZAIVuAhKCVyneFqf8cXKBUorhr+2NQf/A1kKpbPImRe8dAHm:PQI3YQMKBUoF627bbe6
MD5:	360CDFCD83CE2A24376161EF4EA6D66C
SHA1:	F389666B77FD3547D5B618AAE4E3941AAE5DCB06
SHA-256:	947F2F97386B25BCD8E88D720E58056FE37E6420ABB1FAA7482F7BF15973C36E
SHA-512:	ED386F9ECD090CB2838FA0862A2A718736CC86A22DD53C27B92B1074E5B74B11F0047FED9EEEC0B2F8EE703EF4D03B489D9503FAF13327B6FE243653BF1F280D
Malicious:	false
Preview:	Inno Setup Uninstall Log (b) 64-bit.....FileOpenClient.....FileOpen Client B998..... .....n.....q.....k[.....s.....5.8.5 .9.4.8.....e.n.g.i.n.e.e.r.....C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.F.i.l.e.O.p.e.n.....j.. .....]......IFPS....'...P..... ...ANYMETHOD.....BOOLEAN.....TWIZARDFORM....TWIZARDFORM.....TMAINFORM....TMAINFORM.....TU NINSTALLPROGRESSFORM....TUNINSTALLPROGRESSFORM.....

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA6
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-0FUR6.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-0FUR6.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&0001000000000004400002496000100 72wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zRFBKRDtypz8MHsvOxXIrTq4HwI3gUHxIekwE6otym /yYLUZP7PIEy8O/bpGxW6LzHdWOK3fYHRItpDgBaA5X1AxvY2BO/XOfKySo1Db21+l9H//wtfYGiYOORGAUa1z2iOm5ELO3M+r0ktrNKBZRnxOzECsQsuEa/+1aidVgmCc r5OGJOHDz1NMK0yOvHorXY0lEp0E8UW2oOSovzMqnXNMMwnohZZA/WgMLkGJRbbRp9Qe/tz3PFPaGTc4c9uJpl1CN1n1v3n8ScqDkHNQ72m3NFqoEU0IBA6Z MCFRpB3PAx6VQgER3kQUB75gSOYIRe8OFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTI/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-0FUR6.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=wfNamzz0zShBKRDtypz8MHsvOxXIrTqaHwI3gUHxlekwE6otym/yebUZP7PlEy8O/bpGxW6LzHxWOK3fYHRItpDgBaA5X1A5vY2BO/XOfKySo1Db21+l93//wtfYGiYOORGAUa1z2ham5ELO3M+r0ktrNKBZRnx/zECsQsuEa/+1aidVgmCcs5OGJOHDz1NMK0yOvHorXYoIEp0E8UW2oOSovzMqnXNBMwnohZZA/WgMLkGJRbbRoNQe/tz3PFPaGTc4c9uJplVCN1n1v3n8ScqDkHNQ72mgNFqoEU0IBA6ZMCFRpB3PAx6VQgER3kQUB75gSOYlRcAOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQjlOEJyuwk/x+rXld0ne1yi9dcSgih/kSGGEPnISAxskRlCkrqpWfdTJRMD+7negc2JQRjAdpaFIUKJ3ZmXmCKw8aC1F6Ypjp3YJgAGYhkGR1TT7f7tmBmM3Ow5R/RSlhb4U4Q0Fy8Di3AuIKcZ+nXY3KRyHT1OkxMuL8xtcwK52RpN6KGl1McXLIYi4k+HzXTWksHytorOvcqNT4YD+NUbvJyyeauJSvGYqPNvlvmsw0ZoIGDH5KOHUley+9vGyP8vWqMfxM/i+Z8rZw9WUzh8QvZukWUF/Kvhnlci82eegqSdG4MGbsfIubxfArCfQ64TKl1B+H+h5HWyMsIaPrntVQhi4sgM5tYYGqros0o0py2ZFCESgBxPPy/Pe/AorFJoKjzsDfsF/bSeAfJN8lv0aL8JrbukctqROb8gziqsrtHbz1esn4PYRWw3BfHICa6PfiHRQZ7q83b6piRBqYzUh1yqG+1ytB7jBh7A7PjNuK7DMMIVdohKwKMjawkIQHw1j/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	2C335278E6E67FD26AF6DCFC50417CB70EA35BDB4ABA5185F023AEC6BA1948F096677B4A6DA3539B746CC79378F6DAB82F386995CD56F3BD9F977815B11FE659
Malicious:	false
Preview:	lcd&0001000000000004400002496000012824wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwI3gUHxlekwE6otym/yHbUZP7PlEy8O/bpGxW6LzHtWOK3fYHRItpDgBaA5X1AXvY2BO/XOfKySo1Db21+lg3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxIzECsQsuEa/+1aidVgmCc0ZOGJOHDz1NMK0yOvHorXY0IEp0E8UW2oOSovzMqnXNGMwnohZZA/WgMLkGJRbbRrtQe/tz3PFPaGTc4c9uJpm1CN1n1v3n8ScqDkHNQ72mzNFqoEU0IBA6ZMCFRpB3PEx6VQgER3kQUB75gSOYlReMOFEygpaacvJBa+SPwRA0aZu9N3WqHCJ5vks/lgCGrn/fiTl/mokBWgEres7DjQh4OEJyuwk/x+rXld0ne1yihdcSgih/kSGGEPnISAxskQlCkrqpWfdTJRMD+7negcyFQRjAdpaFIUKJ3ZmXmCKwtaC1F6Ypjp3YJgAGYhkGRoDT7f7tmBmM3Ow5R/RSlhbAU4Q0Fy8Di3AuIKcZ+nXZwKRyHT192vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMsIaPrnszQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFOQKjzsDfsF/bSeAfJN8lv1r92vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMsIaPrnszQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFOQKjzsDfsF/bSeAfJN8lv1r92vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMsIaPrntVQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFJoKjzsDfsF/bSeAfJN8lv0KL8JrbukctqROb8gziqsrtHbz1esn4PYRWw3BfHICa7PfiHRQZ7q83b6piRBqYzUR1yqG+1ytB7jBh7A7PjNuK7DMMIVdohKwKMjawkIQHz1j/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwI3gUHxlekwE6otym/yTbUZP7PlEy8O/bpGxW6LzFxWOK3fYHRItpDgBaA5X1BavY2BO/XOfKySo1Db21+l/X//wtfYGiYOORGAUa1z2gum5ELO3M+r0ktrNKBZRnxxzECsQsuEa/+1aidVgmCcrZOGJOHDz1NMK0yOvHorXbslEp0E8UW2oOSovzMqnXN3MwnohZZA/WgMLkGJRbbRl9Qe/tz3PFPaGTc4c9uJpklCN1n1v3n8ScqDkHNQ72l+NFqoEU0IBA6ZMCFRpB3PcR6VQgER3kQUB75gSOYlRaQOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQiAOEJyuwk/x+rXld0ne1yihdcSgih/kSGGEPnISAxskTVCkrqpWfdTJRMD+7negc5lQRjAdpaFIUKJ3ZmXmCKwKaC1F6Ypjp3YJgAGYhkGRsTT7f7tmBmM3Ow5R/RSlhdYU4Q0Fy8Di3AuIKcZ+nXYxKRyHT1OkxMuL8xtcwK52LJN6KGl1McXLIYi4k+HzXUiksHytorOvcqNT4YD+NUbcJyyeauJSvGYqPNvlvmswz5oIGDH5KOHUley+9vGyP/rWqMfxM/i+Z8rZw9WUzh8MvZukWUF/Kvhnlci82eeglydG4MGbsfIubxfArCfQ65LKl1B+H+h5HWyMsIaPrntWQhi4sgM5tYYGqros0o0p0mZFCESgBxPPy/Pe/AorFJAKjzsDfsF/bSeAfJN8lv0KL8JrbukctqROb8gziqsrpXbz1esn4PYRWw3BfHICa87fiHRQZ7q83b6piRBqYzU/1yqG+1ytB7jBh7A7PjNuRrDMMIVdohKwKMjawkIQHxNj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-EBO4V.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:vH6NHxuYvSxaFjN43mKAIz03TusIDR6mZ/juc:yNRuYvSxaFJRIqTvIDR6mZ/I
MD5:	1FF1A88C097A10AF0D2CB463BBB5E4C9
SHA1:	D149B1D0BCD84FAD9A4BD143E7837999BC840141
SHA-256:	3E077B1A201D71636DD045F7B2694AFEE90881DF97704B012DC947C7429492A7
SHA-512:	82AA26F7E0D877A0BEA8D55C57D4D6B98DF283C04360C730E6ED385A589D16438F9BC00B80609B48C33028202661E7343DD4A13A53AE31B6C9A4D8C2E63D102
Malicious:	false
Preview:	lcd&0001000000000044000024960001007 2wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=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\is-ESNP0.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000044000024960000759 6wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwI3gUHxIekwE6otym /yTbUZP7PIEy8O/bpGxW6LzFxWOK3fYHRItpDgBaA5X1BavY2BO/XOfKySo1Db21+l/X//wtfYGiYOORGAUa1z2gum5ELO3M+r0ktrNKBZRnxxzECsQsuEa/+1aidVgmCc rZOGJOHDz1NMK0yOvHorXbslEp0E8UW2oOSovzMqnXN3MwnohZZA/WgMLkGJRbbRl9Qe/tz3PFPaGTc4c9uJpklCN1n1v3n8ScqDkHNQ72l+NFqoEU0IBA6Z MCFRpB3PcR6VQgER3kQUB75gSOYlRaQOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQiAOEJyuwk/x+rXId0ne1yihdcSgih/kSGGEPn ISAxskTVCkrqpWfdTJRMD+7negc5lQRjAdpaFIUKJ3ZmXmCKwKaC1F6Ypjp3YJgAGYhkGRsTT7f7tmBmM3Ow5R/RSlhdYU4Q0Fy8Di3AuIKcZ+nXYxKRyHT1 OkxMuL8xtcwK52LJN6KGl1McXLIYi4k+HzXUiksHytorOvcqNT4YD+NUbcJyyeauJSvGYqPNvlvmswz5oIGDH5KOHUIey+9vGyP/rWqMfxM/i+Z8rZw9WUzh8MvZukWUF/ Kvhnlci82eeglydG4MGbsflubxfArCfQ65LKl1B+H+h5HWyMslaPrntWQhi4sgM5tYYGqros0o0p0mZFCESgBxPPy/Pe/AorFJAKjzsDfsF/bSeAfJN8lv0KL8JrbukctqROb8gziqsrpXbz1esn4PYRWw3BfHICa87fiHRQZ7q83b6piRBqYzU/1yqG+1ytB7jBh7A7PjNuRrDMMIVdohKwKMjawkIQHxNj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-F36NO.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	2C335278E6E67FD26AF6DCFC50417CB70EA35BDB4ABA5185F023AEC6BA1948F096677B4A6DA3539B746CC79378F6DAB82F386995CD56F3BD9F977815B11FE6 9
Malicious:	false

Preview:	lcd&0001000000000004400002496000012824wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwl3kUHxIZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwl3gUHxIekwE6otym /yHbUZP7PlEy8O/bpGxW6LzHtWOK3fYHRItpDgBaA5X1AXvY2BO/XOfKySo1Db21+lg3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxIzECsQsuEa/+1aidVgmCc 0ZOGJOHDz1NMK0yOvHorXY0lEp0E8UW2oOSovzMqnXNGMwnohZZA/WgMLkGJRbbRrtQe/tz3PFPaGTc4c9uJpm1CN1n1v3n8ScqDkHNQ72mzNFqoEU0IBA6Z MCFRpB3PEx6VQgER3kQUB75gSOYlReMOFEygpaacvJBa+SPwRA0aZu9N3WqHCJ5vks/lgCGrn/fiTl/mokBWgEres7DjQh4OEJyuwk/x+rXld0ne1yihdcSgih/kSGGEPn ISAxskQlCkrqpWfdTJRMD+7negcyFQRjAdpaFIUKJ3ZmXmCKwtaC1F6Ypjp3YJgAGYhkGRoDT7f7tmBmM3Ow5R/RSlhbAU4Q0Fy8Di3AuIKcZ+nXZwKRyHT1 OkxMuL8xtcwK52OZN6KGI1McXLIYi4k+HzXfOksHytorOvcqNT4YD+NUaPJyyeauJSvGYqPNvlvmswnZoIGDH5KOHUley+9vGyP9vWqMfxM/i+Z8rZw9WUzh 92vZukWUF/Kvhnlci82eegvydG4MGbsflubxfArCfQ6+XKl1B+H+h5HWyMsIaPrnszQhi4sgM5tYYGqros0o0pr2ZFCESgBxPPy/Pe/AorFOQKjzsDfsF/bSeAfJN8lv1r L8JrbukctqROb8gziqsr73bz1esn4PYRWw3BfHICa7HfiHRQZ7q83b6piRBqYzUR1yqG+1ytB7jBh7A7PjNuObDMMIVdohKwKMjawkIQHz1j/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\L10n\is-F9Q7I.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	A385C69D7CFD88F637D3553BEEFA502563E9620FBA1C502DBCB7CF868383F1CF86D6578FCCCE0EF6B5D0E246E1F94313FF6A3AC01B1529AC78DF5F376B76C3 E2
Malicious:	false
Preview:	lcd&0001000000000004400002496000010176wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwl3kUHxIZw=wfNamzz0zShBKRDtypz8MHsvOxXIrTqaHwl3gUHxIekwE6otym /yebUZP7PlEy8O/bpGxW6LzHxWOK3fYHRItpDgBaA5X1A5vY2BO/XOfKySo1Db21+l93//wtfYGiYOORGAUa1z2ham5ELO3M+r0ktrNKBZRnx/zECsQsuEa/+1aidVgmCc s5OGJOHDz1NMK0yOvHorXYolEp0E8UW2oOSovzMqnXNBMwnohZZA/WgMLkGJRbbRoNQe/tz3PFPaGTc4c9uJplVCN1n1v3n8ScqDkHNQ72mgNFqoEU0IBA6Z MCFRpB3PAx6VQgER3kQUB75gSOYlRcAOFEygpaacvJBa+SPwRA0PZu9N3WqHCJ5vks/lgCGrivfiTl/mokBWgEres7DjQjIOEJyuwk/x+rXld0ne1yi9dcSgih/kSGGEPn ISAxskRlCkrqpWfdTJRMD+7negc2JQRjAdpaFIUKJ3ZmXmCKw8aC1F6Ypjp3YJgAGYhkGR1TT7f7tmBmM3Ow5R/RSlhb4U4Q0Fy8Di3AuIKcZ+nXY3KRyHT1 OkxMuL8xtcwK52RpN6KGI1McXLIYi4k+HzXTWksHytorOvcqNT4YD+NUbvJyyeauJSvGYqPNvlvmsw0ZoIGDH5KOHUley+9vGyP8vWqMfxM/i+Z8rZw9WUzh 8QvZukWUF/Kvhnlci82eegqSdG4MGbsflubxfArCfQ64TKl1B+H+h5HWyMsIaPrntVQhi4sgM5tYYGqros0o0py2ZFCESgBxPPy/Pe/AorFJoKjzsDfsF/bSeAfJN8lv0a L8JrbukctqROb8gziqsrtHbz1esn4PYRWw3BfHICa6PfiHRQZ7q83b6piRBqYzUh1yqG+1ytB7jBh7A7PjNuK7DMMIVdohKwKMjawkIQHw1j/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000004400007488000000000wfNamjzkzT1BNRD8ypz8XHsvOxLIrTqsHwl36UHxId8=wfNamzz0zTYLRniD6tiTVXsvOxTIrTqtHwl3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3jLSxC9j+TlGikgTu62WV+0XP8o3YGiYOORGAV61z2kWm5Dev3M+r00trNKdZRnwrzECsQsuEa/ +1aiddgmCcgJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/Wg+HnC0alboouUpqu3BBmbuIwclJduJpg1CN1n1v3n8ScqD5RdQ72kHNF qoEU0IBA6ZMCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjMXSfbnLk3B7snKKkIbZcVk0lKz0wk/x+rXld1re1yiwdcTV Fh/kSGCEPnlGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3CT5g0zm4vN8l1lk0/frX6DG4GYV+ nXYaKRyHT1OkxMuL826DwK52AJN6KGI1McXLIYi4iOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUley+6PGyP+TkmPbHHsiH Svvul/ui9CoVh6uUA0F/KvhnlcIc2eegiSdGlTibsflvbxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKMKjzsDfsF/bR WwTYBRpsQNHvU/X98mg5B0X/hPiqsrj3bz1esn4PYRWw20oXICa+HfiHRQZ7q83b6piThqYzV41yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6ElQH1Rj/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	80
Entropy (8bit):	4.142037796599528
Encrypted:	false
SSDEEP:	3:5VvXjyoyRd2tUquhltSjt/n:5k7KUquhltSt/n
MD5:	CA943A39A4F5DD13E54089690FEC080A
SHA1:	0DC95BE92BF165A841D1881BC2A14212C31F4792
SHA-256:	FDF6D2CBF65EDCF9E84B66D484BA0FD18FAD427E3EB1BF332C94CADDF1D7EC63

SHA-512:	EE0051B72252A61399E53288CD23EEE59CA4A7139E941A07B750281CFCB77BFD143453BF86F54C03CAD39CABECA7CEC2C5E4D1DC1B8A41E16FB174FA13196 FE
Malicious:	false
Preview:	lcd&0001000000000004400000000000000wfNamjzkzT1BNRD8ypz8XHsvOxzIrTqtHwl3gUHxlek=

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000044000071680000000wfNamjzkzT1BNRD8ypz8XHsvOxbIrTqsHwI3AUHxIcM=kbcczG69mWVBKRDtypz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1De21+ly3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//ILmEWxmCc gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSXN+NJ+Jpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvNEetnG1FF49Zu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPn IGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3ekoep1HY1scU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHytorOvcuIXqM+qAUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh 8hvZukWUF/Kvg3xovOkLf0vCdG4MGbsfIubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPireXi14eFKMKjzsDfsF/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3lCa+DfiHRQZ7q83e76ymojM2FN1yqG+1ytB7jBh7ASPjNuaLDMMlVdohKwKMja6ElQH1Rj/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	4B78F7B57FD666ADA151CFEF2ABAB34A09B5270BE7F7651AEF0AAA1263512C8B35DCB09B70481F010D10417F9D71D13B86A6A51DC77C0FDCA6D50BC5561D6 A5
Malicious:	false
Preview:	lcd&0001000000000044000006400000000wfNamjzkzT1BNRD8ypz8XHsvOxPIrTqsHwI3+UHxIe0=pZZamzz0zTdBKRDtypz8MB1AT3+XyV+tHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1Dc6W+U/1LP9frqI3l/DCuxZZdD6h+m5ELO3M+r0ktrNKdZRnwrqjKsQsuEa/+1aiddgmCc gPXpUlqcqSFMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n3jUnNfeezp1Ni1j01BmCaIXc4NFSZ MCFfpB3PSh6VQgER3kQUfdZgR+YIRZgOFEygpaacvPY1jVivPmUJZu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPn IEMSsVYX2UlodmS4D4cvrOy02QQ6VQRjAdpaFIUKJ3ZnPmCKwRAkxF6Ypjp3YJgAGPhkGRllKUC9A5bAl3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHyvkIOeRI5j2LHOAxL2ERavWdhijDwqPNv4vmsw6JoIGDH5KOHU

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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+NUbHJyyeauJSvGct3NvzvmAw75oIGOv5KOHUIey+7KPWU4jWqMfxYZ3U Aqmtpq7QonNSvZukWUF/KvhnIcic2eegiSdG4MH93oZFPXOzjSfQ67XKl1B+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-0FUR6.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&0001000000000044000025600000000wfNamjzkzT1BNRD8ypz8XHsvOxHlrTqsHwI3AUHxIeY=hIsq91OGqEVBKRDtypz8MHsvOxTlrTqtHwI3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItvWYdchWLTUFk+j5XvXOfKySo1De21+Iy3//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/IubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPqpCst2hZe8hv/RVmBqR/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83f/K+1cIAkFYlln1ki/ZZta1h7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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=wfNamzz0zTIHYFyo8Jz8MHsvOxTlrTqtHwI3gUHxIekwE6ovym /yVrUZP7PlEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKje5hGajxDqhyz/wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa/+1aiddgmCc gJOGJOHDz1NMK0yOtXorXaNjQs8x8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBAjO eW8Z5UXPSh6VQgER3kQUB75gR+YlRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQm1Kde/FtiCB+rXId1re1yiwdcSgih/kSGGEPn IGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3BazkDlzxWRljT7f7tmBmM3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtG wK52AZN6KGl1McXLIYi4iOHzXW/i/D3+6uPuIuYB08ysfAiTYn7OJbAGvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh8hvZukWUF/KvM30Y6xga TI6EkhhcGbsfIubxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKBfy3gDfsF/bSeAfLZ8lv0gL8JrbukctqROb8gViqsr j3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB72H1+AhBDNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000044000034400000000wfNamjzkzT1BNRD8ypz8XHsvOxDIrTqsHwI3AUHxIes=kbccyFKVplJvaECkypz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItsCkQ/dXPjsSvY2BO/XOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//EAxVz4xD1 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSH5sOoTY02Q2UhCYzxaPIKTkon5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvA==

C:\ProgramData\FileOpen\Updates\Lists\is-0GB27.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000044000010240000000wfNamjzkzT1BNRD8ypz8XHsvOxXIrTqsHwI34UHxIeE=wfNamnCHuURBKRDthvWPRAgvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7ODfFtlsckytW6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfK2VR1Da20mlyn//wjnYGiYOORGAUOEdvTam5ELOkK7FtT4KU8IqRnwrzECsQsuEa/+1aiddgmCc gJOGJOGloCcnZyLpxnorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WkLzkGLRbvRkdQe/gv3PFPaGTc4d5jnwH5CN1n1/BaSL6Pk5QwxmwBrWimoEU0IBA6Z MCFfpB3PSh6VQgF3sTB/RNAGNOYIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ9oTM/9gCirhvfiTF3mokBWgEreo+CHMAMOEJyukj2YlMGtBR6svl7VB7eg ih/kSGGEPnIGAxskVVCkrqowEqCiALKN+3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3cOZAGLhleRljT7f2dmBmM3Ow5R5kT46oAU4Q0Fm7KLsn/tW48R 7wJpKRyHT1OkxMuL8xtGwK52AZN6KGJTXrGgcfrLiOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGct3NvzvmAw75oIGOv5KOHUIey+7KPWU4jWqMfxYZ3U Aqmtpq7QonNSvZukWUF/KvhnIcic2eegiSdG4MH93oZFPXOzjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYcBdLoD0oAp62ZFCl+gBxPPy/Pe3UREfc0KjzsDMK42A0 3IH8IV+ZNTL8JrbukctqROb8gViqsrj3bz1etBj4J6FWSyW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB7nGWbAUPjFuerDMMFZdohKwKMja7gBlbCZj/E9kgFfUTywf

C:\ProgramData\FileOpen\Updates\Lists\is-1DS3V.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:wWldo6lPTvnFTx/KTpNsoR0yWx5LT
MD5:	BABA88923DACAC1B9FFCCD1CAA783903
SHA1:	BD9C1D4176B709671310EB31C197E54311DF2E09
SHA-256:	06793859377ADE0F42F713178559A3189B9118884CC9D783E98C36820BEAB899
SHA-512:	C834660D40616847458D21287692BB809101653EE8A29EB24AAC7D7AC6D9967BD78866081216848E073D50ED2E30EF4219CC13BB494A5F6C0201B27CEA5D0ED
Malicious:	false
Preview:	lcd&0001000000000044000003440000000wfNamjzkzT1BNRD8ypz8XHsvOxDIrTqsHwI3AUHxIes=kbccyFKVplJvaECkypz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItsCkQ/dXPjsSvY2BO/XOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//EAxVz4xD1 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaSH5sOoTY02Q2UhCYzxaPIKTkon5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvA==

C:\ProgramData\FileOpen\Updates\Lists\is-3GDF5.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000004400002880000000000wfNamjzkzT1BNRD8ypz8XHsvOxfIrTqsHwI3yUHxIfc=wfNamzz0zTIHYFyo8Jz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKje5hGajxDqhyz/wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa/+1aiddgmCc gJOGJOHDz1NMK0yOtXorXaNjQs8x8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n1v3n8ScqDkH5Q72kENFqoEU0IBAjO eW8Z5UXPSh6VQgER3kQUB75gR+YIRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjPfiTI/mokBWgEreobDjQm1Kde/FtiCB+rXId1re1yiwdcSgih/kSGGEPn IGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3BazkDIzxWRIjT7f7tmBmM3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1OkxMuL8xtG wK52AZN6KGI1McXLIYi4iOHzXW/i/D3+6uPuIuYB08ysfAiTYn7OJbAGvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh8hvZukWUF/KvM30Y6xga TI6EkhhcGbsfIubxfAjSfQ67XKI1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKBfy3gDfsF/bSeAfLZ8lv0gL8JrbukctqROb8gViqsr j3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83b6piThqYzV41yqG+1ytB72H1+AhBDNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

C:\ProgramData\FileOpen\Updates\Lists\is-696VR.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:	0F2ACD1B623362B15C1D634B6E18E14452EAE3BA6F984EEEF2496094EBB258B62EDA2CE607FC99F571EEF54E92507650BB83BA2EBBEAAC223D2346D343DEA 871
Malicious:	false
Preview:	lcd&0001000000000044000025600000000wfNamjzkzT1BNRD8ypz8XHsvOxHIrTqsHwI3AUHxIeY=hIsq91OGqEVBKRDtypz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItvWYdchWLTUFk+j5XvXOfKySo1De21+Iy3//wtfYGiYOORGAV61z2kWm5ELO3M+r0ktrNKdZRnwrzECsQsuEa//6H1Mx7Q/3 gJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPadkJME7TmzSMnTzz1v3n8ScqDkH5Q72kENFqoEU0IBA6Z MCFfpB3PSh6VQgER3kQUB75gR+YIRZgOFEygpaacvNE5i1ySJXkpNIosuQ/1CJ5vks/0gCGrjPfiTI/mokBWgEreobDjQmoOEJyuwk/x+rXId1re1yiwdcSgih/kSGHFXQ BpUX8XZ37B1s9WfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3em0jinbp8fIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGI1McXLIYi4iOHzXWWksHytorOvcuIwk/OcVDLpQlT7auJSvGYqPNv4vmsw6JoIGDH5KOHUIey+6PGyP+TWqMfxM/i+Z8rZw8qUzh 8hvZukWUF/Kvgm9rrzu4bUqWU0j6r+w/IubxfAjSfQ67XKI1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPqpCst2hZe8hv/RVmBqR/bSeAfLZ8lv0g L8JrbukctqROb8gViqsrj3bz1esn4PYRWw3BW3ICa+DfiHRQZ7q83f/K+1cIAkFYlln1ki/ZZta1h7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUl7

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000044000000000000000wfNamjzkzT1BNRD8ypz8XHsvOxzIrTqtHwI3gUHxIek=

C:\ProgramData\FileOpen\Updates\Lists\is-BSLJ5.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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:/HoMwAyoMCkXXIWo1LE+2GK0Jal6
MD5:	55D02DA6997B22D40AC0BBD083D0D79E
SHA1:	5802069EBC18E6B83EF9974E1E88A5DC9AEF3F16
SHA-256:	323CA3057BBCD45288E40132953CD66B7F2AA1A403FA3D336F7E395FB51F94C3
SHA-512:	4B78F7B57FD666ADA151CFEF2ABAB34A09B5270BE7F7651AEF0AAA1263512C8B35DCB09B70481F010D10417F9D71D13B86A6A51DC77C0FDCA6D50BC5561D6 A5
Malicious:	false

Preview:	lcd&0001000000000004400000640000000000wfNamjzkzT1BNRD8ypz8XHsvOxPIrTqsHwI3+UHxIe0=pZZamzz0zTdBKRDtypz8MB1AT3+XyV+tHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3vY2BO/XOfKySo1Dc6W+U/1LP9frqI3l/DCuxZZdD6h+m5ELO3M+r0ktrNKdZRnwrqjKsQsuEa/+1aiddgmCc gPXpUIqcqSFMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/WgMLkGCRbbRj9Qe/tz3PFPaGTc4f9uJpg1CN1n3jUnNfeezp1Ni1j01BmCaIXc4NFSZ MCFfpB3PSh6VQgER3kQUfdZgR+YlRZgOFEygpaacvPY1jVivPmUJZu9N3WqHCJ5vks/0gCGrjPfiTl/mokBWgEreobDjQmoOEJyuwk/x+rXld1re1yiwdcSgih/kSGGEPn IEMSsVYX2UlodmS4D4cvrOy02QQ6VQRjAdpaFIUKJ3ZnPmCKwRAkxF6Ypjp3YJgAGPhkGRllKUC9A5bAl3Ow5R5RSIhfIU4Q0Fy8Di3AuIKd9+nXYaKRyHT1 OkxMuL8xtGwK52AZN6KGl1McXLIYi4iOHzXWWksHyvkIOeRI5j2LHOAxL2ERavWdhijDwqPNv4vmsw6JoIGDH5KOHU

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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&0001000000000004400007488000000000wfNamjzkzT1BNRD8ypz8XHsvOxLIrTqsHwI36UHxId8=wfNamzz0zTYLRniD6tiTVXsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/bpGxm6LzApWOK3fYHRItpDgBaQ5X1B3jLSxC9j+TIGikgTu62WV+0XP8o3YGiYOORGAV61z2kWm5Dev3M+r00trNKdZRnwrzECsQsuEa/ +1aiddgmCcgJOGJOHDz1NMK0yOtXorXaAlEp0E8UW2oOSovzkqnXNsMwnohZZA/Wg+HnC0aIbooouUpqu3BBmbuIwclJduJpg1CN1n1v3n8ScqD5RdQ72kHNF qoEU0IBA6ZMCFfpB3PSh6VQgER3kQUB75gR+YlRZgOFEygpaacvJBa+TPwRA0JZu9N3WqHCJ5vks/0gCGrjMXSfbnLk3B7snKKkIbZcVk0IKz0wk/x+rXld1re1yiwdcTV Fh/kSGCEPnIGAxskVVCkrqpWfdTJRMD++3egc/9QRjAdpaFIUKJ3ZnPmCKwRaC1F6Ypjp3YJgAGPhkGRljT7f7tmBmM3CT5g0zm4vN8l1Ik0/frX6DG4GYV+ nXYaKRyHT1OkxMuL826DwK52AJN6KGl1McXLIYi4iOHzXWWksHytorOvcqNT4Zz+NUbHJyyeauJSvGYqPNv4vmsw6JoIGDH5KOHUley+6PGyP+TkmPbHHsiH Svvul/ui9CoVh6uUA0F/KvhnlcIc2eegiSdGlTibsflvbxfAjSfQ67XKl1B+H+h5HWyMsKSPrntxQhi4sgM5tYYGqroP0o0p+GZFCESgBxPPy/Pe2AorFKMKjzsDfsF/bR WwTYBRpsQNHvU/X98mg5B0X/hPiqsrj3bz1esn4PYRWw20oXICa+HfiHRQZ7q83b6piThqYzV41yqG+1ytB7jBh7ASPjNuaLDMMIVdohKwKMja6EIQH1Rj/E9kwja6IUI7

C:\ProgramData\FileOpen\Updates\Lists\is-UGF2P.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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=kbcczG69mWVBKRDtypz8MHsvOxTIrTqtHwI3gUHxIekwE6ovym /yVrUZP7PIEy8O/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/E9kwja6IUI7

C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	5.228565864551621
Encrypted:	false
SSDEEP:	48:cAn/TLt0J/pXA1JVp/BJVIaSkC9+TON9Bs:pTLt0ZRA1QHksds
MD5:	D88760796BE364BC76C0A7470D9C3DD1
SHA1:	20C810DA01C5F8900ED15BFA7EB17E53A56A9519
SHA-256:	6CFF8173CE17D0D04EA758BCD349510AF229FAFE4871C8AA3117911F46553C35
SHA-512:	48168F46C4E48EDD9C9DE56C63174B83B2DA79E81728487CD2F8368341B3FA83BCCE718CFAF8472463A8F9B3864AA2D52B126987FAD18AE4C0044238F123DB5
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399998126404364</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399998126560620</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399998126404364</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">133051636774803094</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines (2494), with no line terminators
Category:	dropped
Size (bytes):	2494
Entropy (8bit):	5.228565864551621
Encrypted:	false
SSDEEP:	48:cAn/TLt0J/pXA1JVp/BJVIaSkC9+TON9Bs:pTLt0ZRA1QHksds
MD5:	D88760796BE364BC76C0A7470D9C3DD1
SHA1:	20C810DA01C5F8900ED15BFA7EB17E53A56A9519
SHA-256:	6CFF8173CE17D0D04EA758BCD349510AF229FAFE4871C8AA3117911F46553C35
SHA-512:	48168F46C4E48EDD9C9DE56C63174B83B2DA79E81728487CD2F8368341B3FA83BCCE718CFAF8472463A8F9B3864AA2D52B126987FAD18AE4C0044238F123DB5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService d ataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataTyp e="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399998126404364</FirstScanAttempt Time><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399998126560620</LastMeteredScanTime><LastScanAttemptTime dataType ="21">132399998126404364</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType ="21">133051636774803094</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy)

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.750784236184292
Encrypted:	false
SSDEEP:	96:7Hi8isctZYZNnApYZ6hZ3Z5k907HU7/ZaZOZgv2Z1ZeA3iZLpeYZMTag:ri8isSCNnPCpSRU41vdcLpbMr
MD5:	A15680002F4CA722BFF58DBD855B10E6
SHA1:	4A095F6AC4146F0FDFDF56BE2CA457BC9E500467
SHA-256:	7F7E42A44993DA5800799484C1C0ACF237C2DA56372673295B8C33F21C6A3BFF
SHA-512:	13F9A7F7CB140936DC2213EE92E47A1463C496DABB14B1A3FFFF3E868E80CF672271FE6DF79B84734E561E2A170046C93716871C315A5AFCC1574DD96C90256A
Malicious:	false
Preview:	....W..c;.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....V..... .....W..c;.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S. O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P..... ...W..c;..... ....

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.750784236184292
Encrypted:	false
SSDEEP:	96:7Hi8isctZYZNnApYZ6hZ3Z5k907HU7/ZaZOZgv2Z1ZeA3iZLpeYZMTag:ri8isSCNnPCpSRU41vdcLpbMr
MD5:	A15680002F4CA722BFF58DBD855B10E6
SHA1:	4A095F6AC4146F0FDFDF56BE2CA457BC9E500467
SHA-256:	7F7E42A44993DA5800799484C1C0ACF237C2DA56372673295B8C33F21C6A3BFF
SHA-512:	13F9A7F7CB140936DC2213EE92E47A1463C496DABB14B1A3FFFF3E868E80CF672271FE6DF79B84734E561E2A170046C93716871C315A5AFCC1574DD96C90256A
Malicious:	false

Preview:	....W..c;.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....V..... .....W..c;.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P..... ...W..c;..... ....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.608557500697717
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVdpXdJRkt7WviTFJrqzOJkvP5m1:men9YOFLvEWdM9QQdQtOi7Z+P41
MD5:	66F2981575E65A2F2FDCC4DE98F2A5FE
SHA1:	FE844B244DC86B9327CE5D330220278E8D41F5AD
SHA-256:	058913FD74B70A8E9804A56FB71C4A6DB879278D3F8963244D8A78C6BFCB86BB
SHA-512:	277E9588EB812B017DC5780E7CD89E969B071E499F04CA5DDE024CFA24FC791373CDF980BE5ACFB2F5E63159323CCE7301E63753B6101AE33AA47D2A1EA08B2
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ... .R/....."#.DL..w...A.A..Eo.....d.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.557681201069607
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWV7lY61ON5dqkRkt1/lW98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkRC61O7cjt1/Q8Be7YwE
MD5:	319DC6FCDDB50C5A58694C63DBF4F190
SHA1:	98F56C08DE419C2756F5A4068539FF7428F261FE
SHA-256:	B19CA1B8A8660F0CC95AAEC384553C1688DAEFA065A5BD9671C2C4191174AB35
SHA-512:	608952D0422530D4EA0A72E862B728D9B9F064C60087DE76F269552A7709CC7567ABF9A2BA3685FE9BBE590FF3C886ADBA541F7EBAEA678DB23D8B621B7ABA22
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .^R. .R/....."#.D.(.v...A.A..Eo.....9.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.53971454053104
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhumLD3J9tlt/RlUoSjGY1:DyeRVFAFjVFAFmznntZlUo6
MD5:	2C9FDFDFDA4056A0531A4E8300DC8061
SHA1:	EC647076450CE8E4AEDDB9F30AFD8AEDDB311C15
SHA-256:	B05991A50C459E3586C53EA8ED402A7302D9A2EDA6DB26F67E93D3DDAE22DA24
SHA-512:	9F9C02F68AA0AEE579D6B9AEBFC828830BBFB75C955CE9EDDD8E31F9CDA63C98D988DC52155F3A7C7E97320C1F41CA573F77EA9A347C3FAAAD514A90BFDD2EB3
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ... .R/....."#.D...v...A.A..Eo.....Vaa .....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210

Entropy (8bit):	5.559298052540355
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuvnD0S7tTVyh9PT41:pyixRuZnD5V41T
MD5:	F7C4D02DD4B568BAC78D2EF289F9B0D7
SHA1:	99668AE9A240209BCE3CC3902982A076D67F6354
SHA-256:	D23888AC3A1577FB108F53D71C69F4180ABA3784C4AB115836EAA9AA122AAE57
SHA-512:	09EB894A25B9864A5D4257AD8D382445C205BB4283D0FAB404FEDE02836EB98F6CD40A88712AEA049FCCAC3B36D6D93924FE9438930CEFF4DA2D83038657AA1
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js . .. .R/....."#.DV..w...A.A..Eo.....!0).....k.Q.....-_..y.....O...>..1....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.610119085258349
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVmMT/twYk6Rkt0O1xlYo2sZl8xe9:mvYOFLvEWdhwjQRM5A9t003Zll6P41
MD5:	C1682959FEB872D7F51451152C27D8DA
SHA1:	762CE16F308EC3954CEFBEE7152CD67337BD20AA
SHA-256:	C96CBC96D6B39386071CAE710B25E19D97D58795267181C48AAA7C64E83A2166
SHA-512:	F11BCE8359EB0F4B3F0ADED0026DBC9827C71E747D0CFED853468086EBD5ABEE66492D98AF63F4CC48455249C600A39539A4B3C977D5A8139D9EDE969871A72
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..?. .R/....."#.D.l.v...A.A..Eo.....7.....].>....uUf..N...k.....c..l.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.539297172577376
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVD61Ubr89kRkteMlrcyxMtv9G:mJYOFLvEWdGQRQOdQtUP4tZrD6g1
MD5:	3F38FD21C0C37AFD1E69C814F1E7B2FE
SHA1:	76D5BE37C7F5C1C78AF631AA4A79F9F1320A8EBF
SHA-256:	38ABFC208EA6FA32A81C1A562B9F0EF0A88FC8715E1C45CCFCB23EC803A26AC5
SHA-512:	552732ED379E05674A0BE64176CD1A4B2DDBF3A4D8E14AE265CEC944E549A2869157B03AE8FB0145521DD50AF86006AAA2A711D5038B133B65627F46130791A3
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .bE. .R/....."#.D.>.w...A.A..Eo....."....c..y/L....|y.n..C/I.....X7-ne.A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.565488306540718
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVMDv2ukRktAl/llVQMWqg4nRb7om5m1:mOYOFLvECMLM1jtAtEuR/41
MD5:	62A00178CF1CD5765016D20A47AC6930
SHA1:	9B8ABD4E03D33598DD87050DDFDC20E0D7DD27B4
SHA-256:	989DC88890C2677916FD7109AD85DA8C198FA6749D427A96210994A54EB9A92B
SHA-512:	62759FDCF2C032C431116CCECCBD33F0BCCADB8C3A4D09E9C449E99C29E98C9E164ADABE60D78C11978F7B0C2DF4EB84A2AAD449C928D6A272B5729DB975787A
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..k. .R/....."#.D..v...A.A..Eo.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.539496072011788
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuOSem9tktpby0zBUKSAA1:pRg19Qb
MD5:	888A476385433EDD2808F769E870D6F9
SHA1:	FA46876010EBB4E5470592537363F5998434C701
SHA-256:	8EDCCAAFEFBA9219FC05E70206FDE4A0652B20FF7A200D00859BF40B2DB03701
SHA-512:	544570F36F55CCD046D3B0006184B0C55D149A465780494212EC3C0E1804389AAC613E263B22DB4342F7DB5C35D4D236290577BA411C0716B727A0CE5C10B9F2
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .Z.. .R/....."#.D..w...A.A..Eo.....u.....Q..E.=....=h`t..t..3%A. F$..w..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.518916210221289
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvAa0kRktAbWd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvAljtAajUdyP41
MD5:	29B467E83F8964AA3F20D290B85F91F2
SHA1:	81E66428F4B6139802167AA375ED7D0C39E8CC5D
SHA-256:	C08EC5AAA000676AE30952E4C707E40465FF76CAE9F856C40037013E9DE6F6F0
SHA-512:	884BBE61969C16DF5C3351708D309D008E6171A872DC3A846B39856246B7337849AF8DDC51FA2D79A23C77A65F2B4E5E3D5D0C647C965E724813D4B559FC91D
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..X. .R/....."#.Dx|.v...A.A..Eo.....D.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.530556549191272
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLGr6lXs6RktU//jUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLk6lXltUoPqVyM+VY1
MD5:	1C7CD5CCC22219DCE0E733D91C9AE9BB
SHA1:	2442B6F6DE02B22A253247DF7382BD9AA5AEF27E
SHA-256:	CDEEFE433FFA1521E38740F7752ECB300DA33D13C40E9C56AE1F7DBA2D3DD1D1
SHA-512:	7820A795E5740096D3C39A570103F15F0A0BF7C3CB46490A7341620D742E0D9DC53CF2B4FDB4B291786A67B283DDB4C3381D0DBFD91CC6ED0724664A72A4359
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .`. .R/....."#.DK..v...A.A..Eo.....I.....q.O...j....._y..L^z...?..@N..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.555199686075542
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlysC7t+tqtwSeKaT9pr1:URVFAFjVFAFkbtwSeKaTL
MD5:	ECBF53CB2996065C5F85A0EA7D9FFD34
SHA1:	7CDC932D20490004CF8190079A6BBC81222B6C95
SHA-256:	1E837D94125B986B3DDBB41B9F9C501E65FDE7E9EF21AB6F3FEDB1B8C5F0CD07

SHA-512:	3530BE87B6BC0EA0932BC856D11C80C8E51C06ED409ED5EF2224DCBFBF6F7B71358AD509FDDB0E898EBCA7B5CB4A1C749FA9680191078687A712D9DAD73DE D5C
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..@. .R/....."#.D...w...A.A..Eo.....em .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.486279100747757
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvPV3K1HiBk6Rkt+9ll7yrpp:ms2VYOFLvEWdvBIEGdeXureRtmg11
MD5:	036F5CD338D2FC18CA4C41A30C3697F5
SHA1:	6FF1BF3C7D1BEDCADF95188CF2A5CF5026AE8D80
SHA-256:	AC8055A1238A18A7CBC1481A3B064AA8A4051DFFEF19587DB781B58F0365EDF2
SHA-512:	25029D382A3EC3BA5D84DB63F45C893D11AA0DF580E445A071203BA20109266EB2BACFFACB077A09F1AE1FEE56311316815967E1DB1D448467CD86C2A8DA06 E
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .... .R/....."#.D...w...A.A..Eo.....W3.#.....A.o]@r..Q.....<w.....].n\....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.655335360298566
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQxzac7tZyF/7xm7OhKlvA1:RbR16uec7GFTxmJ
MD5:	EF4379FF76719356DFEB8DE38A8A5107
SHA1:	54DE15127AFB982BB8F0127B6B0B1117B0EF8999
SHA-256:	F54C962FC8D75FD2A26FBE02871BF5B0331AA5693601EC2F93D4B3652431D2A5
SHA-512:	FEF85C0DBD12E9B8E265C9005E32BBAE8B540A5E953263812FB3B6FC8444F261374E7F3194B7ACE7E1815C047DD53DD4363CDBCB28983BB4E3DB3C4BB217B FF
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ... .R/....."#.D.4.v...A.A..Eo.....O.....4T].....Tw.....(..b...EO....9.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.5900926923841086
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu7XYk9t2/PdFt1:B2geRHRQmYQY
MD5:	E972D38AFDC985CAFBF337CA58B0140E
SHA1:	A50312E22EDA7EE4AC96ED649AD3BAC44B8C3FA1
SHA-256:	A954D921490216153214A2795DE44CD2CA396D6A8A1AC175CCC4776AD19C58D6
SHA-512:	6A92333836AA9A763EF33E0ABB26CB8A710E09400B88C006B9028BC2557061D9A3FC580BB866409F34332BBE43FB36A5F47AA4E3D6B380A97D2E3AB9945D44C C
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .a.. .R/....."#.D...v...A.A..Eo.....MP.....@..{o]...9o|..qY....T.... {..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.612572912176053
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQZAXq0jtLZgEt1S/1:WyeRluMQEt1
MD5:	7294864F5AB797AAE0855A7F2C46FE06
SHA1:	C9A664771808DDF3A0A64894ECB69F24054E9F87
SHA-256:	AD5C24FBE684F3AB14B24A6C3FB3FF5D2EABE93142101BA9088EA618CA00A7B2
SHA-512:	4B85A771DA13812C6F00421445CBAF298B0509BFE732DC4B28BB686E76CA1FA305FB3852556D9F1F60F24B7BCA4172DFCF433F1844E133954E992C0434E463DE
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .... .R/....."#.D6..v...A.A..Eo.....;.....t\a.....x5.'OuE.C..@.....x..A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.578197774982269
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvihKe7KRkt9tSlwJNqww6U+5m1:mnYOFLvEWdhwyuczJt9tSlwrqwK+41
MD5:	A0B81F50786622C64CA5BAED830732EE
SHA1:	66B5D5A09A920B4768AC916D8EAB357E19EC12FF
SHA-256:	3BBE02BF4138B0EA387E8967634DE1F1047924813BDBBEE1CBC95017BCB6A613
SHA-512:	9EFF9DD7C2704AE87A3577822FDDF60B83587AA34D7E7E1DFE11DD9C2E7162F83D0A506BD0C2B5B8FA8ACF085E7EAA8A577D0AA912E8489E59106421E80A83 B7
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .... .R/....."#.D.g.v...A.A..Eo.....7...o..a=.98I.....(3. $G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.568197757006861
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbull0jtsYfO441:/RrROk/jffL
MD5:	50FE6D717F573667B5722530A7D010A3
SHA1:	9FEC747E27DB142CD4076C636D1B054ED52B8C0C
SHA-256:	1E5A998AA279FCE6882FCA35F85A864120E20BE172B0A3DE310B8F2D09DFFEB6
SHA-512:	27EFB425713EC6CCC3FA5223024EEA40658382066BE6CCC75FC3F23B348737E251923947149F64151A3C8D9C772C2A3B052FCFA576869BF2EFECEEE019015BC
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .*.. .R/....."#.DmU.v...A.A..Eo.....U..J.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.552494387737447
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVQ6lXbrt9kRkt+M/HzoIN1OFPL4m1:mmDEYOFLvEWXIQ6lXl9jtZzV1QPLr1
MD5:	B372E0252B6E2BC6546D423C70E986B4
SHA1:	75248E3602B2143374AFEE81C326B992B29A00B0
SHA-256:	2CE2EF1BA4EE26E8A4EBA7D25E714FC17E36C78604577BD51154367F3B17B891
SHA-512:	B02E823D390650948E91EF3F6A98D37866AF43F0AB2F3B27D07FFF6CF685FB14D9C2C61D2AE8BEAEF28D6B7DD5DBB58D4CB7DF51BCB0365698C3CBEA6D2F0 765
Malicious:	false

Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .m. .R/....."#.D.-.v...A.A..Eo.....g.[.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.5852876423962545
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvLXFa+XR4tBRktAb//m8D6EsEJeUy:m52YOFLvEWdMAuhXFTXttWuEvsEJ41
MD5:	7470A4347A00618F534814897016017C
SHA1:	1479289036FD62996EBFD362593FF93849640113
SHA-256:	63D4E32981625FA29547199E26AA3A3D8531BB748152432F31BE513F40B31D05
SHA-512:	8CE6D7F01A9B5557CEEC9D3A440370410895DD036B2442FB50A27887701A286942FFF11E08B7F64FFD894C3F2DEE0CD792BDACEC8DDA1C0822FC39B58426C8F
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..{. .R/....."#.D...w...A.A..Eo.....A..~.....z._a...'.v.....4p3..1.']...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5518323549476385
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvTFaK15/0kRktaXlGFoDb7M:mYilPYOFLvEWd8CAdAu+K15lt6aong1
MD5:	FAA39476A851888013718A8084365DB1
SHA1:	B824CAD6552BE1F34DD0DEED24BF619B34B2614F
SHA-256:	139F446E427FF3807727A61E900C0B0AE94A6299663895D695389534B56DD7B7
SHA-512:	8EDF470E302277BFC31F855D8DC86D67B19AF5F19E3297F1395E8896DD2295B4FC62042960AB31871852B1B81929C86D34C69B69559ED0ED91CAE4342B9276C3
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .. .R/....."#.D_..w...A.A..Eo.....7M.....c}.H7M=M..-.....Ix..R.I...}Rl .$q.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.614278648013546
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuT81wwVjtkLN16wG1:F8hRrROk/5uSB
MD5:	033732D446F36D625015207DD54ED471
SHA1:	338D0624881C0628C3361BC68CB5EE8850283EFA
SHA-256:	17440A5C44BA886D4E6C17E9AF51664AE94C19EDAF9F13DFEBA7BE7EDFF58BF9
SHA-512:	AE485FE3A499028FC2EDB7BE5A1B3AB57D2BDA0A54A5EB1CBAB4B0E0DA69097320F7BBFB764D3F5E5797B4CBF7C0487EACCEF80B2B7FDFA00FD586660559C1E1
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .... .R/....."#.D...v...A.A..Eo.....`.....%.k.SZ..~W.....:)'B..ad.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.659483910315297
Encrypted:	false

SSDEEP:	6:mLrnYOFLvEWdrloJUQfUeVAG9jt6eJli1:ehRcWUSzjceJI
MD5:	B1C35410C572CD60EEF5C3999BA17D21
SHA1:	5B235E0001C5070B1A6709E2568547E63A1F27D4
SHA-256:	1C0698E6BD1016514259C1D006F18796AC7CA2B3992FDD84397B7A5A272E405A
SHA-512:	FF37897B456607939DC569ED932DC8A0E8E8FAB1E7F2DEE5A426488CC008C7F4E1B772464BB4B45661C710A71EB2893B3EF58CA3AA1EE2E64617E5E5DCDB49 29
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .... .R/....."#.D...v...A.A..Eo.....;"./N_.,.:C..2....9L.H...3:...A.. Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.5521015515022
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFv7/aKlX1Fk/JRktNuNx6mgmOZLP:mOEYOFLvEWdrlhuR/TXQQtNgzgm2d/1
MD5:	37AA77B128B5C95FFF6BFC491C67DA52
SHA1:	1DC7FBDB136068802EE7C619272FF03D232D4B8A
SHA-256:	0D7F5E93B59A92F77A88F9BAB4893E8FE26D90019A29151692BB67B4F70BB897
SHA-512:	3D3E903E929569D4CAB8C6EC8EF7E5F5067447BE9C2330FCEC3CAD187B74073DCEDAB17B1445067A6FAA545BFF0BA900412A7C99FD6A7439A6BE015ABC775 ADB
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..E. .R/....."#.D...v...A.A..Eo.....Kc.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.616958690778208
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvKt6lXzTkd9JRktq9/sBiaQ562HvpMm1:mAElVYOFLvEW1K9QX89Qtqjx56uvp1
MD5:	357DD2ED9B2250BC5414C13590BC244A
SHA1:	72B6ABC5E365EC416ED8CC49228F0A0BEBBA59D9
SHA-256:	F91A4A34A7CD6EEA3EE8E3A989A2F0BAD95CA37495D3BD45F5A8542D79B15FA5
SHA-512:	C450852F47EB234CCEE30444F8E78A3BB104F4ECFD1C0CFDBD9932EA3D750B1A649F02862D4A4162EF33F6E8BF1B35D35C04B197E1EC66C2ACF2AD7B0A0A1 C61
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..!. .R/....."#.D...v...A.A..Eo.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.6572895384755695
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvun/SkdStL9UDLYtmOZn1:xRBJyS7d2DcFZ
MD5:	2A88E5D62B607352B7EDCF32A8E3FBAA
SHA1:	B7278119DAAD9C88476A7EEAC0BA54D89BF2F264
SHA-256:	7C419C76F2B80D5AEA772A458205C610AC15F94F61EFE112D85711B9DCEAC309
SHA-512:	15E0C577B0F14138907D485498CF537B8F944512315A4850098AF1225462529D9826943A8CC06932570FC03DE07E1867FFA8AD1593B176DC671CB4946BA7DFF6
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .M*. .R/....."#.Dz..w...A.A..Eo.....3\.....t.q..W.EZ....1...[.zC.7mD..A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.602084538985618
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvq1YOXl4TkdXRktwtpSKGop:msRPYOFLvEWla7zp75pU7tO8VPu1
MD5:	000B22BB909D6E7350C985CBBD8A6EC0
SHA1:	4AEAB547111D871C9D660DB0BA4981496D26B364
SHA-256:	97D6B197109892E6CA9F746B417A9011B07195B4DAA03DF2D8BF7CC3AD381372
SHA-512:	12AA042980FD3DB9B7E9E39FEEA77FAE9092AD56413FB5350D893D06129CBBC86CACF5D16654AE8AC2F622188B25CE0037C99A4B83056AB11B11C29EB53B4C67
Malicious:	false
Preview:	0\r..m.....S...{.j...._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .Xm. .R/....."#.D.].v...A.A..Eo.....*.....L...Im.@.....E.nW...IP..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.573576236470182
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QbDCcjtPy/CwiM3Y1:bJRT9E2Isfr
MD5:	F78D17150D2B2CA408386EEA9848D139
SHA1:	E195FA40163E359B8678CC41669A2A903274A424
SHA-256:	0903E3005E82112013816FCDE50ABBA18227C53E98DE45F7C650C95A82378489
SHA-512:	B465B9782A1FD7711D755C67AAEDC159B860E7D5FAECD8F705842FB73D2F3E08A1DF34D7DF0358D25FA07C70A2804EFCDD230B74AC313453ADC08A49B0AB24D
Malicious:	false
Preview:	0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..:. .R/....."#.D...v...A.A..Eo.....]..:.....M....m+lS..e.....<7.U.P8*.0K.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.633021082511529
Encrypted:	false
SSDEEP:	3:m+lQWt6v8RzYOCGLvHkWBGKuKjXKjcAW6KLuVY61drlkRktnNB4MY3jBMQ7GRzXA:mQt6EYOFLvEWdccAHQcp1tOjBRCh/41
MD5:	5EDCF39532BCEA1B04D3F2FB23315B20
SHA1:	566D4C5C4CC7D3FD1C1B20535109D9DCAC596AF0
SHA-256:	15E3A1C7807005FA82C89BC3D1ACDCF4ED83FE3EF13262F916F649542447FCD5
SHA-512:	2022197A31E440FA7020FBB6AF0CB6D14A4513E7D0A07D6BF135F749E0BAFFC69B6CB0E038A88C2C77176E9F156CD90C266C34D8F2EB560C9C313A1EE5E1CEDD
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..C. .R/....."#.D...w...A.A..Eo.....>I.....PJm...0x.x..RD...BB!@5..<..]....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.547842738576841
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuzKB1rYQtl3kULlF4r1:bs6xRkiRKPYQ27LlF4
MD5:	8C66385F63D449474044CA4EE8E4BEF1
SHA1:	9464636000030393B9C53F80D273E775013D99CB9

SHA-256:	E09E56354907CB78762DF74CB35DFFBF58C90BB0E8F650A77A509CB8CD9660F3
SHA-512:	7DA5CB9B679623601736ECA8CD0457C674D3FAB2E732903B0BB5DF8B9B2B0135603B1EDF243A1C71E1F712533038D4609277E00AC524CFF63F62BC3C178F2A2
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .<js .R/....."#.D3..v...A.A..Eo.....9S.....P... #4..I....5...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	215
Entropy (8bit):	5.521655388866145
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvCYBlltcxrUG6RktbUXlXECcu1ie:mhYOFLvEWd/aFuNDc39tbUXlEN941
MD5:	E675BFDE70B4BAD8FD368ED872CD84CC
SHA1:	DA5423F89A2B2D4A68803F2A8705E4E80DE3C6D4
SHA-256:	13F01DF7CB5CA9F7E802D0748610BA522C39A8EF452F405153977427C239F744
SHA-512:	C4C171902E7C9B147194793E60FED1114000DC23595065965A26040EA879899D4CB849296C17ADF728CF2201015AD81F04F45AE32F9E3582196467960913C6F4
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .'.. .R/....."#.D...w...A.A..Eo.....V.....a.f.m.i.o.p..3U5.....^...I.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.538409999116882
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQBrn9tc9XVBMqVd3G4K41:2DRuRSJ6lB9Vd2
MD5:	2FB1CD61502A1A0E19FDB25DD52647BD
SHA1:	58B9FF3AA9999CE1596570201944A0684B89DBDE
SHA-256:	034B864A36D28D32F64149DC088024B15884F46C03614E3D7F40D4EB6AC2B585
SHA-512:	4C44BB230DB4DC134FE96EAD462065C1C29D0CEC8663BE6191BE6B2286A0C39F79BF43E589E4F2667A7F9685C17D675A25C8B01340334A55D77FC886442213D
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..V. .R/....."#.D5@.w...A.A..Eo.....fj.....y.$..$.v5j...T...z.]..._S....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.56127863779421
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QZH3K1QNSt16DuA424r1:+RQKH3KKSD6yr
MD5:	367F33BAE28D4C6F76D74E732B055F23
SHA1:	D774E47CB3067AA804609707C07FCB49D32EEC9F
SHA-256:	CE47A89C99673A32BBE9DE6B99D5DAAC7659D6D3AAE118478ABD339151E6A90F
SHA-512:	ECB16BE137C6EB4C95F9E4E3066B86648248491464F63DE8CD1B0B06EFC2BC51539938B95F0C99EA21E1ABC0866D97A61534E89945B5419C6DB35FBDDB231B E8
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .... .R/....."#.Dr. w...A.A..Eo.....8.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

Size (bytes):	210
Entropy (8bit):	5.554682499063756
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFv4RNUKlXrTkxRktBTAg2iHio9:moXXYOFLvEWdENUAuiNT1rntB8yC8n1
MD5:	5D8D23A955EBD495B0769476AA26A780
SHA1:	339C658E86B10E96DC9243F4B532BC81913DCAFA
SHA-256:	2842D49AF4EDFAE012175B7C9A2DBFA1A909AA637D8478F68DC15DBFADF12BB9
SHA-512:	5D2EF13B1B8B5EFC3502FA695D302602CDA65A48DD0509208E379E2669371D980D92539AB261A706E981E6710B81C2E2B918CE7E5D1C8CD71FDBA04A9A1B1B 2
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..t. .R/....."#.D=I.v...A.A..Eo.....8.../...;.\\o....1.....+..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.5929377894266
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVIJ/2kKLuVD59Yk6RktstsYWmYk5m1:mQZYOFLvEWdrROk/VQaCQtstsLmB41
MD5:	FBB83382DEE10B266CF94A4E379255D2
SHA1:	69D5A5FD9F5B5A3DAF2430809822F3FC01B40B10
SHA-256:	54F390F371A8E413A55564538B0CEAEE15817B8E607FE0B7AEC6FD8ED636D41B
SHA-512:	347AE0ED1D49A05555A11ABD79CEA462AF51234FB07FCC09FB8E900A23DD93171AC32FC45F5E493A68CD04F52B6688C4DEF714E4F5CA2E1758D32C19ABF7C2 3C
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .... .R/....."#.D\u.v...A.A..Eo.....46.U..... ./.ev.....N~..6.b.....$ .j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5686348854142524
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWucDh9tL//Jdm9741:qxRck9t//Jdu7
MD5:	48B025322EF5CE3C10B6A4CFF17A8D15
SHA1:	17C85A5789486FAE51CFB4ED347D8C818F1A7D1F
SHA-256:	3D76DCC86E5A2DE996BB5A5B0E53AAB6561157C6F9EF4C122B964160ABC64271
SHA-512:	C438720DA326183B65D85E5105923FC8E35D1A3F118F5669B2E81DABFA1D68C4DADA81C7DC23D17812ED886CD4488E041BFD8D28E6E8478FEE89552F909CAF 6
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .#. .R/....."#.Dd..v...A.A..Eo.....v<.....U...I.>P...X...x..0U.~;m.x.k.A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.538710426542231
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvnapXT/k6RktJHtEB6shoq+Nem1:mMOYOFLvEWdwAPVuN+bk9tlB6Jn1
MD5:	F43988EE6DDD687D5B88A7B6A5A8893C
SHA1:	80022EDEBBC1D9345BB3EE84A539954601EF630D
SHA-256:	418AE1EEA1BE4F438D3C4940D2B97BD4D620C041CA13F851901DD1F2BD151744
SHA-512:	842C75CB997752B144FBE5C14E3E0321E7DC7BDBB84B4E24BD1074451BED6A71439C846D5F0E2CDCE1D5537BB4A122C3C6816CBA5B063A2EA0923E87E9FC2 C9
Malicious:	false

Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..c. .R/....."#.D:..v...A.A..Eo.....Bc.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.679349404573215
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQXk9StLlqhcsBXIh1:mxRBJQ3SiB
MD5:	72E58CC5AFA5F46DFE3FF80AFAA493E4
SHA1:	21366559B986B2EEFFE77C4DDEEA7DCFC548257D
SHA-256:	9824EADCBF0F3486BAFE14F5F2AF265C659BE12D82E0537639E6AEE2A19D35BF
SHA-512:	77D71B8419AA2BCA279981B610D647E16CA7C9D415ED4F9CE396E3782F103C33E138660B6B97AAB1A6EA36E1D92BC2C21CBF7979BCE6359A23F4A3D09358E1E
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..G. .R/....."#.D...w...A.A..Eo.....W.....k..`..N3.... ..d..$[.....{.A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.548560441933939
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQ7hAqjt8c3Me/1:3RrROk/sUAqjq
MD5:	940C3091D259CD46E634A80B1998DA41
SHA1:	ACFFE02EE7D465263EC9FAD533A30594988FBB69
SHA-256:	72B28FCA5EDBF6477C9FB0E49736D5F517C6E2A27B7BB6D57217FB5D2F74F3FE
SHA-512:	86E926FC3CFF5AF0B5D4DE921F87EE3C7B95B6B1CA47B277F3EDD3DD7018AD87DD78BF729C197A7B15E71A45FE305894F6898B1E803F0E498102A741E7D08BBF
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .... .R/....."#.D=e.v...A.A..Eo.....L.....9Q].8O.z....=..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1008
Entropy (8bit):	5.091368420747167
Encrypted:	false
SSDEEP:	12:8Q7+tdcboCH5tQgLxaE8UrkMzl0FKWiUdLimjt8l6SeFH3Qb8AwoZ5T6Q+:8G+tqHZdaXM8NllQWQ+
MD5:	01CD4890796023FFE26B4B6FAD733F90
SHA1:	E22725E8D7D128DCE89A2929A9EFB758EE5D1C66
SHA-256:	30BC515FB3149B660FFC970FD13D235B9FC06E4DA76835A298C2A57774A16D9D
SHA-512:	D55AB4DB596D8B9303A5D95B833BE6508567B255FEF6B98E2FE3C713EB07EA7DD6A55847EAFE1396794A5ADC0DC18B016BF95F58CE77C67E4E65EB1BC628C63F
Malicious:	false
Preview:	....q..Woy retne....(.....P.....*...,. .R/.....:.y~A...,. .R/.....oB*.. .R/.....#...(@.....D.4..o. .R/.....[.i..%..o. .R/.....k7A..,. .R/.....]...I..fq .R/.. .....,+...._.#.,. .R/.....<...W..J.. .R/.....J..j....,. .R/.....6<|..... .R/.....2q.....,. .R/.....P....V.,. .R/.....!...0.o.o. .R/.....P[. q.,. .R/.....3....,. .R/.....v...q.... .R/.....a..... .R/.....C..M..@.....o..k...o. .R/.....*.....o. .R/.....F..=z;...,. .R/.....o...,. .R/.....Gy.'.h...,. .R/.....:..N.A...,. .R/.....;/....,. .R/.....,. .R/.....A?.2:...o. .R/.....q..o. .R/.....u\]..q.o. .R/.....^.~..z..o. .R/.....+.{..'.o. .R/.....MV3...o. .R/.....@..x..o. .R/.....*)....J:.o. .R/.....&.S.....o. .R/.....+.U.!..V.o. .R/.....~.,.4>..o. .R/.....=....m...o. .R/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

Size (bytes):	1008
Entropy (8bit):	5.091368420747167
Encrypted:	false
SSDEEP:	12:8Q7+tdcboCH5tQgLxaE8UrkMzl0FKWiUdLimjt8l6SeFH3Qb8AwoZ5T6Q+:8G+tqHZdaXM8NllQWQ+
MD5:	01CD4890796023FFE26B4B6FAD733F90
SHA1:	E22725E8D7D128DCE89A2929A9EFB758EE5D1C66
SHA-256:	30BC515FB3149B660FFC970FD13D235B9FC06E4DA76835A298C2A57774A16D9D
SHA-512:	D55AB4DB596D8B9303A5D95B833BE6508567B255FEF6B98E2FE3C713EB07EA7DD6A55847EAFE1396794A5ADC0DC18B016BF95F58CE77C67E4E65EB1BC628C63F
Malicious:	false
Preview:	....q..Woy retne....(.....P.....*...,. .R/.....;.y~A...,. .R/.....oB*.. .R/.....#...(@.....D.4..o. .R/.....[.i..%..o. .R/.....k7A..,. .R/.....]...I..fq .R/.. .....,+..._.#.,. .R/.....<...W..J.. .R/.....J..j....,. .R/.....6<|..... .R/.....2q.....,. .R/.....P....V.,. .R/.....!...0.o.o. .R/.....P[. q.,. .R/.....3....,. .R/.....v...q.... . R/.....a..... .R/.....C..M..@.....o..k...o. .R/.....*.....o. .R/.....F..=z;...,. .R/.....o...,. .R/.....Gy.'.h..,. .R/.....:..N.A...,. .R/.....:/....,. .R/.....,. .R/ .....A?.2:...o. .R/.....q..o. .R/.....u\]..q.o. .R/.....^.~..z..o. .R/.....+.{..'.o. .R/.....MV3...o. .R/.....@..x..o. .R/.....*)....J:.o. .R/.....&.S.....o. .R/.....+. U.!..V.o. .R/.....~.,.4>..o. .R/.....=....m...o. .R/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF62cf1a.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1008
Entropy (8bit):	5.091368420747167
Encrypted:	false
SSDEEP:	12:8Q7+tdcboCH5tQgLxaE8UrkMzl0FKWiUdLimjt8l6SeFH3Qb8AwoZ5T6Q+:8G+tqHZdaXM8NllQWQ+
MD5:	01CD4890796023FFE26B4B6FAD733F90
SHA1:	E22725E8D7D128DCE89A2929A9EFB758EE5D1C66
SHA-256:	30BC515FB3149B660FFC970FD13D235B9FC06E4DA76835A298C2A57774A16D9D
SHA-512:	D55AB4DB596D8B9303A5D95B833BE6508567B255FEF6B98E2FE3C713EB07EA7DD6A55847EAFE1396794A5ADC0DC18B016BF95F58CE77C67E4E65EB1BC628C63F
Malicious:	false
Preview:	....q..Woy retne....(.....P.....*...,. .R/.....;.y~A...,. .R/.....oB*.. .R/.....#...(@.....D.4..o. .R/.....[.i..%..o. .R/.....k7A..,. .R/.....]...I..fq .R/.. .....,+..._.#.,. .R/.....<...W..J.. .R/.....J..j....,. .R/.....6<|..... .R/.....2q.....,. .R/.....P....V.,. .R/.....!...0.o.o. .R/.....P[. q.,. .R/.....3....,. .R/.....v...q.... . R/.....a..... .R/.....C..M..@.....o..k...o. .R/.....*.....o. .R/.....F..=z;...,. .R/.....o...,. .R/.....Gy.'.h..,. .R/.....:..N.A...,. .R/.....:/....,. .R/.....,. .R/ .....A?.2:...o. .R/.....q..o. .R/.....u\]..q.o. .R/.....^.~..z..o. .R/.....+.{..'.o. .R/.....MV3...o. .R/.....@..x..o. .R/.....*)....J:.o. .R/.....&.S.....o. .R/.....+. U.!..V.o. .R/.....~.,.4>..o. .R/.....=....m...o. .R/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.2319781134153125
Encrypted:	false
SSDEEP:	6:kfrlL+q2PN72nKuAl9OmbnIFUtWr1ZmwYWLVkwON72nKuAl9OmbjLJ:kpyvVaHAahFUtm/rR5OaHAaSJ
MD5:	B23E47A4D4EB85FD1B0B4CFBE6450E55
SHA1:	E5B5D7383902D7E1DA4EAEBCFAC54537BB343AF8
SHA-256:	E538117601AB9E303FEB2C61C2140DED3C04B25D6B7F596308B4F54FA7AACFAB
SHA-512:	72EEE59169C9AFA5870249D2C3C8813794EFBB7C7E963A7129FB8D83B6CED29C564F1DE3560D50F515E616086439BC766F1EEC6B94B2F81386A2EBFB2BCD8C5
Malicious:	false
Preview:	2023/02/07-18:15:45.557 1a38 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/02/07-18:15:45.748 1a38 Recovering log #3.2023/02/07-18:15:45.749 1a38 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.2319781134153125
Encrypted:	false
SSDEEP:	6:kfrlL+q2PN72nKuAl9OmbnIFUtWr1ZmwYWLVkwON72nKuAl9OmbjLJ:kpyvVaHAahFUtm/rR5OaHAaSJ
MD5:	B23E47A4D4EB85FD1B0B4CFBE6450E55

SHA1:	E5B5D7383902D7E1DA4EAEBCFAC54537BB343AF8
SHA-256:	E538117601AB9E303FEB2C61C2140DED3C04B25D6B7F596308B4F54FA7AACFAB
SHA-512:	72EEE59169C9AFA5870249D2C3C8813794EFBB7C7E963A7129FB8D83B6CED29C564F1DE3560D50F515E616086439BC766F1EEC6B94B2F81386A2EBFB2BCD8C5
Malicious:	false
Preview:	2023/02/07-18:15:45.557 1a38 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/02/07-18:15:45.748 1a38 Recovering log #3.2023/02/07-18:15:45.749 1a38 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF625595.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.2319781134153125
Encrypted:	false
SSDEEP:	6:kfrlL+q2PN72nKuAl9OmbnIFUtWr1ZmwYWLVkwON72nKuAl9OmbjLJ:kpyvVaHAahFUtm/rR5OaHAaSJ
MD5:	B23E47A4D4EB85FD1B0B4CFBE6450E55
SHA1:	E5B5D7383902D7E1DA4EAEBCFAC54537BB343AF8
SHA-256:	E538117601AB9E303FEB2C61C2140DED3C04B25D6B7F596308B4F54FA7AACFAB
SHA-512:	72EEE59169C9AFA5870249D2C3C8813794EFBB7C7E963A7129FB8D83B6CED29C564F1DE3560D50F515E616086439BC766F1EEC6B94B2F81386A2EBFB2BCD8C5
Malicious:	false
Preview:	2023/02/07-18:15:45.557 1a38 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/02/07-18:15:45.748 1a38 Recovering log #3.2023/02/07-18:15:45.749 1a38 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.007641423717476314
Encrypted:	false
SSDEEP:	3:ImtV+2FSn/eElwllx3nOtWGY4/l/ogpn:liV+2EnWMwlr1AtwSn
MD5:	3F4457782C9CC9EEBE17F9895C9FD967
SHA1:	FF92114B4748B5B7D6E9C030A19F243B407A6AF6
SHA-256:	A2A5204132052D33F1CDA90EE648CC06172A18BD3984AC82496C329AABEABA06
SHA-512:	21A6B08D5E0A31A2AB11605971A7F721234251F77D63100E665CE84AC0187E28312448A5ACF03044C4553F7085626CF7C97389F95D98519650C98E6DA0BE17AA
Malicious:	false
Preview:	VLnk.....?.....`.N.7..... ....

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 3024000, file counter 12, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 12
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.567298623060756
Encrypted:	false
SSDEEP:	384:3e59dThWtELJ8fwRRwZsLRGlKhsvXh+vSc:PkYZsLQhUSc
MD5:	87F11CE38578BC1773742B6D30DD1BA2
SHA1:	D53B6198A4DCE68E8483F1F66FD0F17B3E570483
SHA-256:	498666647A77BD9F188E5663EE98724BD193A959A2713D64A40F2991C51C6A8C
SHA-512:	394B2BDA1CE6E1226073086918285090 60F5A64D64699332C42F512D6494A061B10446A4E5F2892BB13E42180F56EE43DE9F93026D403EA16EB40B0A7E4455CB
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....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):	3.203006071963547
Encrypted:	false
SSDEEP:	48:7Mspdom1CiiomAom1Nom1Aiom1RROiom1Bom1pom1FZiomVPiomgdqQlmFTIF3XY:7MiihSCPdN49IVXEBodRBkX
MD5:	8E93F79AC41AA300DAA0223DD3AFCA11
SHA1:	F6E9AF70671FD520F19CC8A0550931B8ADEA5E96
SHA-256:	B9EEBD0E5AC9DB46777F74EEFEBB1CAD2B5DCFEAD2278E0EA256B6D8815D076C
SHA-512:	13F7BC52EDB5E2C4EF1F3B155454D224D07FCED0AEF7DF7F96E1C388F231B08E5E1576E29082F199BBD03EC6C3E519EAD49F2B37D76C9C68EC86204C8DE4B24
Malicious:	false
Preview:	.... .c.....fe.....X.. .L...y.....~.....

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):	63598
Entropy (8bit):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZ0kXVys3DlfOH8V44PDOj6YBmYyu:J0GpiyVFiB0kXVyszprOj64mK
MD5:	8913F7C82AABF8F95358CBF9C91FAC33
SHA1:	AE669715013FCB35E17C57BBA27D894CD5F851F0
SHA-256:	EF8BFBB5F51FA3A2A7F516C7336711E82B08D1E86CE0D6E4EC8AA108AD763855
SHA-512:	066498D112E979D8A7F21CDBFB7770BC0828B5A19B8520C081E51A14F4D71B10BD305FC3C5F522B8FCFC24721807A1E9EDFA3E088D76764B9418AAA04FF556A0
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.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-B

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

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	22024
Entropy (8bit):	5.140349574159579
Encrypted:	false
SSDEEP:	192:O5j5JS1p/1/mLm+4n61N9iuD2tVA01fj/u9QZs2BIjUA:aj5JMp/1/mLm+4n61N9iuKrXMjUA
MD5:	16F96A3C9F75884C826BDEC82AF6891C
SHA1:	6E835BC743BEFC10D3E1FF617793AB1E7C98DEAF
SHA-256:	FC617AE99D52AFB5B76AEAD86EF320A8B440C39DDC8FA131B9235066B3B59035
SHA-512:	CAD21125F6E554B7FF3855D5D1C4F18AC4F1361219972144A52B619C06E27A91E3AE001B8E3CA526A224171882E756C8FF9EFCB3B308672F797B98CFC11B44B4
Malicious:	false
Preview:	.2023-02-07 18:14:58.159 Log opened. (Time zone: UTC-08:00)..2023-02-07 18:14:58.159 Setup version: Inno Setup version 6.0.4 (u)..2023-02-07 18:14:58.159 Original Setup EXE: C:\Users\user\Desktop\FileOpenInstaller.exe..2023-02-07 18:14:58.159 Setup command line: /SL5="$10404,6054369,1320960,C:\Users\user\Desktop\FileOpenInstaller.exe" ..2023-02-07 18:14:58.159 Windows version: 10.0.17134 (NT platform: Yes)..2023-02-07 18:14:58.159 64-bit Windows: Yes..2023-02-07 18:14:58.159 Processor architecture: x64..2023-02-07 18:14:58.159 User privileges: Administrative..2023-02-07 18:14:58.503 Administrative install mode: Yes..2023-02-07 18:14:58.503 Install mode root key: HKEY_LOCAL_MACHINE..2023-02-07 18:14:58.503 64-bit install mode: Yes..2023-02-07 18:14:58.565 Created temporary directory: C:\Users\user\AppData\Local\Temp\is-IORDB.tmp..2023-02-07 18:14:58.612 -- DLL function import --..2023-02-07 18:14:58.612 Function name: OpenSCManagerW..2023-02-07

C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp

Process:	C:\Users\user\Desktop\FileOpenInstaller.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3119936
Entropy (8bit):	6.073128166324036
Encrypted:	false
SSDEEP:	49152:IR/KpmZubPf2S8W2ILeWl+C1p9jWy5Mnd0wigbLNDH:O/jtYLP1Sy5i0qH
MD5:	B7988AC379CEAA456BAA3EF19EB55263
SHA1:	15C13A91E64739C76FF48E20C5BB4182AAD94339
SHA-256:	69383793D354F2A95D88F610B0559F321F37C97197554CD1E9D6D30B038C352D
SHA-512:	22D4544911F496B22AF502869CBDFBC371617A418EB8010319D1842A862F84CA2CA23F1BE505C5F03BD404CB2EE5E489B1FE86B3047356ACE3965F5494AA9FA6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\Local\Temp\is-IORDB.tmp\UtilDll.dll

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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-IORDB.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-0FUR6.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\Roaming\FileOpen\Fowpmadi.txt

Process:	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe
File Type:	data
Category:	dropped

Size (bytes):	60
Entropy (8bit):	5.706890595608517
Encrypted:	false
SSDEEP:	3:ITgt6puhvyyWI2QqH5ArxvlAbkdsn:14uYPXe10kGn
MD5:	2FF5675330538466AC994512DF4ECD00
SHA1:	7DB064334A9342A5C5C97FFF02DC4E41C2AA4EF8
SHA-256:	7F0C0E2518D73DD376E01D066E87F51A34B6F23E98261E3FB01D43BD9DBFD338
SHA-512:	8C22FDF8A005297C6192A6C640DE1843EDAA52510DB0A0420CCCD46DB8976D750F9D54EFF93616F5F18DFAC218C3DB70063AEB711D774DE018CEEBCCFBD24 F3
Malicious:	false
Preview:	.e.Ts...c.h...&.....1:..`..}...uj5..e.T.........<ir'...

C:\Windows\Logs\waasmedic\waasmedic.20230208_021515_685.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	2.734158347135719
Encrypted:	false
SSDEEP:	48:xij1nAr52QH5Wb7kUHb7kENb7klsb7kjb7kbIl9ljb7k0tpl5Cb7kYb7k9b7kwId:xf2eA0UH0W0q0j0U9x0ClA0Y090d109O
MD5:	AC566C1713FE89AD450375CAEE4D5272
SHA1:	05F99F32D98421DE2F152AE2F4F05386CAAC397E
SHA-256:	B005894BC1F6D41DF25CC7B2697A28FE74B88FD738CA19F96A2A5804F276C53C
SHA-512:	D0DF46C9F801ED67E728B38BFDFBD8D0FE480E7EA3D95A6A55010E622D077989FEB031BA4B089315A66E7E7B3A71BC516B32908522CB44FF08D48BA01196675 9
Malicious:	false
Preview:	....!...............................D....&v.....................B........Rc;..Zb....... ....@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... .....]...c;..........E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:. \.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.3.0.2.0.8._.0.2.1.5.1.5._.6.8.5...e.t.l............P.P.....D....&v..9.B. .&v.....17134.1.amd64fre.rs4_release.180410-1804............5.@..&v.....OYo."(.s..O........WaaSMedicSvc.pdb... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.171024618297729
Encrypted:	false
SSDEEP:	192:cY+38+DJ5+inJg3+igJU+LY+XY+ntn+E5L+MQ+7:j+s+j+j3+12+0+I+9+C+b+7
MD5:	B3867667FD78121A3D480FAF35FE791D
SHA1:	DE8F33E392F49195542F3DB2FC023119072AFE3E
SHA-256:	0262501B23D931D43A30D35F9C84F3DF1A22346B6BC06057071E9D4862DED206
SHA-512:	757AAB98CC6DAC521051519AD7BFF9968B428A079CCDDAA31BDC6C5976BAC1BB4E91378C67C072DD4E5C28C20DEE5D981CF43B8221EB989551BBF6F407E78 3BD
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20230208_021514_186.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3937878802200334
Encrypted:	false
SSDEEP:	96:liCLgo+IJV5I59G/YmXCu4I2lWlkle4usT2KjFzaUMCq6JR4Y5Y:P0uusA22uB7Clg
MD5:	6BE542DB315355FA3F622F8E952BE3E4
SHA1:	FBAD2A7171B38E06CBAFD28F49999B97530F4AD5

SHA-256:	6EABEAD9F737391797A5C756CACD8FD0B083D9F5D9AC696D70747E112803044E
SHA-512:	2E3C798B933948DC0056BB1854ABE65A807AE95BABF9EC80C39030D115B0FC3456FE9D62C2FDE63D1E542A7814B2B3B17086E40C4F9A2EE3D30165E1E96F805 0
Malicious:	false
Preview:	....!.....~E.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....7..-c;.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.: .\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o .s.v.c...2.0.2.3.0.2.0.8._.0.2.1.5.1.4._.1.8.6...e.t.l.....P.P.....~E..... .....

Static File Info

General

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

File Icon

Icon Hash:	c0d4d4d4d4d4dc60

Static PE Info

General

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

Authenticode Signature

Signature Valid:	**true**

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

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax
mov eax, 004B10D8h
call 00007F596C9BDD35h
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 00007F596CA60447h
call 00007F596CA5FF9Eh
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F596C9D37A8h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D3Ch
call 00007F596C9B8927h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D3Ch]
mov dl, 01h
mov eax, dword ptr [004237A4h]
call 00007F596C9D480Fh
mov dword ptr [004C1D40h], eax
xor edx, edx

Instruction
push ebp
push 004B6546h
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007F596CA604CFh
mov dword ptr [004C1D48h], eax
mov eax, dword ptr [004C1D48h]
cmp dword ptr [eax+0Ch], 01h
jne 00007F596CA66ACAh
mov eax, dword ptr [004C1D48h]
mov edx, 00000028h
call 00007F596C9D5104h
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
.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

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

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

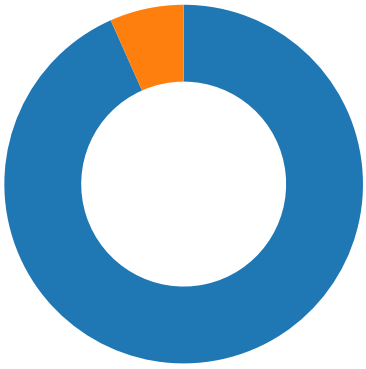
Name	Ordinal	Address
TMethodImplementationIntercept	3	0x454058
__dbk_fcall_wrapper	2	0x40d0a0
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 30

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:15:36.625793934 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:36.625869989 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:36.625977993 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:36.656014919 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:36.656064987 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.085699081 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.085906982 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:37.603049040 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:37.603085041 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.603477955 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.603568077 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:37.611975908 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:37.612005949 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.612051010 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:37.612057924 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.998322010 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.998418093 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:37.998506069 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:38.004544973 CET	49736	443	192.168.2.6	72.3.136.136
Feb 7, 2023 18:15:38.004566908 CET	443	49736	72.3.136.136	192.168.2.6
Feb 7, 2023 18:15:38.144870043 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.144923925 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.144996881 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.145864964 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.145890951 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.576445103 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.576692104 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.581419945 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.581469059 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.581862926 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.582032919 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.582719088 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.582740068 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.723304033 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.723397970 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.723464966 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.723464966 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.726723909 CET	49737	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.726803064 CET	443	49737	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.851418972 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.851485014 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:38.851602077 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.852103949 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:38.852133036 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.132622004 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.135246992 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:39.148889065 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:39.148916960 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.152877092 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:39.152893066 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.449879885 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.450017929 CET	443	49738	72.3.136.132	192.168.2.6
Feb 7, 2023 18:15:39.450186968 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:39.504117012 CET	49738	443	192.168.2.6	72.3.136.132
Feb 7, 2023 18:15:39.504168987 CET	443	49738	72.3.136.132	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:15:36.576718092 CET	59082	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:15:36.613837004 CET	53	59082	8.8.8.8	192.168.2.6
Feb 7, 2023 18:15:38.121723890 CET	59504	53	192.168.2.6	8.8.8.8
Feb 7, 2023 18:15:38.141752958 CET	53	59504	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:15:36.576718092 CET	192.168.2.6	8.8.8.8	0xf3e0	Standard query (0)	usr.fileopen.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:15:38.121723890 CET	192.168.2.6	8.8.8.8	0x5772	Standard query (0)	plugin.fileopen.com	A (IP address)	IN (0x0001)	false

DNS Answers

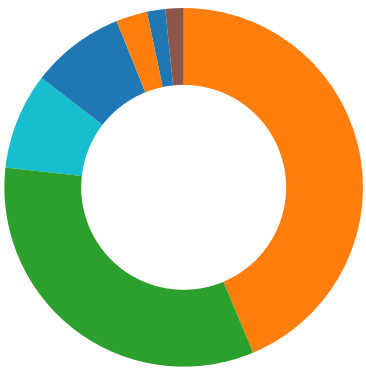
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:15:36.613837004 CET	8.8.8.8	192.168.2.6	0xf3e0	No error (0)	usr.fileopen.com		72.3.136.136	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:15:38.141752958 CET	8.8.8.8	192.168.2.6	0x5772	No error (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



- FileOpenInstaller.exe
- FileOpenInstaller.tmp
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- sc.exe
- conhost.exe
- FileOpenManager64.exe
- FileOpenBroker64.exe
- AcroRd32.exe
- FileOpenBroker64.exe
- RdrCEF.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: FileOpenInstaller.exe PID: **4844**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:14:55
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: **2380**, Parent PID: **4844**

General

Target ID:	1
Start time:	18:14:56
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-0FUR6.tmp\FileOpenInstaller.tmp" /SL5="$10404,6054369,1320960,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-IORDB.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-IORDB.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-IORDB.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-IORDB.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-BU7MM.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-LL3TI.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-SJIP9.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-U9E22.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-KGJ5A.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-GL49N.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
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-EBO4V.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-F9Q7I.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5B6BB2	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\L10n\is-F36NO.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-ESNP0.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-OPHGC.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-AKGRI.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-UGF2P.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-BSLJ5.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-0GB27.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-696VR.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-3GDF5.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-1DS3V.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-IORDB.tmp\UtilDll.dll	success or wait	1	5F77F0	DeleteFileW
C:\Users\user\AppData\Local\Temp\is-IORDB.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-BU7MM.tmp	C:\Program Files\FileOpen\unins000.exe	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\is-LL3TI.tmp	C:\Program Files\FileOpen\UtilDll.dll	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\examples\is-SJIP9.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-U9E22.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-KGJ5A.tmp	C:\Program Files\FileOpen\Services\FileOpenBroker64.exe	success or wait	1	5F7B77	MoveFileW
C:\Program Files\FileOpen\Services\is-GL49N.tmp	C:\Program Files\FileOpen\Services\FileOpenManager64.exe	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-EBO4V.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_de.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-F9Q7I.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_fr.lcd	success or wait	1	5F7B77	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\FileOpen\Updates\L10n\is-F36NO.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_ja.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\L10n\is-ESNP0.tmp	C:\ProgramData\FileOpen\Updates\L10n\fotk_zh.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-OPHGC.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-AKGRI.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-UGF2P.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-BSLJ5.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-0GB27.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-696VR.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-3GDF5.tmp	C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	success or wait	1	5F7B77	MoveFileW
C:\ProgramData\FileOpen\Updates\Lists\is-1DS3V.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 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	136	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	231	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	357	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	432	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	479	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	534	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 31 35 39 20 20 20	2023-02-07 18:14:58.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	593	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 35 30 33 20 20 20	2023-02-07 18:14:58.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	653	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 35 30 33 20 20 20	2023-02-07 18:14:58.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	722	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 35 30 33 20 20 20	2023-02-07 18:14:58.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	774	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 35 36 35 20 20 20	2023-02-07 18:14:58.565	success or wait	3	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-IORDB.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 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.$^I=\=\=\RichPEdR#	success or wait	1	420DE1	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	880	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	144	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	933	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	72	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	990	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	72	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1040	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	63	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	1150	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	63	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	4593	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 36 31 32 20 20 20	2023-02-07 18:14:58.612	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\is-IORDB.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 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.$|pppuspuunputpmtpmspmupuqpqpNlypNlppNlppNlrpRichp	success or wait	4	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	9752	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 34 3a 35 38 2e 38 31 35 20 20 20	2023-02-07 18:14:58.815	success or wait	27	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10382	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 31 31 32 20 20 20	2023-02-07 18:15:24.112	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10425	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 31 31 32 20 20 20	2023-02-07 18:15:24.112	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10923	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 31 35 39 20 20 20	2023-02-07 18:15:24.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	10979	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 32 30 36 20 20 20	2023-02-07 18:15:24.206	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11022	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 32 30 36 20 20 20	2023-02-07 18:15:24.206	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11520	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 32 35 33 20 20 20	2023-02-07 18:15:24.253	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11595	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 32 35 33 20 20 20	2023-02-07 18:15:24.253	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11658	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 33 31 35 20 20 20	2023-02-07 18:15:24.315	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11718	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 33 31 35 20 20 20	2023-02-07 18:15:24.315	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11806	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 33 36 32 20 20 20	2023-02-07 18:15:24.362	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	11868	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 33 36 32 20 20 20	2023-02-07 18:15:24.362	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12301	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 33 36 32 20 20 20	2023-02-07 18:15:24.362	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12374	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 30 39 20 20 20	2023-02-07 18:15:24.409	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12458	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 30 39 20 20 20	2023-02-07 18:15:24.409	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12552	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 35 36 20 20 20	2023-02-07 18:15:24.456	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12596	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 35 36 20 20 20	2023-02-07 18:15:24.456	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12677	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 35 36 20 20 20	2023-02-07 18:15:24.456	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12732	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 35 36 20 20 20	2023-02-07 18:15:24.456	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	12807	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 34 35 36 20 20 20	2023-02-07 18:15:24.456	success or wait	3	5B6D0C	WriteFile
C:\Program Files\FileOpen\is-BU7MM.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 49 6e 55 6e 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@InUn!L!This program must be run under Win32$7	success or wait	191	5B6D0C	WriteFile
C:\Program Files\FileOpen\is-BU7MM.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	12855	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 30 36 20 20 20	2023-02-07 18:15:24.706	success or wait	3	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 31 35 3a 32 34 2e 37 30 36 20 20 20	2023-02-07 18:15:24.706	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	12959	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 30 36 20 20 20	2023-02-07 18:15:24.706	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13039	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 30 36 20 20 20	2023-02-07 18:15:24.706	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13114	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 30 36 20 20 20	2023-02-07 18:15:24.706	success or wait	51	5B6D0C	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\FileOpen\is-LL3TI.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 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 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	13162	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 35 33 20 20 20	2023-02-07 18:15:24.753	success or wait	51	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13486	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 37 35 33 20 20 20	2023-02-07 18:15:24.753	success or wait	12	5B6D0C	WriteFile
C:\Program Files\FileOpen\examples\is-SJIP9.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 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	13628	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 38 36 32 20 20 20	2023-02-07 18:15:24.862	success or wait	30	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	13715	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 34 2e 38 36 32 20 20 20	2023-02-07 18:15:24.862	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-U9E22.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.$1}}}}y	success or wait	35	5B6D0C	WriteFile
C:\Program Files\FileOpen\Services\is-KGJ5A.tmp	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 67 fd fd fd 09 c5 fd 09 c5 fd 09 d1 fd 0d 96 fd 09 d1 fd 0a 8a fd 09 d1 fd 0c fd 4c fd 09 fd e7 0d 96 fd 09 fd e7 0a 8f fd 09 d1 fd 0f 84 fd 09 fd e7 0c fd fd fd 09 e2 14 74 c7 fd 09 e2 14 67 d0 fd 09 d1 fd 08 9c fd 09 c5 fd 08 fd fd fd 09 fd 39 fd 0d 84 fd 09 fd 39 fd 0c af fd 09 fd 39 fd 09 84 fd 09	MZ@(!L!This program cannot be run in DOS mode.$gLtg999	success or wait	32	5B6D0C	WriteFile
C:\Program Files\FileOpen\Services\is-GL49N.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	15505	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 32 30 36 20 20 20	2023-02-07 18:15:26.206	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	15576	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 32 30 36 20 20 20	2023-02-07 18:15:26.206	success or wait	3	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\L10n\is-EBO4V.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-F9Q7I.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 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-F36NO.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&00010000000000440000249600012824wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zQFBKRDtypz8MHsvOxXIrTrvHwI3gUHxIekwE6otym/yHbUZP7PIEy8O/bpGxW6LzHtWOK3fYHRItpDgBaA5X1AXvY2BO/XOfKySo1Db21+lg3//wtfYGiYOORGAUa1z2iam5ELO3M+r0ktrNKBZRnxIzECsQsuEa/+1aid	success or wait	1	5B6D0C	WriteFile
C:\ProgramData\FileOpen\Updates\L10n\is-ESNP0.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&00010000000000440000249600007596wfNamiz0xzddKQHtypz8XHsvOxPIrTqsHwI3kUHxIZw=wfNamzz0zS9BKRDtypz8MHsvOxXIrTqMHwI3gUHxIekwE6otym/yTbUZP7PIEy8O/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-OPHGC.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-AKGRI.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-UGF2P.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-BSLJ5.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-0GB27.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-696VR.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-3GDF5.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-1DS3V.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	19393	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19441	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19538	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19592	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19648	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19706	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19772	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	19829	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	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	19925	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20070	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20127	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20203	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 30 33 20 20 20	2023-02-07 18:15:26.503	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 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 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 fd 6b 5b fd	k[	success or wait	12	5B6D0C	WriteFile
C:\Program Files\FileOpen\unins000.dat	25096	12	7a 0c 00 00 fd fd fd fd 69 5e fd	zi^	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	20282	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 35 36 35 20 20 20	2023-02-07 18:15:26.565	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20341	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 36 31 32 20 20 20	2023-02-07 18:15:26.612	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20384	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 36 31 32 20 20 20	2023-02-07 18:15:26.612	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20432	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 36 31 32 20 20 20	2023-02-07 18:15:26.612	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20470	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 36 31 32 20 20 20	2023-02-07 18:15:26.612	success or wait	12	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20534	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 36 2e 36 31 32 20 20 20	2023-02-07 18:15:26.612	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	20680	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 37 2e 30 30 33 20 20 20	2023-02-07 18:15:27.003	success or wait	9	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21408	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 38 2e 37 35 33 20 20 20	2023-02-07 18:15:28.753	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21588	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 32 39 2e 39 30 39 20 20 20	2023-02-07 18:15:29.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21643	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 32 2e 39 30 39 20 20 20	2023-02-07 18:15:32.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21686	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 32 2e 39 30 39 20 20 20	2023-02-07 18:15:32.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21735	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 32 2e 39 30 39 20 20 20	2023-02-07 18:15:32.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21773	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 32 2e 39 30 39 20 20 20	2023-02-07 18:15:32.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21877	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 32 2e 39 30 39 20 20 20	2023-02-07 18:15:32.909	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21936	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 33 2e 31 35 39 20 20 20	2023-02-07 18:15:33.159	success or wait	3	5B6D0C	WriteFile
C:\Users\user\AppData\Local\Temp\Setup Log 2023-02-07 #001.txt	21985	26	32 30 32 33 2d 30 32 2d 30 37 20 31 38 3a 31 35 3a 33 34 2e 36 31 32 20 20 20	2023-02-07 18:15:34.612	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-0FUR6.tmp\FileOpenInstaller.tmp	unknown	16384	success or wait	1	5B6C3C	ReadFile
C:\Users\user\AppData\Local\Temp\is-0FUR6.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

Analysis Process: svchost.exe PID: **5916**, Parent PID: **576**

General

Target ID:	2
Start time:	18:14:57
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4072**, Parent PID: **576**

General

Target ID:	3
Start time:	18:15:11
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **4808**, Parent PID: **576**

General

Target ID:	4
Start time:	18:15:13
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
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: svchost.exe PID: **2840**, Parent PID: **576**

General

Target ID:	5
Start time:	18:15:13
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4608**, Parent PID: **576**

General

Target ID:	6
Start time:	18:15:14
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **2376**, Parent PID: **576**

General

Target ID:	7
Start time:	18:15:14
Start date:	07/02/2023
Path:	C:\Windows\System32\SgrmBroker.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7f3510000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4384**, Parent PID: **576**

General

Target ID:	8
Start time:	18:15:15
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5444**, Parent PID: **576**

General

Target ID:	9
Start time:	18:15:15
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3672**, Parent PID: **576**

General

Target ID:	10
Start time:	18:15:15
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5372**, Parent PID: **576**

General

Target ID:	12
Start time:	18:15:24
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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: sc.exe PID: **6164**, Parent PID: **2380**

General

Target ID:	13
Start time:	18:15:26
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:	0x7ff732c00000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
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: 6172, Parent PID: 6164

General

Target ID:	14
Start time:	18:15:26
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6208, Parent PID: 2380

General

Target ID:	15
Start time:	18:15:27
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:	0x7ff732c00000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
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: 6216, Parent PID: 6208

General

Target ID:	16
Start time:	18:15:27

Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: **6256**, Parent PID: **2380**

General

Target ID:	17
Start time:	18:15:27
Start date:	07/02/2023
Path:	C:\Windows\System32\sc.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\sc.exe" start FileOpenManager
Imagebase:	0x7ff732c00000
File size:	69120 bytes
MD5 hash:	D79784553A9410D15E04766AAAB77CD6
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: **6264**, Parent PID: **6256**

General

Target ID:	18
Start time:	18:15:27
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: FileOpenManager64.exe PID: **6300**, Parent PID: **576**

General

Target ID:	19
Start time:	18:15:27
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:	0x7ff7967a0000
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: **6352**, Parent PID: **2380**

General

Target ID:	20
Start time:	18:15:28
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:	0x7ff72bd90000
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	7FF72BEF2040	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	7FF72BEF2040	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	7FF72BEF2040	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	7FF72BEF2040	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	7FF72BF03344	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	7FF72BEF2040	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	7FF72BEF2040	CreateDirectoryW

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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	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	7FF72BE58343	HttpSendRequestA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FileOpen\Fowpmadi.txt	0	60	fd 65 fd 54 73 fd fd 08 63 3e 68 0b 04 12 26 fd fd fd fd 2e 31 3a fd fd 60 9e fd 7d 91 14 13 75 6a 35 a2 fd 65 fd 54 0a fd fd fd fd 1e fd fd 17 3c 69 72 27 fd fd fd	eTsch&.1:`}uj5eT<ir'	success or wait	1	7FF72BEF4074	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	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\FileOpen	success or wait	1	7FF72BE55DE9	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\FileOpen	success or wait	1	7FF72BE55E49	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\FileOpen\FileOpenClient	success or wait	1	7FF72BE55E49	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\FileOpen	Fowp3Uuid	binary	DC 65 8E 54 73 F1 CD D8 88 63 C8 BE 68 0B 04 12 26 A6 9B A8 FA 2E 31 3A A7 CE 60 C2 9E B3 7D DE 91 14 13 75 6A 35 D2 A2	success or wait	1	7FF72BE57964	RegSetValueExA
HKEY_CURRENT_USER\Software\FileOpen	Fowp3Madi	binary	DC 65 8E 54 0A 9C B3 BD 8F 1E FE C1 17 3C 69 72 27 DB E8 DB	success or wait	1	7FF72BE57992	RegSetValueExA

Analysis Process: AcroRd32.exe PID: **6416**, Parent PID: **2380**

General

Target ID:	21
Start time:	18:15:32
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:	0xaa0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
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	success or wait	1	AD65C3	CreateDirectoryExW
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	success or wait	1	AFAE05	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	B683C8	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	B683C8	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	B683C8	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	B683C8	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	B683C8	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	B683C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1nwtagc_1ezoe21_500.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	AEEA85	NtCreateFile
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	4	AEEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rtzospe_1ezoe22_500.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	AEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1hk3mc9_1ezoe23_500.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	AEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rktd1y8_1ezoe24_500.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	AEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rq4jo1s_1ezoe25_500.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	AEEA85	NtCreateFile

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	AECF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	AED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	AED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	AED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	AAEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	AAEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	AAEA55	RegCreateKeyExW

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	AFDF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Program Files/FileOpen/examples/installcomplete.pdf	success or wait	1	AFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	installcomplete.pdf	success or wait	1	AFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	AFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	AFDF69	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	AFDF69	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 31 35 34 33 2D 30 38 27 30 30 27 00	success or wait	1	AFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	162991	success or wait	1	AFDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	AFDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	AFDF47	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	AFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	AFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	AFDF69	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	AFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 32 35 34 33 36 2D 30 37 27 30 30 27 00	success or wait	1	AFDF69	RegSetValueExW

Analysis Process: FileOpenBroker64.exe PID: **6576**, Parent PID: **3452**

General

Target ID:	22
Start time:	18:15:37
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:	0x7ff72bd90000
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	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLsts.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkLngs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkCnfs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkDrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkPrs.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkRds.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkNis.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile
C:\ProgramData\FileOpen\Updates\Lists\fotkBus.lcd	unknown	4096	success or wait	1	7FF72BEF2CF1	ReadFile

Analysis Process: RdrCEF.exe PID: **6624**, Parent PID: **6416**

General

Target ID:	23
Start time:	18:15:38
Start date:	07/02/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0x1370000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	3	14783E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	19	1478447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	161	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	14659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	18	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	5	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	12	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1633	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	5	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	17	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	17	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	40	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	44	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	166	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	8	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	87	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	15	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	14	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	323	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	44	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	14	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	14659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	14	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	179	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	207	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	198	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	3	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	32	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	7	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	4	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	2	14659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	7	14659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	1	14659E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	14783E5	ReadFile

Analysis Process: svchost.exe PID: **6232**, Parent PID: **576**

General

Target ID:	24
Start time:	18:15:54
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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: svchost.exe PID: **1128**, Parent PID: **576**

General

Target ID:	27
Start time:	18:16:04
Start date:	07/02/2023
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff603c50000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **5340**, Parent PID: **3672**

General

Target ID:	30
Start time:	18:16:16

Start date:	07/02/2023
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6977b0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF6977DBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 31 00 36 00 3a 00 31 00 36 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Tue Feb 07 2023 18:16 :16	success or wait	1	7FF6977DBC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF6977DBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF6977DBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF6977DBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 31 00 36 00 3a 00 31 00 36 00 0d 00 0a 00	MpCmdRun: End Time: Tue Feb 07 2023 18:16:16	success or wait	1	7FF6977DBC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF6977DBC96	WriteFile

Analysis Process: conhost.exe PID: **5456**, Parent PID: **5340**

General

Target ID:	31
Start time:	18:16:16
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Disassembly

No disassembly