ID: 324346
Sample Name: contract 27.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 11:35:40
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

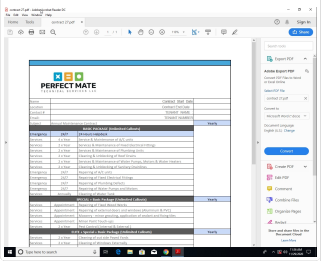
Analysis Report contract 27.pdf

Overview

General Information

Sample Name:	contract 27.pdf
Analysis ID:	324346
MD5:	b5da5a1891fdaa1.
SHA1:	ff748311fe2f1fd7…
SHA256:	03fbf86eb9c46c3..

Most interesting Screenshot:



Detection

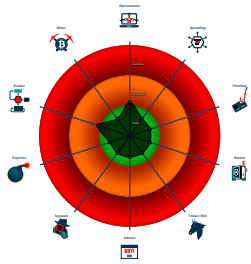
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Contains functionality to access load…

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 3528 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\contract 27.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 1488 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\contract 27.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5668 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6248 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=1720,5757292434480114666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7546301349673146790 --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=7546301349673146790 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6272 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,5757292434480114666,2542267608491848794,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=12817687695606234436 --mojo-platform-channel-handle=1688 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6424 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=1720,5757292434480114666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2753125301934643863 --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=2753125301934643863 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6560 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=1720,5757292434480114666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12075229495714680774 --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=12075229495714680774 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6796 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=1720,5757292434480114666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17952855729266451437 --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=17952855729266451437 --renderer-client-id=6 --mojo-platform-channel-handle=2092 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

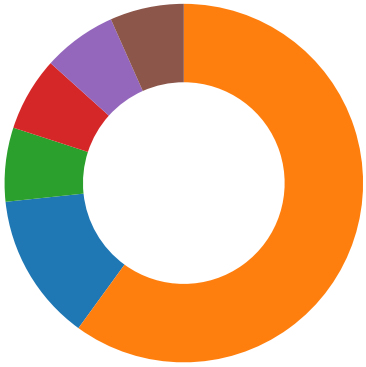
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

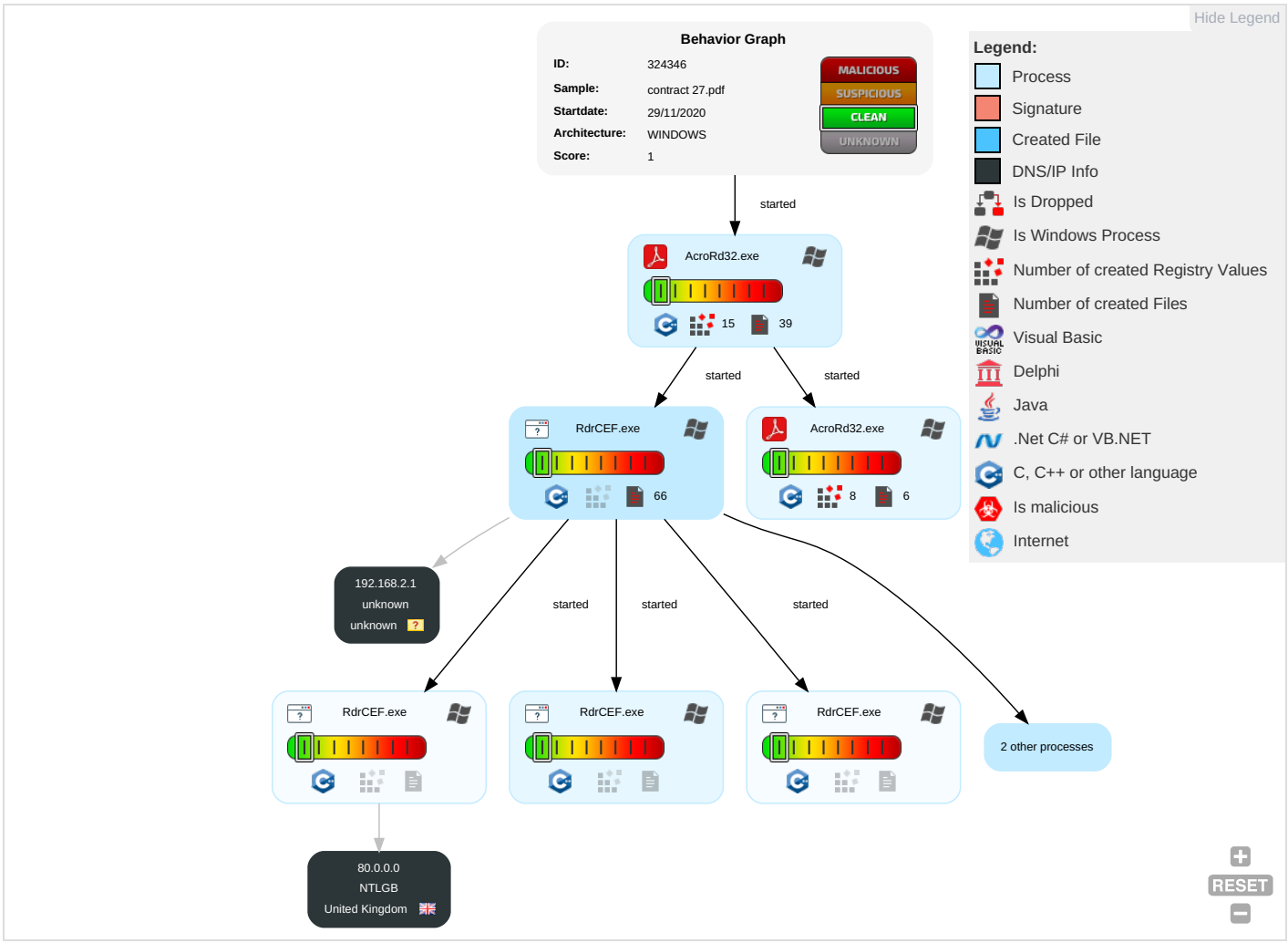
Click to jump to signature section

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 Sy Pa
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 Lo
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

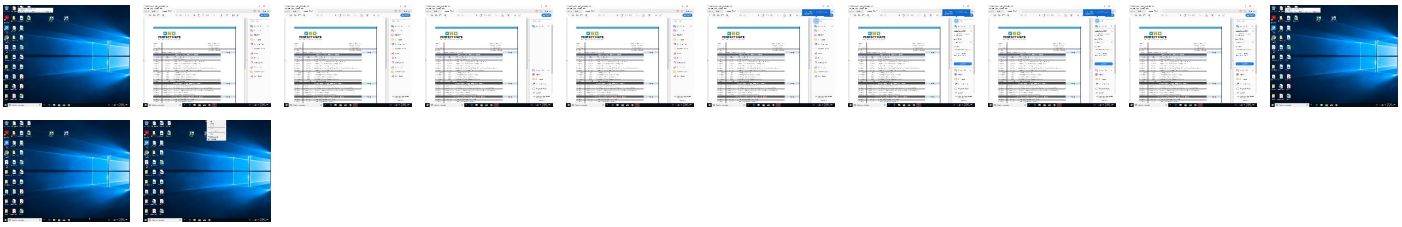
Behavior Graph

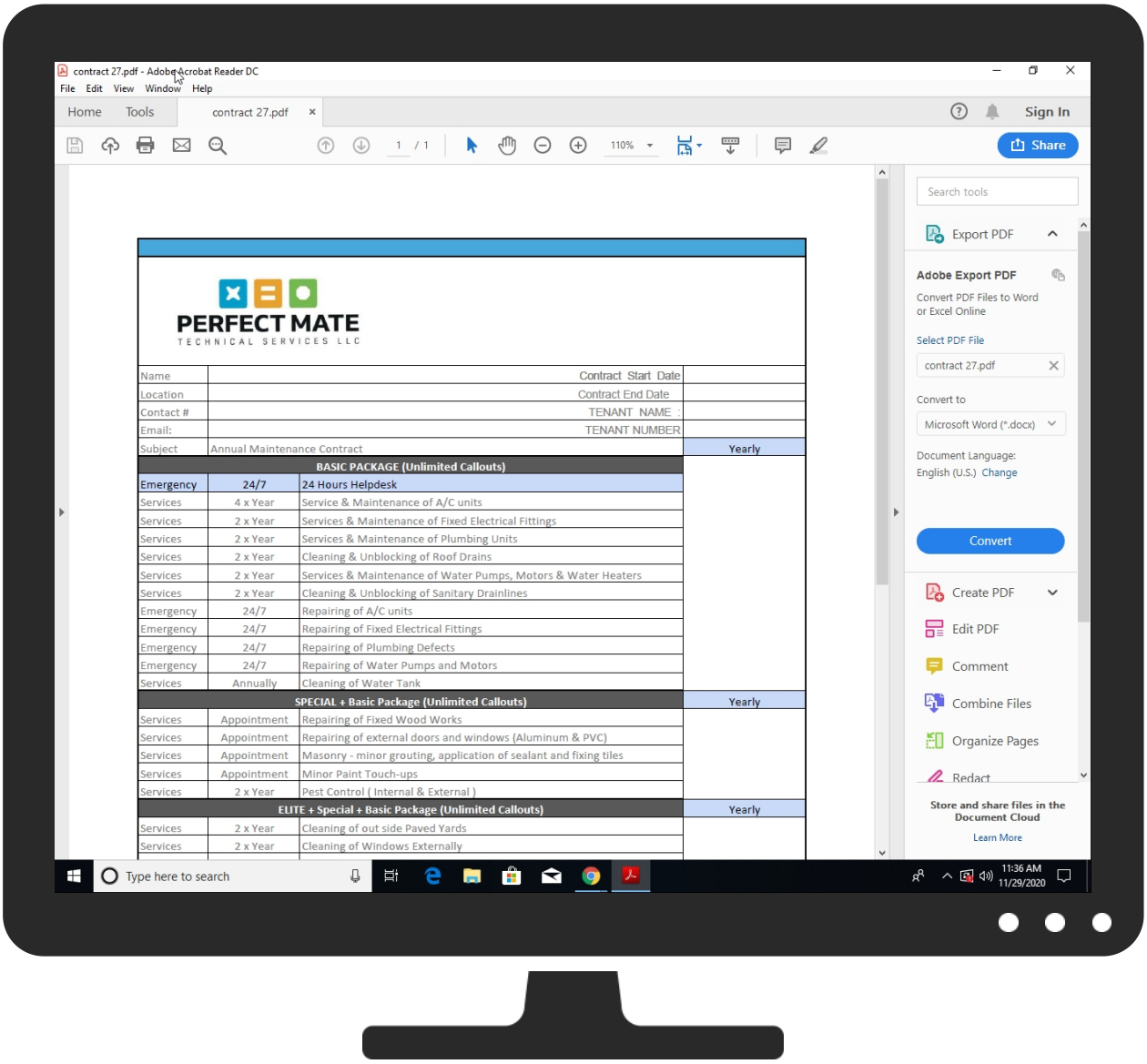


Screenshots

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://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
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://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://api.echosign.comRL(I	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://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/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://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	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://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://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/Upload/.	0%	Avira URL Cloud	safe	
http://https://api.echosign.comlass	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.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/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://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	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$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$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://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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/X7	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/sA7	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/b	0%	Avira URL Cloud	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	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/w7	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

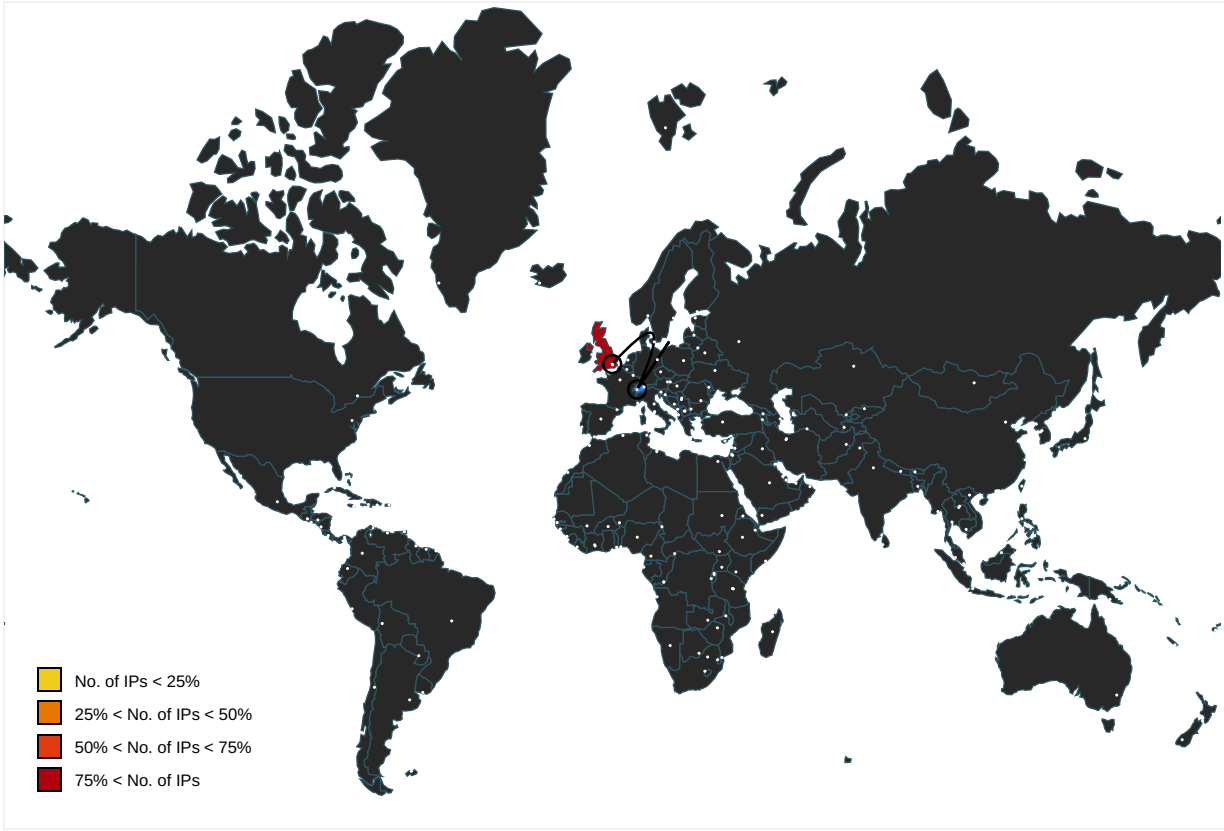
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/type#_	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.367066397.0000000009150000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comRL(I	AcroRd32.exe, 00000001.00000002.375622312.000000000B525000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.367066397.0000000009150000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.367066397.0000000009150000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/schema#(	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/.	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.376907114.000000000D42D000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comlass	AcroRd32.exe, 00000001.00000002.376375186.000000000D2E0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.367066397.0000000009150000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • 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, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.367066397.0000000009150000.00000004.00000001.sdmp	false		high
http://www.adobe.	AcroRd32.exe, 00000001.00000002.377218933.000000000D5BF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/X7	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/sA7	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.useplus.org/ldf/xmp/1.0/b	AcroRd32.exe, 00000001.00000002.367255780.0000000009220000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.362685658.0000000007970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/:	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/w7	AcroRd32.exe, 00000001.00000002.375081388.000000000B132000.00000004.00000001.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:	31.0.0 Red Diamond
Analysis ID:	324346
Start date:	29.11.2020
Start time:	11:35:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	contract 27.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:	26
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@15/48@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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 92.122.146.26, 2.20.143.130, 2.20.142.203, 51.104.139.180, 40.88.32.150, 52.147.198.201, 104.79.90.110, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, armmf.adobe.com, a122.dscd.akamai.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:36:34	API Interceptor	8x 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	CHoyU.pdf	Get hash	malicious	Browse	
	ggBNN.pdf	Get hash	malicious	Browse	
	KKjNA.pdf	Get hash	malicious	Browse	
	IFPoj.pdf	Get hash	malicious	Browse	
	MXNYB.pdf	Get hash	malicious	Browse	
	npmiu.pdf	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sCpYf.pdf	Get hash	malicious	Browse	
	sIdiW.pdf	Get hash	malicious	Browse	
	UsBzT.pdf	Get hash	malicious	Browse	
	VFznx.pdf	Get hash	malicious	Browse	
	mGhdt.pdf	Get hash	malicious	Browse	
	b6egewgab.pdf	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	http://post.spmailtechnolo.com/f/a/h2coVlte-PnQgGolAw1FlQ~~/AAH5oAA~/RgRhk9ssP0QiaHR0cHM6Ly93d3cud2F6cC5pby9kb3dubG9hZC82MTI3L1cDc3BjQgoAJyxWsV-4NRnDUhVzY290dC50YXlsb3JAdG1hZy5jb21YBAAAAG4~	Get hash	malicious	Browse	
	5wnaEGcbc7.exe	Get hash	malicious	Browse	
	Kpw6TB725f.exe	Get hash	malicious	Browse	
	LWwoiTLRjW.exe	Get hash	malicious	Browse	
	Gt2YstXx3K.exe	Get hash	malicious	Browse	
	ForQuotation_RMS22100.exe	Get hash	malicious	Browse	
	http://www.dropbox.com/l/AAA5d-90vlipt6OAJjh2DZ1FLO-gN1n6Y0k	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	CHoyU.pdf	Get hash	malicious	Browse	• 80.0.0.0
	ggBNN.pdf	Get hash	malicious	Browse	• 80.0.0.0
	KKjNA.pdf	Get hash	malicious	Browse	• 80.0.0.0
	IFPoj.pdf	Get hash	malicious	Browse	• 80.0.0.0
	MXNYB.pdf	Get hash	malicious	Browse	• 80.0.0.0
	npmiu.pdf	Get hash	malicious	Browse	• 80.0.0.0
	sCpYf.pdf	Get hash	malicious	Browse	• 80.0.0.0
	sIdiW.pdf	Get hash	malicious	Browse	• 80.0.0.0
	UsBzT.pdf	Get hash	malicious	Browse	• 80.0.0.0
	VFznx.pdf	Get hash	malicious	Browse	• 80.0.0.0
	mGhdt.pdf	Get hash	malicious	Browse	• 80.0.0.0
	b6egewgab.pdf	Get hash	malicious	Browse	• 80.0.0.0
	purchase order.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://post.spmailtechnolo.com/f/a/h2coVlte-PnQgGolAw1FlQ~~/AAH5oAA~/RgRhk9ssP0QiaHR0cHM6Ly93d3cud2F6cC5pby9kb3dubG9hZC82MTI3L1cDc3BjQgoAJyxWsV-4NRnDUhVzY290dC50YXlsb3JAdG1hZy5jb21YBAAAAG4~	Get hash	malicious	Browse	• 80.0.0.0
	5wnaEGcbc7.exe	Get hash	malicious	Browse	• 80.0.0.0
	Kpw6TB725f.exe	Get hash	malicious	Browse	• 80.0.0.0
	EnkIyRDCVr.exe	Get hash	malicious	Browse	• 62.31.150.202
	LWwoiTLRjW.exe	Get hash	malicious	Browse	• 80.0.0.0
	Gt2YstXx3K.exe	Get hash	malicious	Browse	• 80.0.0.0
	ForQuotation_RMS22100.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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
File Type:	data
Category:	dropped
Size (bytes):	820
Entropy (8bit):	5.7123589524269365
Encrypted:	false
SSDEEP:	12:vDRM9AVOZiE3DRM9zpAZiE75DRM9aZiECDRM9IZiE:75EzQfEhuEw0E
MD5:	1BC81019C3699684D0506F4C28F38C1F
SHA1:	E7195B08DD59EC70A9EFCE6499B4497724036E10
SHA-256:	7D77DADE01D64D0E81AEB6542268BCE38238536FA49F531BE808C349CA664F23
SHA-512:	F4689CE9E1B7D917C4EEF4AD88DB32E8B59D698111AB59A74906968A2F6E64EDE53E8504C882B4A739530811CC314F17D1DA5BC34197C21CA623CC0064B30D4D
Malicious:	false
Preview:	0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .Z.K../....."#.Dv.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... ..U.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .J[.L../....."#.DbLD....A....d.{v.^.G...d.W.:....P..k%..A..Eo..... A..Eo.....v.g.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .QA&L../....."#.D.....A....d.{v.^.G...d.W.:....P..k%..A..Eo..... .....A..Eo.....y1d.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .].oL../....."#.D.~.....A....d.{v.^.G...d.W.:...P..k%.. A..Eo.....A..Eo....._.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	5.62615420807545
Encrypted:	false
SSDEEP:	12:V9zwaZ9PQdzH9zZc9PQR9zti9PQB9zAG9PQ:Xz59PQddzW9PQbzc9PQLzAG9PQ
MD5:	9F38D1BDDAD4DC842F9F076082F3CB79
SHA1:	E59ECB1709BD59F7C03FEA4A1AE777FE85035A98
SHA-256:	1A2C76CF7ED579A4A87A955046D7765C39CBBEA1EDC13A9B5293E94FC9A36DDC
SHA-512:	AB55453E7C99B0BD35A1228751CA9F709E6B4088211929CD25510BCE2FB7FFE47EFB682938BF341A9F7FB44EA3E10D61322C9EDF81BE78607896C84919143C86
Malicious:	false
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ...K../....."#.D].....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....{#.....0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ....K../....."#.Ds/.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....\.....0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js .Z ".L../....."#.Dd.x....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....b.$.....0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js .v.aL../....."#.D.....A.1.x.' .vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....w=.....

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):	984
Entropy (8bit):	5.6535856904603845
Encrypted:	false
SSDEEP:	24:tB4v4cSB9B4v4cSBfdB4v4qSBhB4v4C6USB9:nMXSBXM7SBPMNSB7MdSB9
MD5:	AEC854B17078AC7D674FA3D958B85B80
SHA1:	3536B716FD75E9BE1D7951B2659EF9FE45FB3830
SHA-256:	C1BA3CAB8F38C80E79244F2AF287EA53BE3C6E8EDD74A565838E892294348372
SHA-512:	246DD2FB1880AD586B8217829F3CB660CB6E3E617DC760DF0C0F22C77876BE22EE7314E9A8815997855B9B3B8F9586F42E0E53A77446C78C05411D70CC3E9AF5
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....K../....."#.DHS.....A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....0.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .?..L../....."#.D2.<....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....9K.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .[.%L../....."#.DV.....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 .K@nL../....."#.D&.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....U.....

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):	464
Entropy (8bit):	5.729065702843923
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RslL2AUb0iWulHyA1TK6tCflMNtVYOFLvEWdFCi5Rszx/yi5:IbRkiDKU5WussowbRkiDSNWussv
MD5:	4C513602E7DFE6032C089991F9C7BAC6
SHA1:	F6D69F89897F1CCA172FE1DC96F78DE6E0F5F925

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
SHA-256:	59F69CC460701D1DED7A414305D70EB356AAB5957856A65ED8937A422B797536
SHA-512:	F3686A0D7385E5E6DADC68B3207884ABF3DD134522DEAD048D782F88CA1A74FD6154FC95ECDAFC0C11D6DD764C6767A38413B42371C9A636305F2A6B64CBA0 5
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..1.K../....."#.D.....A..8 P..a...R..Y....7.@..2Dm{. .A..Eo.....A..Eo.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...*L../....."# .D).....A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....-.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.628884614693151
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuu1/hkkVyh9PT41TK6tPe+yiXYOFLvEWd7VIGXVuf/NVn:pyixRuEvkkV41TE5hyixRupFV41TEr/
MD5:	22D7AAD6941E5836596B9E17D26508B8
SHA1:	0F0C777BACD2761B1194BF3399368FDA911ED79F
SHA-256:	5505DCE98DB5EFFC96AE830B598D8AB9AA0DD891CA798B5D9E3578DB8B81386E
SHA-512:	26283CDB2EB92AC951DB76F1E421299C53C6E16E2ABD1D975E9A3741035D50A5C4A0AD873E791B63E954A51AA5B3773F87599DC4211535874051926FC103B519
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .N..L../....."#.D..;....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....- 3<.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...nL../....."#.D.....Ak.Q.....-_..y.....O...>..1....A..Eo..... .A..Eo.....)[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.656900451133761
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQHk4CnhLZIl6P41TK6t4U8vYOFLvEWdhwjQpvt6hLZIl6P41TK2:0RhkSCnhLZC1aRhkq8hLZCtl
MD5:	58A18C2FAFD0568D60BA8614A4012FDB
SHA1:	E17BA1DDB4B9094BB00F13FDECEE6D09B03A5F23
SHA-256:	95F34443DFD857B83210AE196C685D8FDFB0D2FA5B2A467F34A6853370FC6E56
SHA-512:	271277930435971C867871373B9163AB4402D4C733898996D84245D45BAEC605C91301DCB89A4D7A49728A51085834A2E5BB935EC88EB8DCA37CDC6EFEF8F8B9
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....L../....."#.D..*....A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....V.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..NlL../....."#.DU.....A.].>....uUf..N...k.....c..l.A.. Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.549122389384574
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQ1A/9VF6g1TK6tHJYOFLvEWdGQRQOdQTfF6g1TK6tu:2RHRQCGAVT1BRHRQCw1
MD5:	17547A4B5B88242BA05F890B2A2AF4CC
SHA1:	5EB4DA03167F57140272E6029310D7551D678035
SHA-256:	E265875120269A2EBF7FED36873A8E617A0C099BC01D9B1A2BD88E61279194AD
SHA-512:	39388C1F1F9F4F4410BDDA3F490C5ECD8EB259F1680F542DFF19659620BB69A66EB771DDA77AC579AEE22704E1A42D5CBAEE22D4A4E820AF62F1CE1A2A8680 5
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .U..L../....."#.Do.=....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....*.~B.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..4oL../....."#.D.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..... .....A..Eo.....#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Size (bytes):	716
Entropy (8bit):	5.618732165011809
Encrypted:	false
SSDEEP:	12:Z5MiAMuR/ER5Mpl9LMuR/EP5Ms/xMuR/EJtr5M47LMuR/Ez:ZSquR/ERS9ouR/EPSFuR/EJtrS4suR/Y
MD5:	53E52C8995D55601D329BB0FFE5A149B
SHA1:	261C2F7EFF756A3A8181A8BF1033361F437E9F46
SHA-256:	646BD235549D1EA7B93A8D13BCF4A5FB97BCB6C2B99088440BD74E25008D099F
SHA-512:	43C8F54D5883484481743F04F129BA7C51B0CAAF11E0A3FC8E34D8E0620AE04743C2F752D79CBCF6BF236DFA5E5B8C64ADDE2C255370F6CEE56477ED9BEE12 1
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....K../....."#.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 ....K../....."#.D,D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....PT.d.....0\r..m.....3....<lb.. .._keyhttps://rna-resource.acrobat.com/base_uris.js .jA.L../....."#.D..x....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....hW.....0\r..m.....3....<lb...._keyhttps ://rna-resource.acrobat.com/base_uris.js ...aL../....."#.DY.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....i.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.613254232517166
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu2MtX2Sm0bbsIDMGH41TK6t1:XfRMSRKsIZE
MD5:	53AB2FE722A0E771B8E56D2DA2E48361
SHA1:	0BDB14D45B3132D7CD3BFA9BDCBD3DD1E00C1E68
SHA-256:	3EB51C9140CAAE5AA813EBF69E5BFA4348FEB6E3B4DC70F197BB3E5103FB5DE5
SHA-512:	F6211AC166A1CE9C3729661F8237BB6B6D6368F84D3B05993B0FAAE43B6A8B5E59ADB368DD123415F1FC18118271B53EB1B666D6A49A7B05041A957888823982
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ._.L../....."#.D.ZS....A..`.....^....L>..Xa./.....C.y.A..Eo.....A.. Eo.....}..#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.579308059609667
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuV/Uuby0zBUKSAA1TK6t4IllM4fPYOFLvEWdtuUqI+by0zBUKSn:pR8MubeVRx+be
MD5:	F00F0EC075CE343C22E271F3F9038919
SHA1:	2BC8B38BCA0713D3450076601C7FCE8C1B88997B
SHA-256:	6248141E29FD5A2216FBA936DD43A4979FD740B42B71184C7DB709B302ECE851
SHA-512:	09E518EFE2E7DE12D34A85FE38F85F406247240E3EE2D0D163446077851F11F35E019B835688A0CCEFD452EDE947394AB0358CDAB543109EF1BAB99530ECC39I
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....L../....."#.DQ->....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....z..U.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...oL../....."#.D.d.....AQ..E.=....=h`t..t..3%A.F$ ..w..A..Eo.....A..Eo.....`|.x.....

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):	708
Entropy (8bit):	5.64589455825765
Encrypted:	false
SSDEEP:	12:KkXxKMSCvYS4tUlrkXxKMSCvzytUljkXxKMSCvaztUll4kXxKMSCvrtUl:KkXxiCj4WrkXxiCmWjkXxiCizWakXxi3
MD5:	515D8C7B90B9B1CFCE4CBDBF6D33895E
SHA1:	EE429583AD67D0BF65EC53F39D463F9D77E18865
SHA-256:	D5C0E71B5E486F80156D97CE348DBB26D91B29B62140E2A8D6E411DEA93603B7
SHA-512:	6FCF920528C73D7B9DB185C8C3545FB43058C330F9CC96F0F92F51DEF8C66FD2CAD725A10601294CC15956D3E2DD97DE3176F24B55EE5E0B380B4A135257237
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 ....K../....."#.Dx.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....w..^.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ....K../....."#.D.=.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .L?.L../....."#.D..x....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....2.0.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...aL../....."#.D.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Rv.....

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):	748
Entropy (8bit):	5.6180206849852
Encrypted:	false
SSDEEP:	12:5h6OLEY1l0EkCh6OLFQpVUkKhh6OL8+bbk6zh6OL3kN:5h6hweCh6PBKhh6Z+bAgh6xN
MD5:	CFC2B243CA5065BB7096699ECECF0998
SHA1:	E7869C72A9BDBD2BAB8486C46C1258FFDBD79D9E
SHA-256:	1D14B799E964687952CEFC883D608DB39885F2377A5379B1CFEE9959687EC5B5
SHA-512:	A0C8A950F7787C2819AAC49EC4C7242AFA53A5467619F7A66E5B0333ED02693ACDB77CD9FC704B7CDB5B9674253664A35F9456AF7367F90BE9C11D7AF9588E8
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...K../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....Z@{v.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .)j.L../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....I.W.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js . .!L../....."#.D.K.....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 ..5jL../....."#.Dz9.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....a-.....

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):	976
Entropy (8bit):	5.680356511064494
Encrypted:	false
SSDEEP:	24:UB4v4ZwzXLnGB4v4XwzXLnuB4v4flwzXLnmyB4v4k5wzXLn:8MPbn2MlbnOMSdbnPMWbn
MD5:	3679E78C91A60D6F7E5EB534618DD292
SHA1:	5F5D9D5D17943AC77C20F0EE5F988271E61577D4
SHA-256:	93E5B8CF602B6AA92D2C13F1EA5749911721BB1F8362B5CCEBCAD171E6592CD1
SHA-512:	0EA4AC8F2B393A3BE7DA108E0FE933E665D1B60AC1A59EFDF712D3112750E661D11128A0E602DDAB24D3BAE1C5FB970338BEFCBEB35157A5C730E755678257FC
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 ....K../....."#.D1(.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....@.....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 ....L../....."#.D.[@....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....}.6.....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 .\~&L../....."#.Dg_.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....f+T.....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 .H/oL../....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....D.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.569753701207293
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQ0Pxel5GFCaa+41TK6tf:NRMHdX45Gda+Ex
MD5:	6E562528BFDAA4C7EA258C7456CE6B55
SHA1:	A3B63A216AA0EFBF8003F7E94C73E0381512EF0E
SHA-256:	07E44B0803D4F31F30F2A570F5610864C82C6F00FF403C26E5B802DA525071A2
SHA-512:	983A33F4E06F711426D45A187B3E9D73A428C91F97ECDD0467AB049F07657D05D7320ACC1904BE4B81868D5C67F196CDEE30C2A2519BC725F4A482FAD6B0975
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..a.L../....."#.D..S....A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....C.....

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):	422

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Entropy (8bit):	5.549634776966673
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuyvl/4sdo11TK6tes2VYOFLvEWdvBIEGdeXuMDzo11TP:BsR2EseqsIjsR2Ese1nWgol
MD5:	B81D2B7851A24A49662DC2DAECC26D73
SHA1:	BE3C83902E18747297DFEDEB2B0155D4744EB1CB
SHA-256:	01F5FB2C6CDDC79AD8D724AACA9AFD4380FAD0D5FA8A69EDFAE52B09414DFE06
SHA-512:	3BE8982539D258CC0DC610DD26E47DF03105A34266DAB13CB11BA93D76D669F694C2F3302079F6B2B5D4062C2332946A73400F513C8F3D9D7F0A90E1AEE18DA
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ....L../....."#.D..=....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....6T.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .@.nL../....."#.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):	404
Entropy (8bit):	5.688638980486722
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ1sFNVTB7OhKlvA1TK6tLleaVYOFLvEWdwAPCQqPiciB7OhKe:RbR16mshVJkFvbR16bgJk
MD5:	9E0E7204404C2F54522F6171C2BFBFC5
SHA1:	1BD47AD330EF433CB8D9508DD31F49AC03E1805C
SHA-256:	886D8AFB308D6D55B098C23414C666563AF60F4874992A682F92157033903227
SHA-512:	36B1BC037D6EF436DB713A28C4F6878478DFD77FD217D2003A69DF087DCB42385BF45857670999B07D65B1502232D992B6E9389D5B70C6158EEFB7FEFB9C43C
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ....L../....."#.D<i*....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....?..y..... .0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..LIL../....."#.D.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....M..^..... ..

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):	422
Entropy (8bit):	5.598042019878591
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuU7l/GjQdFt1TK6tk+s2gEYOFLvEWdGQRQVupVsJklUjQj:B2geRHRQjA0y2geRHRQxql00
MD5:	AE6DCF23ACA63D278E24B9B7D40E7674
SHA1:	72D14585C987F233E88974E4F08E6E6EE27454A1
SHA-256:	1EDA179A142B66B4640424FB0C83CDE45B145E961ABE93A917C667DB8EC95121
SHA-512:	1674252C9DEACA62E6C64B7C4C7DF7F462C0CCE7949B8AD36206296BFCAFFC07F92EA2F86BF22743CD9863B38DB641537593A99D1251A16EFBD5D119683467A
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ....L../....."#.D..=....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....*s.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .&hnL../....."#.D.&.....A@..{o]...9o|..qY....T....{.. u.b..A..Eo.....A..Eo.....u.....

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):	824
Entropy (8bit):	5.667646617158866
Encrypted:	false
SSDEEP:	12:WyeRlWLK6t1wmyeRl/6t1wEyeRlys6t1weU0yeRll/t6xc6t1w:WJw3fwmJKfwEJqRfweFJTgBfw
MD5:	8A7F19E20E235DF3944190CB9F035E3E
SHA1:	F8209C081C5B2346E605F5E0521917DE742D3E4F
SHA-256:	1E2F1095197E136692C51420A73598585FECD296016674D1EF25425FD8CFD39E
SHA-512:	DA4F75DA6D60BEB318CA11D9E3DAF153419E9A071CC90889689D82E2FC74271F33D8C7B2366A5157C19A5424DB63196BB4E750B032DCE545DCBBC375FE342A F
Malicious:	false
Preview:	0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .5.K../....."#.Dk(.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... ..5.....0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .F..L../....."#.Ds.#....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 .d;$L../....."#.DV.....A.t\a.....x5.'OuE.C..@.....x..A..Eo... .....A..Eo.....4jW!.....0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...jL../....."#.D.w.....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):	436
Entropy (8bit):	5.597686995512026
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuwq2ZqwK+41TK6tOnYOFLvEWdhwyuMqTdJfqwK+41TK6t:wRhkwK+EKRhxYLSwK+E
MD5:	6A83FFD2B2477CF25483DAC838AFE454
SHA1:	B64D8411AF1B4DD73AF367D3A729879D360A39CD
SHA-256:	2702900BFADD6BEC617D15022A3EDD0A78D1F4CC80011F07E02DAE220D142AC0
SHA-512:	ED61102BB9A912E6F615969A3CB97C819991D20D2E04462D1DB18E5A8DB96BE76B831615DB562D83D6A42A6F1B77F53E60E597E95E2916F715E41F7B8CD27B9
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..P.L../....."#.DAF*....A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo..... .....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...lL../....."#.D.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....N.....

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):	920
Entropy (8bit):	5.6508098067615515
Encrypted:	false
SSDEEP:	12:/RrROk/ifLEttvRrROk/QopfLEfRrROk/QfLEC3RrROk/RwfLE6:/PJ/i4tlPJ/1p4fPJ/Q4C3PJ/Rw46
MD5:	C60EDD2EA4BCD7AE89E3B4BDCB1A15C5
SHA1:	4E863F7C24B1BCE4F144D3051F3E03E632D76475
SHA-256:	7415244384C91169538A79AEFB3DBC30854A585BFD50A04398B0F0C16E4667BC
SHA-512:	8C262E9039B02992E7E0F4BDD45C27F2DB28072918481D8DB68602860979599E4F8205407DDD9A67AFC3C16547EA32E045596F7FF9578E429A018CD6F94B8B78
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .#..K../....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....V.o.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....L../....."#.D..#....A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....D.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js . .9$L../....."#.DH.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....k.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector- files-select/js/selector.js ...jL../....."#.Djg.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....q.....

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):	744
Entropy (8bit):	5.681257242135361
Encrypted:	false
SSDEEP:	12:xqTyiNCPLndBqTfdbZNCPLnQqTARNCPLnbqT0Q+xNCPLn:A/MnmNXMnHM/MneYQ+fMn
MD5:	466553932AB460E3E790AAFEDCC9062E
SHA1:	B545302A8EA1ECE56935913A27F702B30D68B163
SHA-256:	D90622A67CCCA96015D2D78BC510664271AEA3873468271337D4A88136227C3C
SHA-512:	860C6FEE0003C8FEF36DFEF69A049BB2FCF85375E6FC16CE90E45E2D0326F9E4832F33E012F8EFFB045F750AC8A85327C10994243217EBAE4097B3B654C36BF
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...K../....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....=.V.....0\r..m.....:... .f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..\.L../....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:...f....._keyht tps://rna-resource.acrobat.com/static/js/config.js ...!L../....."#.D.$.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:...f....._keyhttps://rna-reso urce.acrobat.com/static/js/config.js ..*jL../....."#.D.4.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....-.z.....

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):	828
Entropy (8bit):	5.723439398601371
Encrypted:	false
SSDEEP:	12:zRMMsDYRMCb2NsDnRMRVgsDqRMH8ZsDv/:z2DYFlDnYpDq+8GD
MD5:	991BAE52DE0EBCF0AEA5176138365B7D
SHA1:	2E0DDADAE6D90ABD6D8A8C13D881BA36E56A9515
SHA-256:	64BC6795F6A9F188E962B4768B96583D3196BBC1B69AAC754AA415728ABB21E8
SHA-512:	E0A907062687146251B205E7EB64901FC97465EFD6C5F40E0FF7289BD0006C86EBBEF76AEA20D534E3123BE9BBDB08F6FB2CBEF09F3C07F1366480EE99869B2

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..K../....."#.DF(.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... .q.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..;.L../....."#.D)?=....A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....$.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...%L../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo .....A..Eo.....x.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...nL../....."#.D.....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):	840
Entropy (8bit):	5.65498625438588
Encrypted:	false
SSDEEP:	12:6lJRKYoM3/UlJR9xgoMfClJRgfgoMglJRRKYoMLl:YpoM3/y7KoMYi4oMWn7oM
MD5:	33B17EAD13CEA9F24E2BEA8351F4BAD7
SHA1:	4D15D0EF1D6F7608F669631E3C708BE44030984B
SHA-256:	5C664CE5237121ABE24FD6A88A1BE1487A38C606A5149584316718022C1AD6F0
SHA-512:	96A8A0D8EA3F12575FA0BC8FE4C54F028FD293E6DC31188B497B1CF2435195BFE93E25E5B4B1342CD742AB7EFD308ADD0FA4772DC81AE33C2CC265A31E0BCI DA
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ....K../....."#.D.@.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..E o.....o?.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ....L../....."#.D+.;....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.... .....A..Eo.....g!.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .,.%L../....."#.D.....Ac}.H7M=M..-.....Ix..R.I ...}Rl.$q.A..Eo.....A..Eo.....B.f.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...nL../....."#.D.....Ac}.H7M=M..- .....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....iE.....

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):	892
Entropy (8bit):	5.663371056996808
Encrypted:	false
SSDEEP:	12:F8hRrROk/WJ2Gn8hRrROk/Ll2w/8hRrROk/WHl20/8hRrROk/8J2:UPJ/82GSPJ/Ll2wqPJ/4l2jPJ/8J2
MD5:	FC8239DC9B8F2CAA42527F075E9DC57E
SHA1:	C4025051AC4EC9F38BA7155BEAF7649469172657
SHA-256:	8513E4B29049497B1FE4740EABDC3763115A9B54B208E912CFB6CA871BF6E358
SHA-512:	2C899907AB97E8048D83CE8BF5103B83D2DFFA7E05A738ECEEE162BBAE039A9CF0616C7F69C8B8FE984C262289B50E1F00CC833618AD08D3C9F1DB8478FB22 9
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..K../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo..... .....A..Eo.....=?!.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...L../....."#.D.z#....A..%.k.SZ..~W.....:)'B ..ad.....A..Eo.....A..Eo.....J.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..6$L../....."#. D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....wz.o.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js /selector.js ...jL../....."#.D5].....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....4:.....

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):	852
Entropy (8bit):	5.728714641914765
Encrypted:	false
SSDEEP:	24:ehC17JICVQhCxJJICWhw7JICHj/QhKanpJICD:e8152gTWuEQKzD
MD5:	1F8236CEE01B590C0682FCC3D1EBBEA4
SHA1:	472FF051DFFF70403402D8391EE27E8A51146573
SHA-256:	1667284F533D41791585C4A2B36325FA7C3D9E4937DA0AB3E26D503B8F098DB3
SHA-512:	E12699275B414BD3037F9E42564869D43393C62E5613410E1EBCCBC56790D7F50C4B03F4D343FB6FE2A374D1474B2058CFB5B09A9EE4DA49A659E38241638BF1
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...K../....."#.D.J.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A.. Eo.....z.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....L../....."#.D2.#....A.;"./N_.,.:C..2....9L.H...3:...A..Eo. .....A..Eo.....7.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..=$L../....."#.D.#.....A.;"./N_.,.:C..2....9L.H...3 :...A..Eo.....A..Eo.....U.b.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...jL../....."#.D.....A.;"./N_.,.:C..2... .9L.H...3:...A..Eo.....A..Eo.....rY>.....

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):	832
Entropy (8bit):	5.674739802854444
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuQxjLzgm2d/1TK6tZOEYOFLvEWdrIhu4QqEBjLzgm2d/1TK6tS:0RAReZR+sBHReGRCReBR79ReK
MD5:	7CE670AD31A0BE49C8AAC2798175AF5B
SHA1:	CE7A95FFB6E78DEE7C69579A674440488F203213
SHA-256:	B203DC9BAA7196D8A8B38FFA7421861927E46DAFFB3DC457C0B71DE52F2AB4CB
SHA-512:	77BDE80D06D014A37D8956590B9851D1669036B4E80D8E4AB4C5555B03CD55373206A56F48D0DCE797B8A5A5A42D2906D957E183D4BB0D48266334107BC5F24E
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .;W.K../....."#.D6.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....?Y.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .{..L../....."#.D.P#....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....3.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .B.#L../....."#.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....2.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .6.jL../....."#.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....V.....

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):	752
Entropy (8bit):	5.68591812628379
Encrypted:	false
SSDEEP:	12:6JJKYk1vIuJJK/+IIiJJKfltOlGJJKaVvIvl:6JIguJI9IiJItDGJIaVwv
MD5:	EEF9D46111F61AB2214C346EC514A03F
SHA1:	B233BB3F43A447080CA657505CE9514D1C23F108
SHA-256:	7A2B213039642D4EF344905CF9F6DCB46D035C1B3B52E620399228295979A59F
SHA-512:	389A1C59CDC4A321749870983AAD2CF31E129864A3FD9ABD9460C11A33C119CBF5DF9780D7789F0EF8668283254824D5B6FBD41A290408167282E110601CD654
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ../.K../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....\9gf.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....K../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....&.y.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..A.L../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....pn.}.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..cL../....."#.D.h.....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):	428
Entropy (8bit):	5.676855770004914
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvubbK//YVbhUDLYtmOZn1TK6teWYOFLvEWdBJvvukLNtevhUDLk:xRBJYbuDcFZLbRBJxppDcFZL
MD5:	A7EB2BEAF27F26671E2408EEFB19601B
SHA1:	DA9A8D1BCCE5EFB73AE1B44E8C17F608E51FFB75
SHA-256:	524ECACA4E6744813F701CFEA8BFF1011836555A006408E7DE30D5693D430B83
SHA-512:	D874EC487B2A9C74E33EB3840C8391D4DE2F9AE821DD0AB9F245CB1FE5312D9E387E389A720D814E58C0F4126A3A2E4A296CB50992A3D973F9241F25E04C662
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..7.L../....."#.D:$=....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....^.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...nL../....."#.D.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....!I.....

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):	844
Entropy (8bit):	5.656602815767283
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7ZlGVPu1TK6tAesRPYOFLvEWIa7zp7jqeWVPu1TK6tssRPYh:BPHhGcuZPHkcpPHrUcmPHBxUcL
MD5:	D3E7D50E10FD2671F208601C60A87334
SHA1:	80F4353ACF22E506161DE5A748A1B76E6C871EF4
SHA-256:	0B3BC75938D798401301495A30AF778B01213EE375B68C948996CC66074B2360

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
SHA-512:	0ADB56411B57AEC443681AFBF8AFFDC10BD6E608F312A56F623B591E739D6CF4F0F316602CBE718AD0A6597887EFADB53DCFA218B91F404B3254A254AB3BFE29
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....K../....."#.D,(.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....)]..... 0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....K../....."#.DLq.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....1u..... 0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..B.L../....."#.Dy.x....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....4..... 0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...aL../....."#.D.G.....A..L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....cL;.....

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):	416
Entropy (8bit):	5.622212384654037
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QEp/tXZPiM3Y1TK6tr2KPYOFLvEWdENU9QOXdlPiM3Y1TK6tS:bJRT9rzPr05rJRT9rPr0k
MD5:	22C0EE7BBA436199FF3CE85DE9701A95
SHA1:	248570F40E32E54504FA870B3EC4F1342B08A03B
SHA-256:	DED43D00E1F61B9418D94936E4A6D945A9097E2717B7CE3699D3504018A5BCB9
SHA-512:	D64F1CDEB83BB009FDD9BC136767B7C657B458554572F927B190218B28481D275D863456DE6A7286090208431CF710E7E0D62701EE3B771D67BAE729E5532902
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....L../....."#.D.O.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....Z..... 0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..MlL../....."#.Du.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....9h.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.625442050858557
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQw/rGjBRCh/41TK6t7eQt6EYOFLvEWdccAHQQR9bjBRCh/t:XRc9pyDi/EtfRc9BDDi/Em
MD5:	3A08F943E6FF384FDF68BA96EE67713B
SHA1:	F29833D42B603A540D1B26B80A8A42DE908CBEC6
SHA-256:	CD7F7B15E8E7A030D4E060488469E19CC8E82A7DE729C704E3C37C3FE0EDDC6D
SHA-512:	BD7D5F41A4D157ED2D0B24909ABB532EC96E401AFB24F41C7E609ACC78E4D3EA4809D1DFCFDC868C2073D3D45D9EF8161954B3BCACAB3F0B795B16400B3A403
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....L../....."#.D5.F....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....5c.0..... 0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..3oL../....."#.D=G.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....XU.....

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):	462
Entropy (8bit):	5.6329217797133735
Encrypted:	false
SSDEEP:	12:bs6xRkilLlF4n7lDs6xRki/ElLLlF4n8:brxplo7hrxp/2Lo8
MD5:	52DB1C1F0C4EC2A8031B800ED3045C5D
SHA1:	BC1E2C082B1EA81773B99DF1FE612AAEEB36F162
SHA-256:	D5B4670AD44AEA3B8F2E900C3AC75D4BCF65007389FD549441BC79873B3F60E1
SHA-512:	8D3706A40971907AFFA508EB5ECDE4003BEDCD5C099A07314EF9153A530AFCA11467015A754A186CCB185D5AA1F9D663D6FA5BE49F859FBFC4D8750690C6292
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..3.K../....."#.D.....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .v.$L../....."#.D.....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....+/K.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Size (bytes):	430
Entropy (8bit):	5.5835152598070055
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFufp1//FEg941TK6tchYOFLvEWd/aFu+stXYUMxx3w941TK6td:WR9f/N19EGRptIUwxg9E
MD5:	2EBEF0EC33AFB5B98F2CBAD305890D2C
SHA1:	B9D9A6420433B15D66C6151B5B7E970CFE87E503
SHA-256:	BF39241CDA6DE4ED5353E99773F08789E0DEC11BDABBEBD0164B06F62A151CE5
SHA-512:	F7E8AF78E68E9449A6D1C873BEAF3FB6C3AF2A9DD9DA1000A32E32A7B1577727F8D3F646590C8DE59962798BC11E31F99493E3F86B1EC030440CE9257BF01B7
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ....L../....."#.D.6>....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....f.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .v.oL../....."#.D.q.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....:P.....

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):	416
Entropy (8bit):	5.591941095731364
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQwp9/F8GoBMqVd3G4K41TK6t/FER9YOFLvEWd7VIGXOdQu:2DRuRV3NtoB9Vd2kDgDRuR/4oB9Vd2k
MD5:	ABBD08752230A44B4775FB9D53033E1A
SHA1:	8799D39B7F8EA5D99D89EC62B89E10943040F227
SHA-256:	4A3346D811AA962CA12D89581BE2B52CFC7ACF7CC27868BA5B8E7076FCCA4EBE
SHA-512:	B86247E881435EB0FDB121C3DBCD6592DD5FE05D728CBC5F7E20EB34EEB8E7DF9CD05886BE121FC8CBF819E3502B529D2A32DEEC22BC55F6BC7F1376079FF CAA
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....L../....."#.D].>....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...oL../....."#.D.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....8.....

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:	modified
Size (bytes):	832
Entropy (8bit):	5.697525464916001
Encrypted:	false
SSDEEP:	12:+RQQ8Wzrn2RQtiJzrneURQ6PzrncRQZzrna:+78W/n2ca/neUh/ncy/n
MD5:	D0957E392C1F5D9AA4C1BD689B7C9ED9
SHA1:	FDEFD26679CCFB1D0900ED0DA437B930A90B34E7
SHA-256:	D49B46B64FA91418799BC336791FC761F5B2ACAA7AAD3A45D552C4BAB52098CE
SHA-512:	75FAAF7E4E2A7F42780D7414F4B6CB823A914CB54B5E259215400A2D1A60852F0DEFB789D620272EC8D6B333E5D0135AFC0072CCFE878759BA86277C91AE197
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .N.K../....."#.D.b.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....N.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....L../....."#.D:yG....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....[.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..B&L../....."#.Dj.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....Q.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..oL../....."#.D@.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....B.....

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):	420
Entropy (8bit):	5.607169613212863
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuiqhyC8n1TK6tVq9/EoXXYOFLvEWdENUAu5EltK7JduyC8n5:xhRTB7Q3q9DhRTglEJdu7Q
MD5:	830CC48540EFAD3334D2459DC8D9835F
SHA1:	65A88997D26ACE4FE3A98BAF84EF17CB3B9DDEE5
SHA-256:	8CE264C540A3CF502B0D8763FC59954E1621FA0AE6762B09D1BEAAC85F128AD3
SHA-512:	0BD71E0A51EE93BDD7C2AB9F525AC4C3FA6B0190E39F51157C67C58D21DC9A311506B0DDF1D59FFA6ED47F4A882DBA2F36F20D72D64B7DE1083C42D9AC8E0 2D
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..N.L../....."#.D.4*....A8.../...;.\\o....1.....+..A..Eo.....A..Eo..... .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...lL../....."#.D.w.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.. ....:.m.....

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):	884
Entropy (8bit):	5.668322497517114
Encrypted:	false
SSDEEP:	12:nRrROk/Vum5RrROk/VSFmf1/RrROk/VUmPRrROk/Vpmn:nPJ/N5PJ/t9/PJ/vPPJ/O
MD5:	4B859E4BE10FBC846849DC365B6D48C8
SHA1:	79CD45AECD852CF70C2A5E31A89F30D23402DA79
SHA-256:	0D55CA277B6F488EE8E20A50EC40E02EF860E79436664B5DF9948B785B045465
SHA-512:	08E47DB1426FA219B2C028E380F6C28340EB132AD5298487A276CF5BA321C883FFFDE5A1FCE7E06D74AA79281869408850942 6B4DD615BF039BE61BB46D67268
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .[.K../....."#.D.b.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....}.0.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....L../....."#.D..#....A ./.ev.....N~..6.b.....$.j;: C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .VS$L../....."#.D,F.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....<.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .{.k L../....."#.D*.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....[G0.....

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):	420
Entropy (8bit):	5.627285263355503
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu1F/8S5GAdm9741TK6tk+Z/lXYOFLvEWdccAWutXt53FGAc:qxRc6Ydu7EKyxRcTDldu7E2l
MD5:	F24CC2FA3709BBC3F582126E947CEF2D
SHA1:	AFD65B9926F834B56F0887C4E34486B6C66D3D21
SHA-256:	79A343A88E158190A45295A9C78C711A7FF35D3263627D2A2C3B66BF859C670B
SHA-512:	BD8F11F79BDB52C4FD0A60DDF533CC594FBB8F3649B2A8467780DA5FDD0312F9687D8FFE553981C9FB400FBC99C751AC6064633B35DF9A248ABC06ADF1C0D9 F
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....L../....."#.D..<....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....`t.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..[nL../....."#.D.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.... .....A..Eo.....7..*.....

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):	408
Entropy (8bit):	5.591762206106413
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVu9+0WZJn1TK6t3+MOYOFLvEWdwAPVuIPTTrJn1TK6t3tl:2R16WnL8R1hpL
MD5:	9C2C43611A631E4437089CC87AA82B56
SHA1:	CDF6574A9DC6296556057E9B83E697DC47D19680
SHA-256:	3FEE3BD48DA260649C8D5BD3E15F86E362F06DE3DF91AE50AC9EBD554E3051E0
SHA-512:	3F6EEF990FBA98718D4DA5A4D0B3A9F2D524909F26ED56773C58D6661FC36614E22C33296D3AD73ED1419FF01AB6A9C69929B22E4E273E7B4BE422383CFD8A1
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..L.L../....."#.D..*....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ....U.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .1.kL../....."#.D)_.....A.....k....F..D..O.n;[.1m.....=..A..Eo..... ...A..Eo.....%.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.686299848682821
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
SSDEEP:	6:m3PXYOFLvEWdBJvYQU9/OwdizhcsBXIh1TK6tl3PXYOFLvEWdBJvYQjaXBYJzhcB:mxRBJQhNiDB0uxRBJQDRYJDB03
MD5:	EE7F5CE0C78503CB889D9126BCE48AF2
SHA1:	2B240C2CDBBB00E8CA33251351DBC5A617F1E839
SHA-256:	163CA1A45909EDF47C81F923C66AB3E23470EB80F68413F4CC519473F6DB8B28
SHA-512:	0F10CF565AAFB149696919E503C35D036753C797C324DD430704D1A592E67B264E7561B8C3AFA3B8B02E7634289E47FF7BA1DD2C6FF5EEAD6854206A80776261
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..Y.L../....."#.D..=....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....i.. .....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .N5oL../....."#.D.V.....A...k..`..N3.... ..d..$[.....{.A..Eo..... .....A..Eo.....^k.....

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):	912
Entropy (8bit):	5.657081471129071
Encrypted:	false
SSDEEP:	12:3RrROk/shDcX/lHRrROk/sSwFcgRrROk/sW4cVdRrROk/sNxc:3PJ/Eg9HPJ/iugPJ/1VdPJ/z
MD5:	186E2F4920DF5543FF28F5130AFBD6DD
SHA1:	F8C87B88407AE9B26DF749909D56762DB0B906A0
SHA-256:	161FC2E20FC8B3C27395FCC97C4E874F0391923ADCE941A7017827B7FD6F56AD
SHA-512:	EF23CB1172738F7FC5AC31E4B780C1EB0F2E29065509560192711 0B1DB624194EB6863DD4515EDEFDF178C907DFFA365BE9AF19F9B8FE7D9847676761711040A
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .k1.K../....."#.D^.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....h;.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .;..L../....."#.D..%....A..... 9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....Y.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...$L../....."#.D.y.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....9@,.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .>.kL../....."#.D.....A....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo....._I.....

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):	2064
Entropy (8bit):	5.3021350028110374
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QP8QEC9wM0V4ZSeMbyjfPY7qMLi10NA1KGXq4/+EifMU6:h1zZ4+dsp6kQi19IRdU
MD5:	AD25793CFD5C62C7FF46248875D187EC
SHA1:	735A59129FD610411B1958B8321B5ADE52BA2830
SHA-256:	3E9033784FB861E482524E48231E8227BB57A0BF585DF77A070DE8CB59C771B4
SHA-512:	53F2A3046E6C6E7AA6915FA7AA41B0251A0C6006E9ADF81862AA9B88BCF63554C1A8535D4008BEC0356197651AFB8AE229FB19413030029920697 06F71AE8DCF
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./ .....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./..... .....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z. B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./..... .....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0.....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):	292
Entropy (8bit):	5.246916296492127
Encrypted:	false
SSDEEP:	6:qTHVq2PWXp+N2nKuAl9OmbnIFUtwfTlX+gZmwyfTlodsIkwOWXp+N2nKuAl9Omb5:qpvaHAahFUtwfBz/yfM5fHAaSJ
MD5:	AB4AF0CFA8C85470ADD23269C1C03EF3
SHA1:	F309338ED4EA3C9C89ED10F8C5815273ABD92276
SHA-256:	30B4C535F442ABEFB9D9EA885A06BF4021A86E50AB384E0A33EDCF78897F16C3
SHA-512:	C5CC65656373E0BD022BC4DEDF6D5BA553F3CA6E42AE230C09A00AB2A94E900C788B4405C11A9B77BF036CF0DBF56174EF9E18539F4A0A456D71FA68A0E7C3 8
Malicious:	false
Preview:	2020/11/29-11:36:39.275 1860 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2020/11/29-11:36:39.283 18 60 Recovering log #3.2020/11/29-11:36:39.284 1860 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):	1835008
Entropy (8bit):	0.009659826032596219
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDgsMiDgsMiDdsMhCDOsMhCDo+sMhCDo+sMhCDo+sMhCDo+sW:trrCXonononononono
MD5:	21243F04C89A197BB6B7F6F83FC3143C
SHA1:	86C39801641D4689AF8792AFB690A0CADBE81263
SHA-256:	B71EB44A7471A903DEFF3A492C2981A68BFB32AB60A5D162E43364864DE135A3
SHA-512:	F36B2C48C1F0C30494202D6990352BF864F6D0EF073D8981C8033ECEDE9A0B55F90B422110C91DF95B7E714B5F7F1928FA75A64BFC2A9723234A7073AC945316
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129193634Z-198.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.6308136311381016
Encrypted:	false
SSDEEP:	192:DP/HhbwJX0wqpYjfXB2xyTKyGVDfwSIjNU6TTFnnBUlRmDRJO/k1g4bv1X+oqsuW:jlTXy/VnB/
MD5:	CE0BCEF8C33C0F4B51EA9060433D9956
SHA1:	47E8E11FDDA86F74D7C46573B35472E2643D9087
SHA-256:	FDC9E76483D447C17242C71D7E9B8E4D57AA6F8B34A04FAC9AF5EFD7F666ABBB
SHA-512:	C5ABAB9A9730125CFDED5B87062C6CC425698F7855D32906777D60BCBB0FA8D32A2DF4BDF9EA9DBFC8212C40643A013C13D8C60E473353CA2B58F6D8A85719F
Malicious:	false
Preview:	BMV.....6...(...k...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
Entropy (8bit):	3.388557492247401
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQNOhFVCsL49IVXEBodRBkRkNOhAVCs749IVXEBodRBklkNOhgI:iGedRBjedRBQedRB2edRBU
MD5:	FE6304CE77A92D83BE9804F733691937
SHA1:	BF83C5A27CD10DBB449D4A4939395D3B68219632
SHA-256:	69A5B913D82A2A297A8BF857775BB720527A305507A3E78069757D4B8DFC4187
SHA-512:	641026B928C15A089CF4C10D827C3A3537AD223B46C156A2F16B01491E357D5CF49959393D6E35F8A25005400830C5F47EF9738391587E45FF145CC21E239BFF
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):	3.202035483362059
Encrypted:	false
SSDEEP:	96:zq7OhFVCPW949IVXEBodRBknNOhFVCstLR49IVXEBodRBkNkNOhAVCssd49IVXEG:eyiedRB/LGedRBgCedRBEyedRBo
MD5:	3C207ABBE4AB58B3660EA798CDE2DDBB
SHA1:	2E100792CF25BA064F2D126E14DD20B8A01E9DFE
SHA-256:	C1BD41D0DE2E7657D4A463BE55A164C2CEC9AB63F86C8DFAE010636022363A10

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
SHA-512:	94A0A30A21A37B248E4744118DCEF8066C15063D09E3D31101740854338BAD46340CD7ACD65D988E02BB502D47CC41A59B02C7FFB973E3B0DCDD2AF84E07F81
Malicious:	false
Preview:	.....*Y.P..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1488	
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

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.8953416079630445
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	contract 27.pdf
File size:	133942
MD5:	b5da5a1891fdaa1449189146385ac7b0
SHA1:	ff748311fe2f1fd75e4d7c52833914746e986086
SHA256:	03fbf86eb9c46c37a236098d47bd5b35d92d0a2f07acdce28b3b5467b2cf95f6
SHA512:	fab2d725f81f6041b58c4d03c5c69771c62c66dea258df68c87a62ee535ab8dd91d109a9f096e94739eb31c585219e53c37c2a378a4f96f277e35173fffd9cc6
SSDEEP:	3072:UWj6p17PP1cNejXT9Kmu3PCPXI0jZ2/OomhIHOTXy:UWjm1z1UejD9KnaP30H7
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 15 0 R/MarkInfo<</Marked true>>/Metadata 316 0 R/ViewerPreferences 317 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[4 0 R]>>..endobj..3 0 obj..<</CreationDate(D:2020

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.895342
Total Bytes:	133942

General	
Stream Entropy:	7.972816
Stream Bytes:	123259
Entropy outside Streams:	4.271644
Bytes outside Streams:	10683
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	23
endobj	23
stream	7
endstream	7
xref	2
trailer	2
startxref	2
/Page	1
/Encrypt	0
/ObjStm	1
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

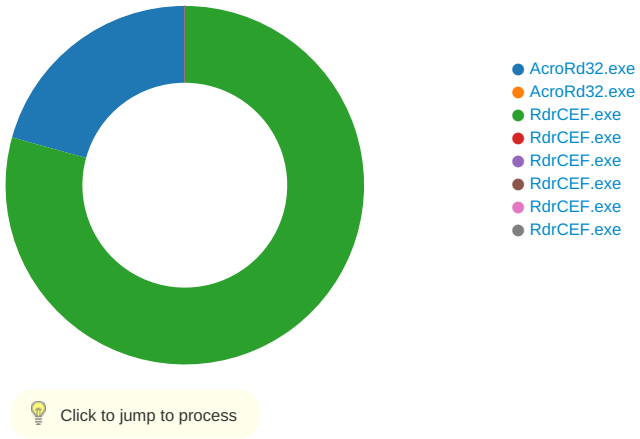
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 11:36:21.644170046 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:21.671312094 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:22.714082003 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:22.741303921 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:42.768143892 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:42.805552959 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:42.866297007 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:42.903403044 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:43.819376945 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:43.858511925 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:43.861967087 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:43.897495985 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:44.828515053 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:44.863909960 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:44.878510952 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:44.905590057 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:46.828938961 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:46.864821911 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:46.878935099 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:46.914340019 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:49.257488966 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:49.284702063 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:50.837589025 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:50.873145103 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:50.884459019 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:50.919855118 CET	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 11:36:55.148260117 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:55.228395939 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:55.914957047 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:55.942126989 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:56.679868937 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:56.720053911 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:56.780754089 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:56.807929993 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:57.493659973 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:57.520797968 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 11:36:58.151819944 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:36:58.187248945 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:02.275271893 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:02.311019897 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:02.990792990 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:03.026329994 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:03.689018011 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:03.716244936 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:06.386311054 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:06.422036886 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:10.984772921 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:11.034876108 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:28.473565102 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:28.501169920 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 11:37:31.519602060 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:37:31.556441069 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 11:38:02.899945974 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:38:02.927180052 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 11:38:04.299647093 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 11:38:04.326908112 CET	53	60633	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 3528 Parent PID: 5696

General

Start time:	11:36:26
Start date:	29/11/2020
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\contract 27.pdf'
Imagebase:	0xbc0000
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
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	BF65C3	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	object name collision	1	C1AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1488	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	C0EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock3528.1.4018593677.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	C42657	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	C0EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129193634Z-198.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	C0EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	C883C8	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	C883C8	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	C883C8	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	C883C8	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	C883C8	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	C883C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rd1lm56_lxo89e_15c.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	C0EA85	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	C0EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1v8x1wo_lxo89f_15c.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	C0EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R171og2q_lxo89g_15c.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	C0EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rbcgn9g_lxo89h_15c.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	C0EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1gcq0l5_lxo89i_15c.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	C0EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1488	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	C4D405	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	C0CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	C0D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	C0D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	C0D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	BCEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	BCEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	BCEA55	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	C1DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/contract 27.pdf	success or wait	1	C1DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	contract 27.pdf	success or wait	1	C1DF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	C1DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	C1DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 63 6F 6E 74 72 61 63 74 20 32 37 2E 70 64 66 00	success or wait	1	C1DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 30 31 31 32 39 31 31 33 36 33 34 2D 30 38 27 30 30 27 00	success or wait	1	C1DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	133942	success or wait	1	C1DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	C1DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	C1DF47	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	C1DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	C1DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	C1DF69	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	C1DF69	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 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	C1DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 1488 Parent PID: 3528

General

Start time:	11:36:27
Start date:	29/11/2020
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\contract 27.pdf'
Imagebase:	0xbc0000
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
						Source	

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

Analysis Process: RdrCEF.exe PID: 5668 Parent PID: 3528

General

Start time:	11:36:33
Start date:	29/11/2020
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:	0xaf0000
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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	BE59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	5	BF83E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	113	BF8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	216	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	BE59E2	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	16	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2166	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	8	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	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	BE59E2	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	BE59E2	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	4	BE59E2	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	4	BE59E2	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	4	BE59E2	ReadFile
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	4	BE59E2	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	24	BE59E2	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	4	BE59E2	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	24	BE59E2	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	4	BE59E2	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	55	BE59E2	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	4	BE59E2	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	60	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	87	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	BE59E2	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	4	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	55	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	59	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	BE59E2	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	20	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	16	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	BE59E2	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	20	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	238	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	286	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	BE59E2	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	267	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	BE59E2	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	196	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	32	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	BE59E2	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	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	BE59E2	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	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	169	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	BE59E2	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	16	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	BE59E2	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	BE59E2	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	325	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	32	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	10	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	2	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	BE59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	BF83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6248 Parent PID: 5668

General

Start time:	11:36:36
Start date:	29/11/2020
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=1720,575729243448011 4666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7546301349673146790 --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=7546301349673146790 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
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: 6272 Parent PID: 5668

General

Start time:	11:36:37
Start date:	29/11/2020
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=1720,5757292434480114666,2542267608491848794,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=12817687695606234436 --mojo-platform-channel-handle=1688 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xaf0000
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: 6424 Parent PID: 5668

General

Start time:	11:36:39
Start date:	29/11/2020
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=1720,575729243448011 4666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2753125301934643863 --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=2753125301934643863 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6560 Parent PID: 5668

General

Start time:	11:36:41
Start date:	29/11/2020
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=1720,575729243448011 4666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12075229495714680774 --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=12075229495714680774 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6796 Parent PID: 5668

General

Start time:	11:36:48
Start date:	29/11/2020
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=1720,575729243448011 4666,2542267608491848794,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17952855729266451437 --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=17952855729266451437 --renderer-client-id=6 --mojo-platform-channel-handle=2092 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis