ID: 412658
Sample Name: Covid screening questionaire.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 20:49:12
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

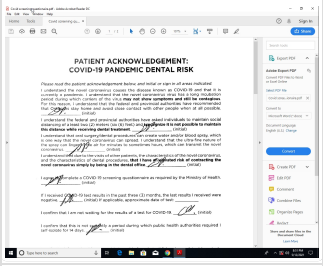
Analysis Report Covid screening questionaire.pdf

Overview

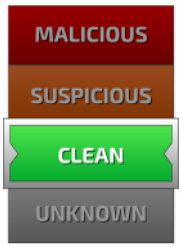
General Information

Sample Name:	Covid screening questionaire.pdf
Analysis ID:	412658
MD5:	e87f93f286ff7cc5..
SHA1:	099b509e715dbb..
SHA256:	12b425e76752e7..
Infos:	

Most interesting Screenshot:



Detection

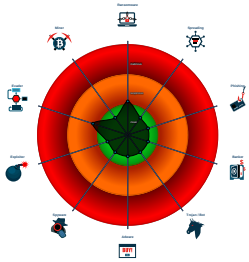


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to access load…
- IP address seen in connection with o…
- PDF has an OpenAction (likely to la…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 6480 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Covid screening questionaire.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6548 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Covid screening questionaire.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6816 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7032 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16739402187565574225 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=16739402187565574225 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7064 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=15525037812135764353 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7132 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=844945410949651913 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=844945410949651913 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4240 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=357690743904107764 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=357690743904107764 --renderer-client-id=5 --mojo-platform-channel-handle=2084 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

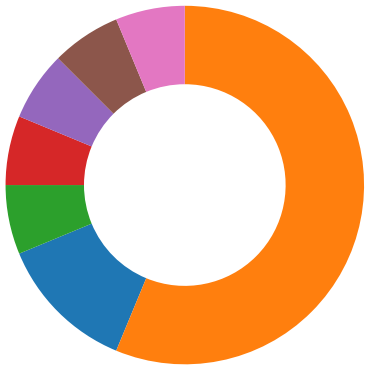
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

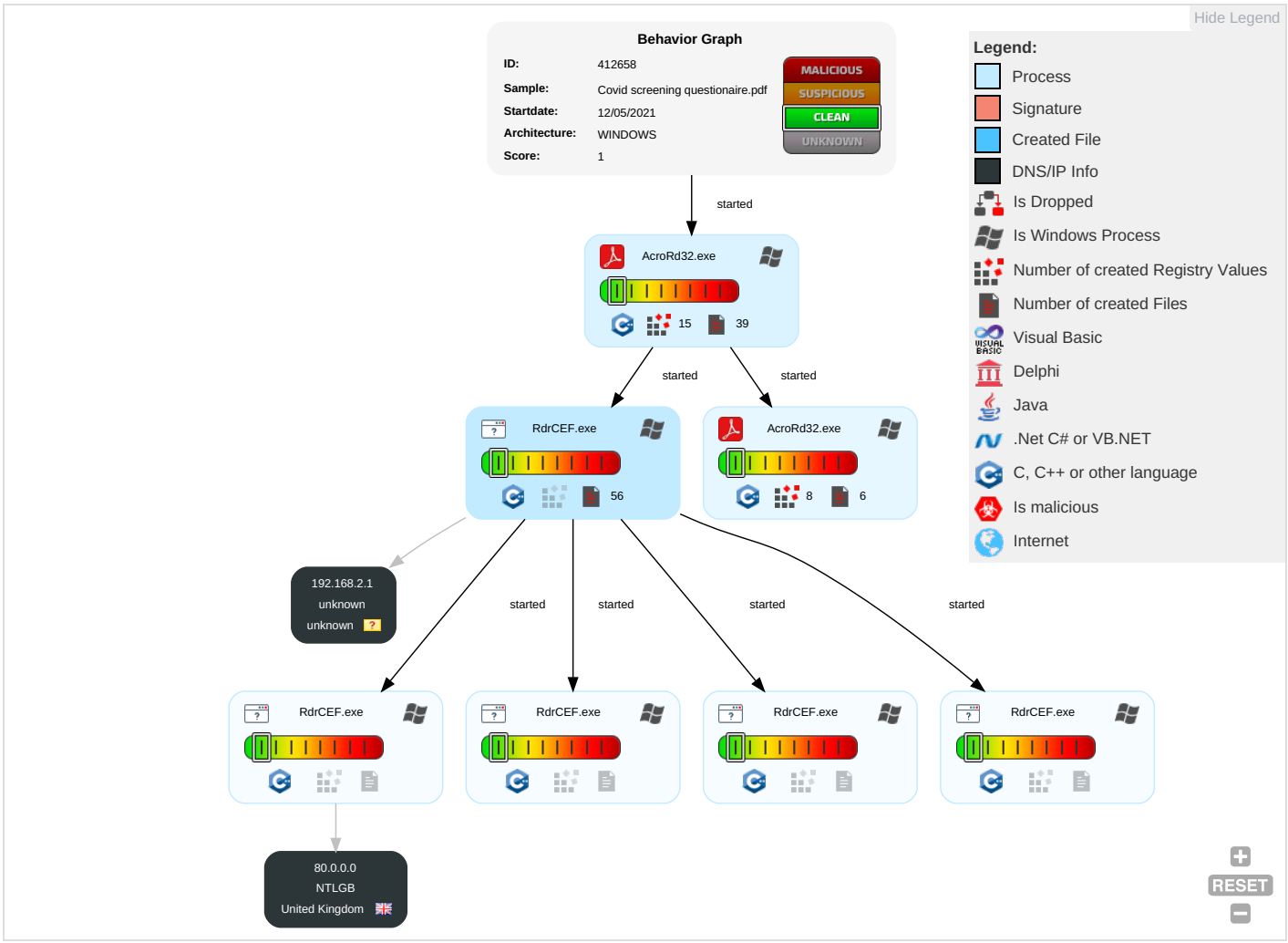
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	In
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

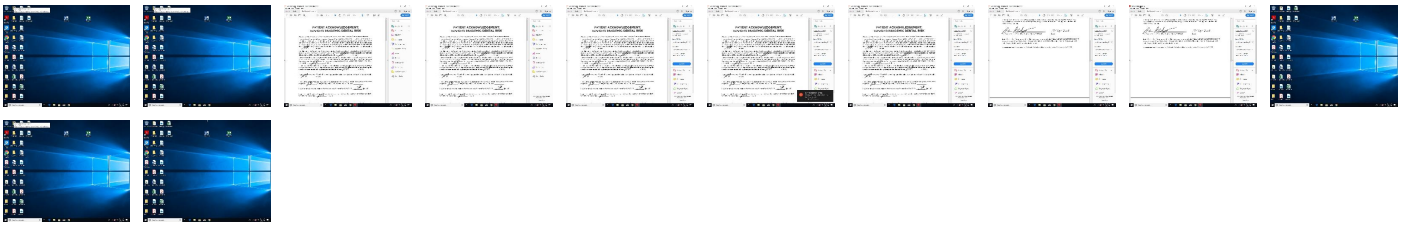
Behavior Graph

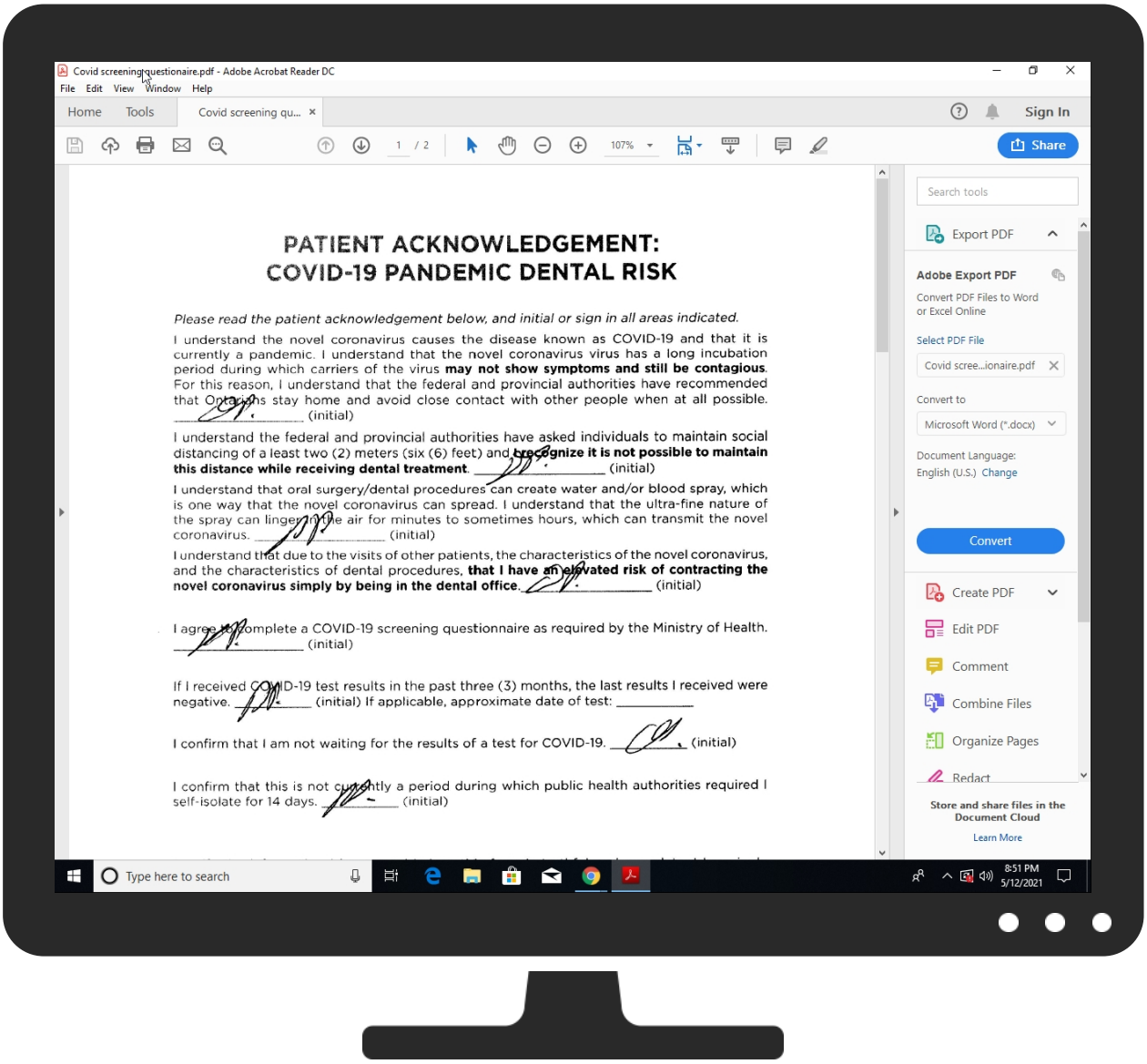


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/i	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://ims-na1.adobelogin.comol	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/d	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/L	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4F	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/S	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/A	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/r	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.adobe.	0%	URL Reputation	safe	
http://www.adobe.	0%	URL Reputation	safe	
http://www.adobe.	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

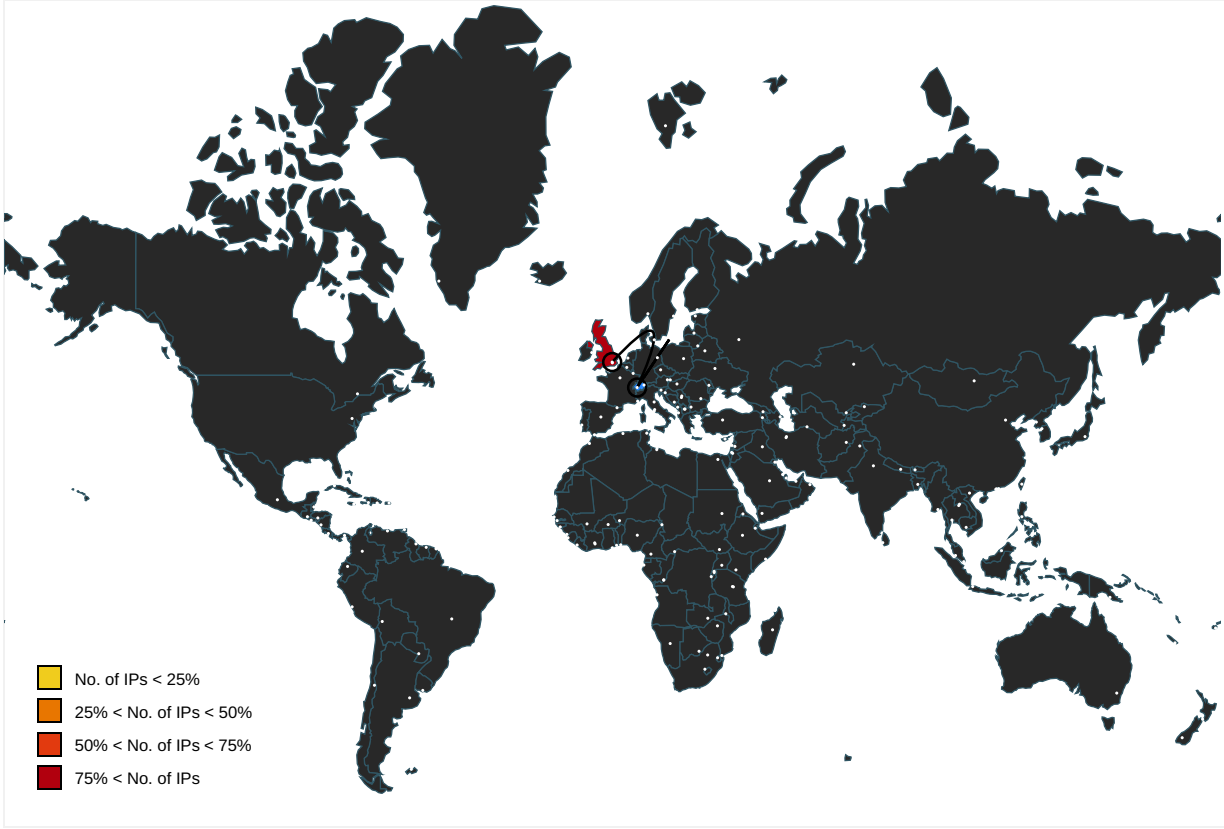
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/)	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/i	AcroRd32.exe, 00000001.00000002.602353615.000000000AFD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.comol	AcroRd32.exe, 00000001.00000002.594582632.0000000008F53000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/d	AcroRd32.exe, 00000001.00000002.602353615.000000000AFD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/L	AcroRd32.exe, 00000001.00000002.600476606.000000000A37F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4F	AcroRd32.exe, 00000001.00000002.600476606.000000000A37F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/schema#B	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/S	AcroRd32.exe, 00000001.00000002.602353615.000000000AFD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfe/ns/id/I	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/A	AcroRd32.exe, 00000001.00000002.602353615.000000000AFD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.604492315.000000000B3A3000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.600476606.000000000A37F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfe/ns/id/P	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false		high
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.602323706.000000000AFBF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comRL	AcroRd32.exe, 00000001.00000002.604492315.000000000B3A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.602353615.000000000AFD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/r	AcroRd32.exe, 00000001.00000002.600476606.000000000A37F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.594582632.0000000008F53000.00000004.00000001.sdmp	false		high
http://www.adobe.	AcroRd32.exe, 00000001.00000002.623213006.0000000011E3C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.589627373.0000000007740000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#M	AcroRd32.exe, 00000001.00000002.603585188.000000000B2BC000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/:	AcroRd32.exe, 00000001.00000002.600476606.000000000A37F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412658
Start date:	12.05.2021
Start time:	20:49:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid screening questionaire.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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
Detection:	CLEAN
Classification:	clean1.winPDF@13/47@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 52.147.198.201, 13.64.90.137, 92.122.145.220, 104.43.139.144, 2.20.142.226, 2.20.142.233, 2.20.142.203, 2.20.143.130, 2.20.142.225, 92.122.146.26, 2.20.142.228, 20.82.209.183, 92.122.213.194, 92.122.213.247, 67.26.137.254, 8.241.126.121, 8.253.207.121, 8.241.79.254, 8.238.85.254, 52.155.217.156, 20.54.26.129, 23.57.80.111, 20.82.210.154 • Excluded domains from analysis (whitelisted): e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, acroipm2.adobe.com, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/412658/sample/Covid screening questionaire.pdf

Simulations

Behavior and APIs

Time	Type	Description
20:50:18	API Interceptor	16x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	XNAFrameworkClassLibrary.pdf	Get hash	malicious	Browse	
	ATT82166.HTM	Get hash	malicious	Browse	
	business agreement.exe	Get hash	malicious	Browse	
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	EiK2ZuecHv.exe	Get hash	malicious	Browse	
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	HunpuKMHQt.exe	Get hash	malicious	Browse	
	JbQoNNPVOk.exe	Get hash	malicious	Browse	
	_vm583573758.htm	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	XNAFrameworkClassLibrary.pdf	Get hash	malicious	Browse	• 80.0.0.0
	ATT82166.HTM	Get hash	malicious	Browse	• 80.0.0.0
	networkservice.exe	Get hash	malicious	Browse	• 86.16.83.28
	business agreement.exe	Get hash	malicious	Browse	• 80.0.0.0
	8UsA.sh	Get hash	malicious	Browse	• 82.32.79.178
	x86_unpacked	Get hash	malicious	Browse	• 82.17.192.153
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	rIbyGX66Op	Get hash	malicious	Browse	• 86.18.93.173
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	J76uxxiy.exe	Get hash	malicious	Browse	• 86.18.99.199
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	EiK2ZuecHv.exe	Get hash	malicious	Browse	• 80.0.0.0
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_Express_Shipment_Confirmation_BKKR005545473_88700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	410
Entropy (8bit):	5.654018499724671
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QlD//trBwi7Z+P41TK6tUF8en9YOFLvEWdM9Q3/PNGwi7Z+P45:vDRM9WRrBLZiECDRM9U9GLZiE
MD5:	DEC335E88D36035E590C4702721CCAD5
SHA1:	ECA1F4A9E515FB639D4E46B2AFBFCC5179213529
SHA-256:	690DABB7025EF80F26A88557736A8EB3DC58158D4792121A58A38F87A60CCACD
SHA-512:	EE15777828DC134D66581A590CA1F38C45F1A4C2ED1D5AB173E447E0904F2024E84021098F70278C746776FF8F871B0C18E5B2EDB964FC477316EE14045CFEAE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .LU.O. /....."#.D)?.('.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....7.j.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .. .P. /....."#.D..y.('.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....6.....

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):	522
Entropy (8bit):	5.602053535195373
Encrypted:	false
SSDEEP:	12:V9z+f9PQgHd9zSlzCV9PQx9zLqi5i9PQ:Xz+f9PQgH/zRV9PQ7zLL5i9PQ
MD5:	688B8DD41C34C35DA4867498F980C0F7
SHA1:	DA214A9B170B24B0A966F5CB17E5E019AC47FCEF
SHA-256:	E3E589AF203FF88B7609C5DE31F6E4DCF25123FF5DB11DA54474CFEDD6C82E4B
SHA-512:	1C437A95A03DAE06D504237861E473C0AE0E752BB24515058231A720E4B7F9A2C16CFB3C3EEEDF2C386BE14DA85B4609DFEB9A867A684B4DAC40B4B7F2169F4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .q..O. /....."#.DDL..('.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....O. /....."#.DU.o.('.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....q.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .<..O. /....."#.D...('.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....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):	492
Entropy (8bit):	5.604216761198642
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFI14lUo6jDyeRVFAFjVFAFCmlUo6jA:tB4v4s4SBtB4v4CmSBA
MD5:	34518FF7C31410A119F9AA4316D88055
SHA1:	AEE30F18EFC6835670FB30836FF109A48671A594
SHA-256:	E7C1EBAF14688007A90E3FF1ABA9FD337AC41B629961BA7B2A1A46ECD596EAC1
SHA-512:	AA365517017C6EBA4336666A2A28BABFFCE4E1A733FC951C5E2F653E4357EDCB13EAFC9152007C7EDE3A947A68C5F00205266575966E1ABEF6EB6B5FEB86A2AF

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Malicious:	false
Reputation:	low
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 ./..O. /....."#.D...('.A..hvDO.N.t@....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....P. /....."#.D]1o.('.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....Z^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.674740600799347
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsg/ll/QoJiWulHyA1TK6ta:IbRkiDplAWussk
MD5:	5F5CF41FA60536A6003C3EC0616527D4
SHA1:	D6B7923DC2F230499A84CFD63FC4F9F6B6CA3D80
SHA-256:	F1114394DC66FB83E6AE588DCFD07CBFC7EF0F9C7B99306B7BC70DFEB582F49B
SHA-512:	EAF06E781F6F89CDC6AE32D6C88FA968B5483D4F690FA305499D168765D87154D3E4972DF1E9F4302838990229F62533426919BCF681B794C037AFAC4EA2B62B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ....O. /....."#.D...('.A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....}J].....

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):	5.5517093475716255
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuqjR+//CgVyh9PT41TK6tt:pyixRueE/KgV41TE
MD5:	AB03215B697DAB407F43A127EFD7A0D0
SHA1:	C902DDE27A25BFAB83ABA218C76DBE0344850758
SHA-256:	9C2D8C72CEA9B9A0CFB6395D79F7395833D1385F0E4DBF365B6AE56B1A48DD18
SHA-512:	0891D6F00BC7B6F819339D4EBD204617EC6E00556D64A04540F91718B782A0096B951555F1DF56F06AD56ACE241033F3D44EC7C36F8B75E084CE59FD9615C01B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..`.P. /....."#.D..q.('.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....t.1.....

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):	5.606624235711296
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQuC/WgjgNLZIl6P41TK6tWD:0RhkwegjgNLZC6
MD5:	284865294CDC9D7245488B83662C53CF
SHA1:	A3A4BF13A9C959A80E2E971805DB22C7E657C49D
SHA-256:	527675C50CBCF1596F7A779B59A4DD928EA31DECDAD76658D7BF1D6CC2629EC1
SHA-512:	381742D1C3FFF02EA88FAAAB79EF5491B8D70E1F70D48AA4ECD4E68865A4E0CA4CD69202B1EE10FCDE887710F415F94F8DAF8A3706A3664063F210E84703906
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....P. /....."#.D.ES.('.A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....Y.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Size (bytes):	209
Entropy (8bit):	5.545254648643579
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQxKl//mkyB6g1TK6tl:2RHRQC//uk41
MD5:	63D0CAB3F2E208CE2E49D28570B846A1
SHA1:	ED0E75CA469945BA882FED887660ED65212F3D22
SHA-256:	AAB914F416106BC98273437DDD14CB5E34E849BF8391B9CA4EF5A45DF955EF44
SHA-512:	C01E07F08AE83712656B4AD6DF3C333A6438C58C43827E31F5F93FDBB2CA78BFCE719F2F6795553018397D61E540B160BC23BADDC687165F7EBADDE16D17CE 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..l.P. /....."#.D..q.('.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....5.B.....

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):	537
Entropy (8bit):	5.619776998478812
Encrypted:	false
SSDEEP:	12:Z5MqIUMuR/EVtr5MHznMuR/Ed/z5MdWeMuR/E:ZSqlNuR/ErSguR/Ed7S0uR/E
MD5:	D6887184F539BCCC2F729B6555964216
SHA1:	EC06E1B6D5F3C4315A4716E23C8A355AFBD75827
SHA-256:	4B8B0C60C7F843B1487DAAB3051B3A70BE7A941A7CAF68070D0C640AB607C7E0
SHA-512:	B5D8C26FAC8BC02A5B887FDAA1D04680FEF2BE4A99282F25A9334B74EA7FE5C98BD57D234882BD3C4F1BE03C6ED447FA613FB9BA0AC34886B0BC7566764A9E E9
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..#.O. /....."#.D....('.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....>|.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....O. /....."#.D.Op.('.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb...._keyhttps ://rna-resource.acrobat.com/base_uris.js ....O. /....."#.D....('.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....\.o.....

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):	5.427085817724821
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtucQ//q1xMby0zBUKSAA1TK6tPt:pRpQ3sMbeZ
MD5:	7BDB7ACFF32E1A3A0F52EC22A48356AB
SHA1:	4ADD0FE1225CF20649C35CB8D4D2C5CF8B9305CC
SHA-256:	9FEFFCD8E28FC3467793B33740D9CD4B5AEAF08E786237FF6D6A5ABC8B90C2A6
SHA-512:	42BD8C942A9DB831D7D188E8FB64E48C8F980CCAF9A587B87A845F63757DD6EE740FBEC91494DE9A635E2BE2E2C44F77ADF337488A3E33EAC34801E45F8491 B
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..s.P. /....."#.DA.r.('.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....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):	531
Entropy (8bit):	5.5641850957306325
Encrypted:	false
SSDEEP:	12:KkXxKMSCvAtUlHJakXxKMSCvnVtUlF/wkXxKMSCvgtUl:KkXxiC4WHJakXxiC9WNwkXxiC4W
MD5:	A3F54427D23B74BE9D244931C5683B14
SHA1:	91B35CA442C40055B3B5D6652CF64D3B6551C8BE
SHA-256:	32D0AB05207A063E91A1DC4532EBBE05430ADB9CACB9B623CBD419CC54E1FDE7
SHA-512:	DB176A17DF5C0A16E3552289D5D6D7302F6B1023044C46BB07D46C9A516432A4A165DFCCDBB688BBAADAB4DF3322F9390FCCF1378348757C5E59D7765528EFI F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .. .O. /...."#.D0f..('.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....6i.....0\r..m.....1.....5... ._keyhttps://rna-resource.acrobat.com/plugins.js ....O. /...."#.DU.o.('.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....X.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ....O. /...."#.D....('.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....A.7p.....

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):	374
Entropy (8bit):	5.5836107687605745
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL1rl/E57yM+VY1TK6tL+9/Ekl9YOFLvEWsfOLDl/2yM+VY1TKl:5h6OL1raEkoFbh6OL9kG
MD5:	66E6ED0D962BE147C369F94A9DE137E9
SHA1:	CB4352D612AB727CEC3F183453B2DA94E252B6EB
SHA-256:	2E5307125E130196E06A355CCA955001C4E66E2739BFB3E88019606B7EAEE9FD
SHA-512:	E090BC9F74E0751D994B39F0630CB16FF63C8021B6D436E1B3F845A32479078085DA924AE49D83A354D651D3ECDE302D74362D23E912489102A5C5DCFC196D2(
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....O. /....."#.DU...('.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....?[.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..].O. /....."#.D..A.('.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....p.....

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):	488
Entropy (8bit):	5.62650088717274
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFw0NbYwSeKaTLnLFmRVFAFjVFAFoHswSeKaTLn:UB4v4w0NswzXLnLFmB4v4oHswzXLn
MD5:	742996CEFDF85D437C061B85613B793A
SHA1:	05F5331E9DDB6607C4F98BA34047F360725A5A14
SHA-256:	02916063126D94FB21007CB2009D5195AD6ADED4882E51F2221D60BAB3574616
SHA-512:	7F6DD50589ACD2505D6E6AE32E2AF5727411725EB9FB13E21DB372321E8FAC71C75787455947AB55F76BFDB1FD8AF7F8F63B9377741ADB51C7D4D9C1BDE37B(1
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 ....O. /....."#.D...('.A.....H...{...2.. /.k`..r4.C. .A..Eo.....A..Eo.....Ee.....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 .Td.P. /....."#.D..v.('.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....(.IY.....

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):	5.5202737354369065
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuuJ/FNCP11TK6tKl:BsR2EseVXCV
MD5:	44FB8FE3DF8F87895781CDBE224C532B
SHA1:	2D13DA47ED67F13A11E2E2BEF77991500A38B214
SHA-256:	9CFF4A5E3B534DB15442840F178816E8CC76934FDAA250DFBFF357EEF0383254
SHA-512:	9FA962F30621D36CB0B0F78D0AFE8BE3D51137704C2CB346A7FA0177C032CF4676EE88BE8CE642AFAE5DA7B4D007148B4C1643F43703A514630B8C760DB4ADI B
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..H.P. /....."#.D..n.('.A.A.o]@r..Q.....<w.....].n\....A..Eo.....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):	5.621895323159144
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQPu/9Bx4B7OhKlvA1TK6tI:RbR16J1YBJkC
MD5:	7B004F7AD57B25BC5040F11DD2EE4B24

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
SHA1:	C49F15C23D3A1F1D82D3E6DF26C4E57141E751A5
SHA-256:	7D106DCC83E4EF60B8D75D0843BBCB32C28F2485220A68D4379129BFA065F3AF
SHA-512:	7105AFA5422A7ECE013A91901530D59A9C1CD60BB33061D12BD07DEDD952FFAAF5778C52170803EA4D04FD62EB2FBE9DD1984C6F2BCFEAD2B50280E03ACFFDA
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .x..P. /....."#.DD.R.('.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....P.....

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):	5.549689095703955
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuyJ/4nQdFt1TK6te9//:B2geRHRQbQn0E
MD5:	61C3EDC03B7A27D14269110E46206ECE
SHA1:	01280D1C2D6B48925F9969893741FDE1A9FFDFCF
SHA-256:	A5F200CB5E7BE94E58E4133CEC252C6524C3060045A7B5F1309613C00FE4DD75
SHA-512:	196E447C0114A622A372F3854B5245935BA742BFCEDBEF0CF7337E362FAC032D898B16EBF9254AE834D9ACF65147F661CD6C2AFB8618BA6D11D7C9DD2FA645BB
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..2.P. /....."#.D..o.('.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....d../.....

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):	412
Entropy (8bit):	5.638034623330597
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQOu/1t1S/1TK6tKzyEYOFLvEWdrIOQp/JoREt1S/1TK6tkN:WyeRlUt1wAyeRlEt1wq
MD5:	D83D6D9CEE5E070FD03832A67B575131
SHA1:	EC5BED8076C731407BF3FEEF1678B75E1B605DAE
SHA-256:	DF8B53481EF69E1008A3883F80015128B4AD4A97333FCDD885A41BA9821F723C
SHA-512:	9046B8BB6BED4D8424E184CC007B4FD7C4E76EE51482ED7154BA1EA6ADFAC980687AA00E752661E5CB356BD957EED43A3F3F0F29203EB2034F499FEAB26CD198
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .0..O. /....."#.D>...('.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....$.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..K.O. /....."#.D..H.('.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....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):	5.526326561390346
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuQt/EblwrqwK+41TK6tW:wRhhCjwK+EQ
MD5:	13BEA2361F857F84E17F00329FFD4B85
SHA1:	39C39B1D03641B4795DA392467C670C75FF2BBF7
SHA-256:	F979D1F5B06D4EA6AFD8CAD07E4CCBD952E2AFB1B812C71D6DC9C80758FAA533
SHA-512:	F935FD32458CDB58D975CF38563CC141B56099D25A9777072480BD213BFF645F9A1F356ACE5215F50E222B54A704F37D1FF0C5B713EDA4EEFED60B82825B5FE8
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..b.P. /....."#.D..R.('.A.....7...o..a=.98I.....(3.$G.A..Eo.....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):	460

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Entropy (8bit):	5.630708382011567
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuDw/3apfO441TK6teYXYOFLvEWdrROk/RJbu9//uzfO4h:/RrROk/MQapfLEVRrROk/8ezfLE
MD5:	92BED6AA14A6FB64498835C0114441C8
SHA1:	D3F8B4687EC74B36B9FA81E17910723F3DCB1A03
SHA-256:	6AD78C84DDC46DBC867BFFAF788675264F86FC16E95E5EA98C59A34700916EE1
SHA-512:	544BB270B6287F17E54E63F6D5895D1D7051B83A8CDAED1CEC89E30AE8486545A8F7D7BE58A2DA0DC5B4A40FEC312E359ECF633879A6B3A07C86772D33F9AECC
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....O. /....."#.DV...('.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....[.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....O. /....."#.D..G.('.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....8.....

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):	372
Entropy (8bit):	5.627001326177895
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIG9/ll/Z1QPLr1TK6t7RmDEYOFLvEWXIFal/LnoK1QPLr1TK6tR9:xqTFr/CPLnRUqTSmoKCPLnv
MD5:	4654CD13E1B4F935A0A7FAF8F30FE5BF
SHA1:	0CC80F1B0DED77D0E5749C63E06D5CEE8F62AE23
SHA-256:	7EC1438E90C389B79C5ECAA87CF6FBFEC16F5DDCF09ED514878CB62EF746301D
SHA-512:	AC772C63EF36A772FE8431519BCE325FA1976CC97EBE42C010433110E51DECC22D887B1A924E62535FA846FC59187ECCADB036A7704CE24B7BB60C35F1FA260
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...,.O. /....."#.D.{..('.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....e.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .4N.O. /....."#.D..B.('.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....l..l.....

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):	414
Entropy (8bit):	5.609451816918566
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAu1u/8jlsEJ41TK6tO52YOFLvEWdMAuH/BsEJ41TK6tP:zRMgsDVRM9JsD
MD5:	DA9B0C676B73C5D889C6372B5DF762AB
SHA1:	32D18A9D072DC061F75BA9B8C460BDB146C62866
SHA-256:	CB583BBA1B9A1DA05A19F7830C204505211A0B876559725F9BF1714861F8E4A2
SHA-512:	F6A6ABEFB64541B35D14A198826BFE6248193F2799561959D0ABE0C69A3CBFCF06E072ECD0409C2000032B27A8C8ABEE1B9AA4983D0D5B5102E174B3FC4E16E3
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....O. /....."#.Dp...('.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....o.n.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..R.P. /....."#.DOYq.('.A..z._a...'.v.....4p3..1.']...A..Eo.....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):	420
Entropy (8bit):	5.60683929488263
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAucTu/o+Fong1TK6tTQYilPYOFLvEWd8CAdAuIdKt//QhFz:6lJRFTqFoMKlJR9ItnsFoMx
MD5:	E7BF42053D0309661E4301B476D3EFB5
SHA1:	2750515034E816C2C6A4482F0E09FB5C464107FD
SHA-256:	16F99D3D7E3938F3CB5795EB1F8C84662D67B7562969F6A2DB3B206777E96E00
SHA-512:	F996AB721EDBBE1B95D01BD94E3C95A32B0D2AEDC787589E458D6706CAAAB34D7352C2610DD9EA91D2E8669B1D961D07735E127FAEC698C7A26BDD92DE99417
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .P..O. /....."#.D....('.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....f/L.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .uF.P. /....."#.D.uq.('.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....9.....

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):	446
Entropy (8bit):	5.5959356557566915
Encrypted:	false
SSDEEP:	12:F8hRrROk/OUNhOe2n/n8hRrROk/3+qKOe2:UPJ/OUNhN2aPJ/OqKN2
MD5:	B4CECFA68E9A454FED73FD315D5CC447
SHA1:	220EE72F21E46F5A09D3A0B80125AF2DCC783F3D
SHA-256:	445165CE216F90B77871598935C567F209CEBC91F1A4808DF752830142717C2E
SHA-512:	864D4B46A808D746428AC7046AA0D0186EC30B850C93A09CABE5F2A12623252EDE9713F93D7BAF0267435F207655D84113736B5713D8A2ED1535FFD071BB7559
Malicious:	false
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .d..O. /....."#.D.r..('.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....}.r.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....O. /....."#.D(.G.('.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....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):	426
Entropy (8bit):	5.688531673448058
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQaQ/adrrNJli1TK6ttLrnYOFLvEWdrIoJUQDb/a/qrNJli/:ehRcjNrNJlCPhRcbirNJlCb
MD5:	7E462C28365B5E0D5F07761CB6D3A503
SHA1:	AC5D137C194EBB265DCCAAEABCE44745E0AEA453
SHA-256:	36C0A0599D7FCC51B78F562EE7D897FEEAE1DCB2356F5EFDBFAE444BE9CCF943
SHA-512:	C7F4D4A4956DE723E9AAEB6202BBD2FC6B11AE1C96C0D8126340B3A03BF9657354042D8AFD2C34CFFB8E6648457422B1BB34AB2C96A824C859E00235ABB4401
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....O. /....."#.D...('.A.;''./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...O. /....."#.D.:H.('.A.;''./N_.,.:C..2....9L.H...3:...A..Eo.....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):	416
Entropy (8bit):	5.604808200730213
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhup/jQwZLzgm2d/1TK6tDP9/EOEYOFLvEWdrIhuYl/arZLzgm2U:0R4wRReV8RJrRReW
MD5:	BB8B7CA041DA49260F9F71AFB808D68A
SHA1:	0D95A3F0AF2EC3961B2966A0238F65D35F8987E1
SHA-256:	CB07156C717624C71A95FF0E69886A31641208C8E7A35AB1195E7A033374E90B
SHA-512:	39B2162644CE597A05BA35D35BBD6993F225272A7FE201DBDA31DB7AE7B5EE6F03FF86FFFEC20C114D28718B7C57C5BDCAF5A76443CD0EF85AA0976A08DCBI91
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....O. /....."#.D.:..('.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....'.8.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....O. /....."#.D.G.('.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....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):	376
Entropy (8bit):	5.642850545814132
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kll/X2kx56uvp1TK6tw/MAElVYOFLvEW1KCQ/Nf5Okx56uvp1Tg:6JJKn9ewJJKp2
MD5:	ACEF3DACBE5C07BE6D3E600C9D7B264B
SHA1:	ECCF9C16513739726D9D2D46937F327A2258D84B
SHA-256:	1D69CEE790D35BB7C6778E736273CE7F74C6A7AA5B08ACFBCCCAC7F82C724D29
SHA-512:	2F89555929892CD5193E620835334ECAFA3500EC37EB264B38C95A2DADFE0BA3B806940BB3331F84BE71B0F03AA0940E9299D90FD9C58FEC85CD1CB8357679B

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..x.O. /....."#.D+3..('.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....hI.....0\r ..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..p.O. /....."#.D..*.('.Az?...SwC...^..y.....V..7R-O.....A..Eo.....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):	5.6479437440830464
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu5aTu/CBlihUDLYtmOZn1TK6tJX:xRBJJTuKBlXDcFZLH
MD5:	0AA030D90CC31BEF9E5AEF39721A7F23
SHA1:	F222B5211F1CF592CBFDD5C6DEE79594DB060686
SHA-256:	1D90A32EA6614CFF59B536BE19C040AF1D9BE78EBB028E2852646F630BD16B7D
SHA-512:	7F56D73A605FEF03401D2BFB456FAFE56910C6E80D42ACC9908263879FBF6EEBC0C020617C2556567CB79CB8E9A80DDAA9FE8A7F5E6D5E9079105F63C928826
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .6L.P. /....."#.D.,q.('.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....S.....

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):	633
Entropy (8bit):	5.644573125305351
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7eQ/dVPu1TK6tssRPYOFLvEWIa7zp7Ql/zkVPu1TK6tcV8s9:BPHDcxPHvc6VrPHTNac
MD5:	C636B839F65FECA43D9BFD2E7CB8B832
SHA1:	6E61ED5E78C231F80ED5AB28F6C5834EC2D10F69
SHA-256:	4C221D9EB353259644265DC7ACFBB25B3AD9C46398248643A49B93FCFCA97986
SHA-512:	C52ABEDD859B281A2341A6B64C24A58DB6FA004C659285797F6B846AD271C265137AC38A87F4B239564AEB8B416D93A7B67EE3B8CE5BB5DDD3C6A79EF5E694 D9
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..@.O. /....."#.Dz7..('.A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....2.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....O. /....."#.DM.p.('.A...L...Im.@.....E.nW...IP..A..Eo.... .....A..Eo.....E.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .O..O. /....."#.D-...('.A...L...Im.@.....E .nW...IP..A..Eo.....A..Eo.....j.....

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):	5.563960851854798
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Qb/zbiwiM3Y1TK6tON:bJRT9sLuwr0
MD5:	55FE447E96941A879A685ACC5175F72F
SHA1:	3E521F85FAF60F2C4060E2F5E00CDBF652622A19
SHA-256:	D321A8534A5026E6C7F298557102A6A3264F6491465318959777544CF9903290
SHA-512:	F3781D277A85ABCF9A5C134C54C146F3DC04A6FD581716EBCF9A070C4F93E346A4C6196FD9A05951E8887E00A05847549CB91506F1434371BD0FA14FA62CC098
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....P. /....."#.D8.X.('.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....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:	modified
Size (bytes):	208
Entropy (8bit):	5.61379031328076
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQnKt/b32jBRCh/41TK6t6N:XRc93tz32Di/EAN
MD5:	DC0156730EC250A3393EAD9408911EB2

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
SHA1:	EC4B5717EA219A94B5C16C6C192991F66DFFC7C9
SHA-256:	9F6420D7CC7DEDB7DED8580062C1DBB0952C36528CEE67AC81F291AD650509F9
SHA-512:	9AFA74D950965413C533877DBB1E80691B0080057D602A009FF4A069F827A6D3D0DF4C7D342406961DF3A25FE0FCF99008DFD2F0961370EC41864A94612C8F36
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..f.P. /....."#.D..|.('.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....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):	5.5821936841774
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuHl//GwVULlF4r1TK6tr/:bs6xRkifWZLlF4nt/
MD5:	D0C487A2B367E8031201DED4E1BEF7D7
SHA1:	D413025D9B23D99B74CFF8834D862CDDCF2AFF75
SHA-256:	1EEEBE423796826C5AFF46C66064934D15491F3C21C2D8837E93D7F4BE60D62F
SHA-512:	5ACB05CBE49609318482E3FB2CC755508AF7129B487FA6FC8E4F567D69ADEEE003830BB7E3DB15FAE849B34AE99661BD398A597B910B0C990DDB4B14903F75C F
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....O. /....."#.Dd=..('.A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....0S1.....

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:	dropped
Size (bytes):	215
Entropy (8bit):	5.504940839826921
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvWkrwl/LYECcu1isLK5m1TK5ktrN:mhYOFLvEWd/aFuk/EEN941TK6t
MD5:	62E008A7D8FFF3F711E613B48FA44B2C
SHA1:	5AEA20A400051F13A5459BCC0AB99E275D507CCB
SHA-256:	324C1A5B748792B21DC7D88259ABB751E350A7615737FFAC79B77DFAF530EDA3
SHA-512:	504BD04AC68616B5BC51B39697ED9E046C38A2434F6EE782B33114BB68F1DDB4BF637D4BE239CBABA1D45D5B454DA4AA163651F4E56305451AB8E389C70B69E 0
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ....P. /....."#.D.r.('.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....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):	5.526917886013214
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ8u/2XoBMqVd3G4K41TK6t8:2DRuRTuOYB9Vd2kK
MD5:	B7BE78F75F1E1585EE5C3A23732471DC
SHA1:	77D6E2777CB15C030998D763AF52AA5F8E0C6642
SHA-256:	B4B775AA7EAE048C989C81A2902E54289A37C2C052132658709049B79EAA68F0
SHA-512:	60DD90378F05CEB598742C4FA497D25476E40B4481E3F2F77F4D007EF3E5DBB7F8AF68693C543410CEF1A82C3A31CE1B47F5E545BB0BA38BCC9C44B77DCBA4 5
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..I.P. /....."#.D..q.('.A..y.$..$.v5j...T...z.]..._S....A..Eo.....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):	416
Entropy (8bit):	5.614572592029062

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QA/20dmuA424r1TK6tn+kqYOFLvEWd8CAd9QvKt/Q3uA4244:+RQK07rnsRQbt4ern
MD5:	914CB09E8409B485EF76B53A4EAD1C7F
SHA1:	231142F2F148111ED79BD2FF8235902D84FFFA0D
SHA-256:	C65751920890B7A394358AB374E5F6C637F01F5A33C5B1BEF4BC392262C87213
SHA-512:	86A1B90B93C29D78F36EB71F4D9D242DE3D076518360474C0F90E08633B9E4E71AB98AC5CEC429F849A57DD31B3557AA221858E5A3A649901AEDAEED31A5729
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .eW.O. /....."#.D.Q.('.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....qk.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..(.P. /....."#.Db.}.('.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....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):	5.5082815371993235
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAua+//eyyC8n1TK6t:xhRTxGy7Q
MD5:	4DEC24470D21F21DC2470CCE0FBD47CC
SHA1:	C4AEB3007486B2F292DD67FC4352D9B7160300CB
SHA-256:	C0F63C7D9C9A75B0C50BA98C67D6A2EAA132E149596E2E41BEBAAE8F06DDC7A5
SHA-512:	33BFC19C0CDB4DD1AAA955B9300DE9BA9D9DE904012EE189BEC9F017652C5FD560E666E0CFC9BA44E736FBCE4DE14182BBFBBE42295B1FAA695CAB666793A322
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .o^.P. /....."#.Dn.R.('.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....d.....

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):	442
Entropy (8bit):	5.669621689119283
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQFC/Fb6LmB41TK6t5NMQZYOFLvEWdrROk/VQQC/n50LmB4o:nRrROk/V9TmRlRrROk/V0VmM
MD5:	84C86397F33CF46D316050516C3E9B0D
SHA1:	55430B172A7AF2401840DECB5DF2ADBD0982348A
SHA-256:	7A7469C7D3E415895FEFC460D0E22880E24EF2A0BB07F7B5343E481663FD6F70
SHA-512:	23CA021B290CB27F62A012D70BAC69F907CB601A01CAD756B98D2CC5D5D353BBE4E51D4BF9D132AF85CA0280D529E5CC638D5089704E4D5826FAAFC9B93A02C2
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .'..O. /....."#.DG..('.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....).....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .d..O. /....."#.DMLH.('.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....r.Zz.....

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):	5.567960078509127
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuK/axAdm9741TK6t:qxRcEyxAdu7E
MD5:	BA811860949FBEF0B2B3667352E5E5F7
SHA1:	107818D7821A1E5567175E0B8C58C1E47EA36AD8
SHA-256:	320A26BC4C406A7653AFF97366F0505593854126410B3F35441602494AF7989D
SHA-512:	EECBD4D7C6ED11FA30F94818E9E0790970CEF6A225372F1EAA0DBE26C14E1EAA92152FC91DE8E3E570D4906B28C6404091C7B245B956BED54D4ECFB52F489AE0
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....P. /....."#.D..o.('.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....21.....

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):	5.535079718631051
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuZeQ/BAkJn1TK6txIFll:2R1yZAqLTIf
MD5:	3F89BF26CEBC79EF4EA30450BF90507F
SHA1:	E224E3300AD5D72E78BA6C0B7C23C850E1AEFE92
SHA-256:	6566E685906B746FC0AB40266EB58A33AEA4273224E4FFB21FC8B0CD2866EDC1
SHA-512:	23FDB7D808E7E5466B35DCE559A4FF9AD6180A77ADF3900081CD7D328EB9A7C9B54F83605B1874DF901F5520D476CC733D4A6D5BD05389A78916E5E29138C79
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..[.P. /....."#.Dk~R.('.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....Q-.....

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):	5.623216694526563
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQN//P54s2zhcsBXIh1TK6t:mxRBJQGHl2DB0
MD5:	93D2BED395B9B53D622BE99BD5BD9F79
SHA1:	7E44BFA9B4E786F3E8D5EF4EFFFC99B725332D86
SHA-256:	E9696368456E7C98F9FD5BA4E78B4150FA3C83F9E8CE7DC36AE920DE5C3388AD
SHA-512:	9AFAF5680B0092350D158B6D710951BA560B32AE145A67D4438093BA5A958E7D8F8FFEECDD4F463F2968DB4AF98373E6FB169D109013FF59DEF32A4C71DE74C
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .)..P. /....."#.D-&r.('.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....n#.....

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):	456
Entropy (8bit):	5.617118546169625
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQRt/moGc3Me/1TK6tQ2sPYOFLvEWdrROk/RJUQ6/DVoMr:3RrROk/scQoGcyHRrROk/sxVlc2R
MD5:	2A5CC43C5300D69A0AEF18AD0EBC755B
SHA1:	949B0D321C3B35F5775A5E45C1FB3871EDBA5E1C
SHA-256:	4B44F07FC64AD9BCE03ED976858DCBEAB83DE4BA3BC9799E6CCBA50CF0D5D35A
SHA-512:	C91F4881C4BEC2797B4AA578CA7FB3B25A7ADAD650E773AA20B0D817D1E3E60C2ACD9AE3A8B286B7F29A00B635ADC378D4583E67DFFB8E65C17A7BD6A620E86C
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..5.O. /....."#.D.M..('.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....O. /....."#.D.H.('.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....htmL.....

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):	2016
Entropy (8bit):	5.319564755198512
Encrypted:	false
SSDEEP:	48:JGnojTcmSBoiMJMRy1Q3V1gMcFiLLIlSOVBmWGsAg15G29FSGIWj:Jjgon/Mwxj
MD5:	4441C84D470AC556388E9A809802EDB3
SHA1:	DF2700C7CF90F29EE63857386A1092EA1CDA8D2A
SHA-256:	2ABDD21EC295680E92FE6ACEEC16DD7EE50F43582D191BA7970B1ECA74A5401D
SHA-512:	3140E3B2D9D3AF5105B6A09C8D4DF0F06459DE91D7320B69658319358299F4F2273147387BCE2DD108BF1DCFCB19A56C746B2A00BEBE958390D7CD086FF8E50
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Preview:	....U...oy retne....'.....'.....;.y~A.@.....*..@.....oB*@.....#...(@.....k7A.@.....D.4.....[.i..%.....<...W..J@....., +..._.#@.....J..j.....6<|...@.....A?.2:.....+.{..'.....*)....J:.....2q....@.....P....V@.....+.U.!..V.....P[. q@..... .....!...0.o.....u\].q.....@.....*.....o..k.....^.~..z.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@.....v... q..@.....C..M..@.....a....@.....~.,.4>.....&.S.....@..x.....=....m.....;/...@.....q.....MV3.....:..N. A..@.....>.O.oy retne

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):	295
Entropy (8bit):	5.151182115669985
Encrypted:	false
SSDEEP:	6:mXVQ0q2PN72nKuAl9OmbnIFUtp8VQ7zZmwP8VQKkwON72nKuAl9OmbjLJ:sy0vVaHAahFUtp8yf/P8yK5OaHAaSJ
MD5:	9DABEB68FC8EF65616B05A46D9EF73ED
SHA1:	F245046888E5B2CAAA4686671AE7A33077FE88BC
SHA-256:	312256FF622E1928E9AFF8C970AED5368628B85C4706397D7F0772F121F93913
SHA-512:	6D376958B3BFF2A4F21A8C93B4E596E047C3A7EED42E529E30382B09CDEA512F467FB85BC38A42E3F8744EF04057B01CAA84A1ECB40DAB55E67CC7A5DB2CC2 4E
Malicious:	false
Preview:	2021/05/12-20:50:27.367 b40 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/05/12-20:50:27.372 b40 Recovering log #3.2021/05/12-20:50:27.373 b40 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):	917504
Entropy (8bit):	0.007716873612814605
Encrypted:	false
SSDEEP:	24:T+X8I5mv+X8I5mv+X8I5myrY5mrY5mmHY5mmHY5mm:To35Oo35Oo3525T5K5K5
MD5:	545783574F55AE7B68107D94104DF5DC
SHA1:	A165613C78A951FE14CC2DE4C0119545FB09CB97
SHA-256:	4FD5A8538D675D352B60CCF8E1EE7BC3A43F35696354EAFF170465BBD8D6D2B0
SHA-512:	8E235F34944EF6299185ACA3691FA27C31BD81110EE08898801A333A0D4C6F89D398AAC6AEC54C1CAA649C592C3F9F008DF7124C216A0AFEAC8087AB2DC00B5 A
Malicious:	false
Preview:	VLnk.....?.....`.N.7..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2105130035019Z-248.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 92 x -152 x 32
Category:	dropped
Size (bytes):	55990
Entropy (8bit):	2.175166721963963
Encrypted:	false
SSDEEP:	192:NzpwhCg1InAs3wmHRncVR5CWdQIiD22PBt/WXmtZZ/1ImdYNSWp:Nzpw52As3wWRncVHN4D2o75NImdQSm
MD5:	3E298A727A119EED868056DB8DA6AABA
SHA1:	89CC1B3CF843B43864CD15181298F7C455B61DE7
SHA-256:	6388A23A4CEE5DD1C5A5AF2F09E53AEF7ED48BF458C13B6732FE3BE5B49F89D9
SHA-512:	DD09D315D2986315E3C2D843DA8C06472765CAB9AAC2F7CBE6F034E3082BE8D2B220EA69AA1CF89AF243AB861A15AF213EED86DDE7A05369539953F9CA8874 A
Malicious:	false
Preview:	BM.....6...(...\...h.... ....

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
Category:	modified
Size (bytes):	32768

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Entropy (8bit):	3.385087204832873
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQIOhFVCsL49IVXEBodRBkRXIOhAVCs749IVXEBodRBklXIOh93:iGedRBwedRB6edRBxedRBj
MD5:	9386494C66C372EA3BF1F17D4826B911
SHA1:	213CAB456BDA0F802DEF3DA88CAE65F8A8122DF5
SHA-256:	0896349509AAAC2EA4234830CE85F5CB6F848DC0A92FE59C7F4C27D7ACDF06EC
SHA-512:	3666B241DD3F8AECA3382A8F73BD462EDC88CB9EE92CDBA0285D7C4ED77766079DDCEB48AC899152CD278DBC1A118AB6F1F40A88E5BD0CB25B1176163929AEED
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:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.1986323233414984
Encrypted:	false
SSDEEP:	96:a7OhFVCPV949IVXEBodRBk1IOhFVCsPLR49IVXEBodRBk2XIOhAVCsOpd49IVXE6:aZiedRBMLGedRBhpCedRBOyedRB2
MD5:	95FC30A0977C2461C0905101188B97A2
SHA1:	CDE343AA3BC922627E31F18C917C9B6D3EB68FEE
SHA-256:	AB4ABE43BA2CA2DBD8341AE73CFF5518C38FA26E80D516627465A250255CE361
SHA-512:	DCFB4807EF90DC5C3922689919FE9A07FB8605C144831BB41D1A21FA8F86F355003D9C44BAA47236BEB5CED61080765512EE27EFC1D9872F1C87014AEA2ED04
Malicious:	false
Preview:	.....hy.....X.. .h...y.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6548	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

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:PCbGNFYGpiyVFiCUZAKnlfTgi3vQo9SWsMwQaUIh8Yyu:J0GpiyVFiBAKnlfTgSvQhHh8K
MD5:	3204E5B2245450A47E241E7AA67B94A6
SHA1:	82F955990016B054234270375692724BC04EDCEF
SHA-256:	86B97FC8D11CF2FA9B15ACEE204F8AC0D2C2A7ACCBD27F2B1F8B159AE64923B3
SHA-512:	D260977E17A99AAA02F8025F8298B9D8012D4AB70E1D7AF4072BFCAD42AC27D74FEFA3569584CFD09DC42CB053BB4E6D6E39D3A7B5A0BF65D0D3EBF69CED54B

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

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.769316128514805
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Covid screening questionaire.pdf
File size:	1889954
MD5:	e87f93f286ff7cc507263e8d35e0f326
SHA1:	099b509e715dbbbc8d3a634b6b450276a3f2c901
SHA256:	12b425e76752e75a87ccdfc8537f7d208fc57c77ff23792f9475b720d1985c03
SHA512:	e0c6427d30a5bb4982c71b93fdb048cbc867eba65805bfdc201a722e53e2b370370d7ccbea254b2bb24402eb60c077b034ccb403e64979a376fd2675f970424a
SSDEEP:	24576:SVdpN+pxCF1O6WmRGgYQjdRA1+iAURvF53s6+y1N626ayePg:SjUaIggS0X3NLjcayV
File Content Preview:	%PDF-1.7.1 0 obj.<</Type /XObject /Subtype /Image /Name /Im1 /Width 2550 /Height 4200 /Length 932444/ColorSpace /DeviceRGB /BitsPerComponent 8 /Filter [/DCTDecode] >> stream.....JFIF.....,.....C..... $.' ",#..(7),01444.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

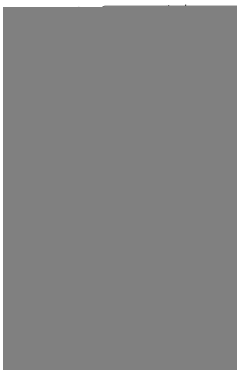
Header:	%PDF-1.7
Total Entropy:	7.769316
Total Bytes:	1889954
Stream Entropy:	7.768843
Stream Bytes:	1888087
Entropy outside Streams:	0.000000
Bytes outside Streams:	1867
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	12
endobj	12
stream	5
endstream	5
xref	1
trailer	1
startxref	1
/Page	2
/Encrypt	0
/ObjStm	0

Name	Count
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	1
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview
5	1337233337371800	5f2c2559a34d7cc338e2aeddb0ebbec9	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:49:58.947738886 CEST	53	58377	8.8.8.8	192.168.2.6
May 12, 2021 20:50:00.292471886 CEST	55074	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:00.350013018 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 20:50:01.665342093 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:01.716906071 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 20:50:02.247436047 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:02.311527967 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 20:50:02.792363882 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:02.843997955 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 20:50:03.681477070 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:03.732913017 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 20:50:04.733994007 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:04.783029079 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 20:50:05.700767994 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:05.758119106 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 20:50:07.228642941 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:07.278812885 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 20:50:09.136807919 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:09.185689926 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 20:50:10.922595024 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:10.974298000 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 20:50:12.374263048 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:12.426855087 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 20:50:13.511872053 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:13.560576916 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 20:50:14.304697037 CEST	56061	53	192.168.2.6	8.8.8.8

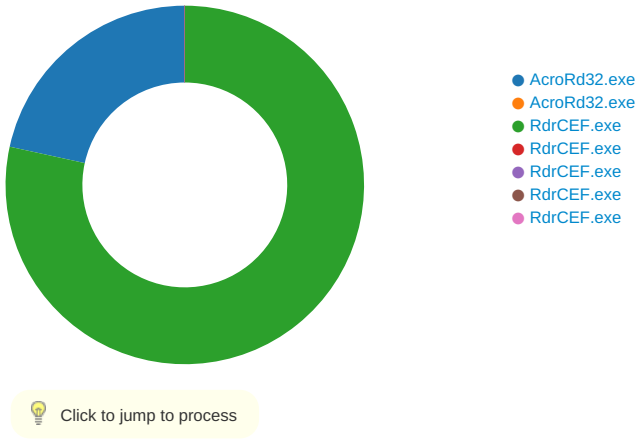
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:50:14.356369019 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 20:50:15.434683084 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:15.493505001 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 20:50:18.002841949 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:18.051497936 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 20:50:20.780456066 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:20.831969023 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 20:50:26.647129059 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:26.664149046 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:26.708224058 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 20:50:26.724596024 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 20:50:27.520817041 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:27.570167065 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 20:50:27.647268057 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:27.694108009 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:27.704601049 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 20:50:27.753485918 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 20:50:28.694247961 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:28.743119955 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 20:50:28.756726980 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:28.814501047 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 20:50:29.649420977 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:29.701577902 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 20:50:30.743951082 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:30.795936108 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:30.801767111 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 20:50:30.846111059 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 20:50:34.747320890 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:34.808429956 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 20:50:34.856472015 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:34.905275106 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 20:50:36.521317005 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:36.581729889 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 20:50:42.078983068 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:42.140525103 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 20:50:54.117219925 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:54.179619074 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 20:50:58.666032076 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:58.777053118 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 20:50:59.430545092 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 20:50:59.491303921 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 20:51:00.065659046 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:00.177536964 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 20:51:00.374206066 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:00.445522070 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 20:51:00.637666941 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:00.697876930 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 20:51:01.277488947 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:01.337687016 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 20:51:01.897491932 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:01.958791971 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 20:51:02.499034882 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:02.556307077 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 20:51:03.342489004 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:03.401976109 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 20:51:04.571592093 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:04.620486021 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 20:51:05.156728029 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:05.216288090 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 20:51:12.847362995 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:12.906177998 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 20:51:34.591957092 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:34.653673887 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 20:51:45.458004951 CEST	54683	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:51:45.515403986 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 20:51:46.903016090 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 20:51:46.960410118 CEST	53	59329	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 6480 Parent PID: 5944

General

Start time:	20:50:08
Start date:	12/05/2021
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' 'C:\Users\user\Desktop\Covid screening questionaire.pdf'
Imagebase:	0x11c0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	11F65C3	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	121AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6548	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	120EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock6480.1.458508967.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	1242657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	120EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210513035019Z-248.bmp	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	120EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	12883C8	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	12883C8	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	12883C8	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	12883C8	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	12883C8	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	12883C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R150kmwn_gsjvi0_51w.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	120EA85	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	120EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1n8koxf_gsjvi1_51w.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	120EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R19jgh3v_gsjvi2_51w.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	120EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R17c4rxo_gsjvi3_51w.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	120EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1si7rez_gsjvi4_51w.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	120EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6548	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	124D405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	120CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	120D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	120D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	120D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	11CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	11CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	11CEA55	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	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Covid screening questionaire.pdf	success or wait	1	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Covid screening questionaire.pdf	success or wait	1	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	121DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 65 6E 67 69 6E 65 65 72 2F 44 65 73 6B 74 6F 70 2F 43 6F 76 69 64 20 73 63 72 65 65 6E 69 6E 67 20 71 75 65 73 74 69 6F 6E 61 69 72 65 2E 70 64 66 00	success or wait	1	121DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 35 31 32 32 30 35 30 31 38 2D 30 37 27 30 30 27 00	success or wait	1	121DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	1889954	success or wait	1	121DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	2	success or wait	1	121DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	121DF47	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	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	121DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	121DF69	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	121DF69	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	121DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6548 Parent PID: 6480

General

Start time:	20:50:10
Start date:	12/05/2021

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' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Covid screening questionaire.pdf'
Imagebase:	0x11c0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 6816 Parent PID: 6480

General

Start time:	20:50:17
Start date:	12/05/2021
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:	0xc60000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	2	D559E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	1	D683E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	34	D68447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	165	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	17	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	D559E2	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	D559E2	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	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1628	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	30	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	4	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	D559E2	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	2	D559E2	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	2	D559E2	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	D559E2	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	2	D559E2	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	D559E2	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	2	D559E2	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	4	D559E2	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	2	D559E2	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	2	D559E2	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	2	D559E2	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	2	D559E2	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	2	D559E2	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	D559E2	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	2	D559E2	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	12	D559E2	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	D559E2	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	12	D559E2	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	2	D559E2	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	28	D559E2	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	2	D559E2	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	30	D559E2	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	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	D559E2	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	1	D559E2	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	44	D559E2	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	1	D559E2	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	1	D559E2	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	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	D559E2	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	10	D559E2	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	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	D559E2	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	6	D559E2	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	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	143	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	D559E2	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	134	D559E2	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	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	97	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	D559E2	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	15	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	D559E2	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	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	D559E2	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	2	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	D559E2	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	1	D559E2	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	1	D559E2	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	D559E2	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	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	D559E2	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	84	D559E2	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	1	D559E2	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	4	D559E2	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	1	D559E2	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	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	D559E2	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	1	D559E2	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	D559E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	1	D559E2	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	1	D559E2	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	1	D559E2	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	8	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	161	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	1	D559E2	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	2	D559E2	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	1	D559E2	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	74	D559E2	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	1	D559E2	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	6	D559E2	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	1	D559E2	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	16	D559E2	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	1	D559E2	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	5	D559E2	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	1	D559E2	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	D559E2	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	D559E2	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	2	D559E2	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	1	D559E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	D683E5	ReadFile

Analysis Process: RdrCEF.exe PID: 7032 Parent PID: 6816

General

Start time:	20:50:20
Start date:	12/05/2021
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' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16739402187565574225 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=16739402187565574225 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xc60000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 7064 Parent PID: 6816

General

Start time:	20:50:22
Start date:	12/05/2021
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' --type=gpu-process --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=15525037812135764353 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xc60000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 7132 Parent PID: 6816

General

Start time:	20:50:27
Start date:	12/05/2021
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' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=844945410949651913 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=844945410949651913 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xc60000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 4240 Parent PID: 6816

General

Start time:	20:50:29
Start date:	12/05/2021
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' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,7532418871871553696,2370599676892093201,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=357690743904107764 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=357690743904107764 --renderer-client-id=5 --mojo-platform-channel-handle=2084 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xc60000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis