ID: 324349
Sample Name:
image20201127115854.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 12:38:25
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

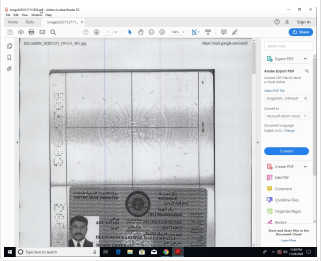
Analysis Report image20201127115854.pdf

Overview

General Information

Sample Name:	image20201127115854.pdf
Analysis ID:	324349
MD5:	94481d1abb00f00.
SHA1:	13d999eac4b938..
SHA256:	55e4417b68134b..

Most interesting Screenshot:



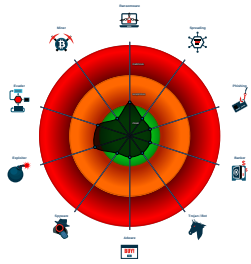
Detection

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

Signatures

- Contains functionality to access load…
- High memory usage for Adobe Read…
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 1004 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\image20201127115854.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5976 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\image20201127115854.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5080 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6148 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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3833046004073922652 --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=3833046004073922652 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6180 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1704,16962285166967419287,12971905902240953692,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8625267804615807816 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6232 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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2248458598877757648 --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=2248458598877757648 --renderer-client-id=4 --mojo-platform-channel-handle=1836 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6548 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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14297594785272241091 --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=14297594785272241091 --renderer-client-id=5 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6612 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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7771386638328599311 --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=7771386638328599311 --renderer-client-id=6 --mojo-platform-channel-handle=2196 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

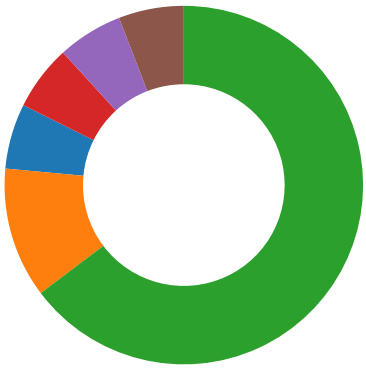
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

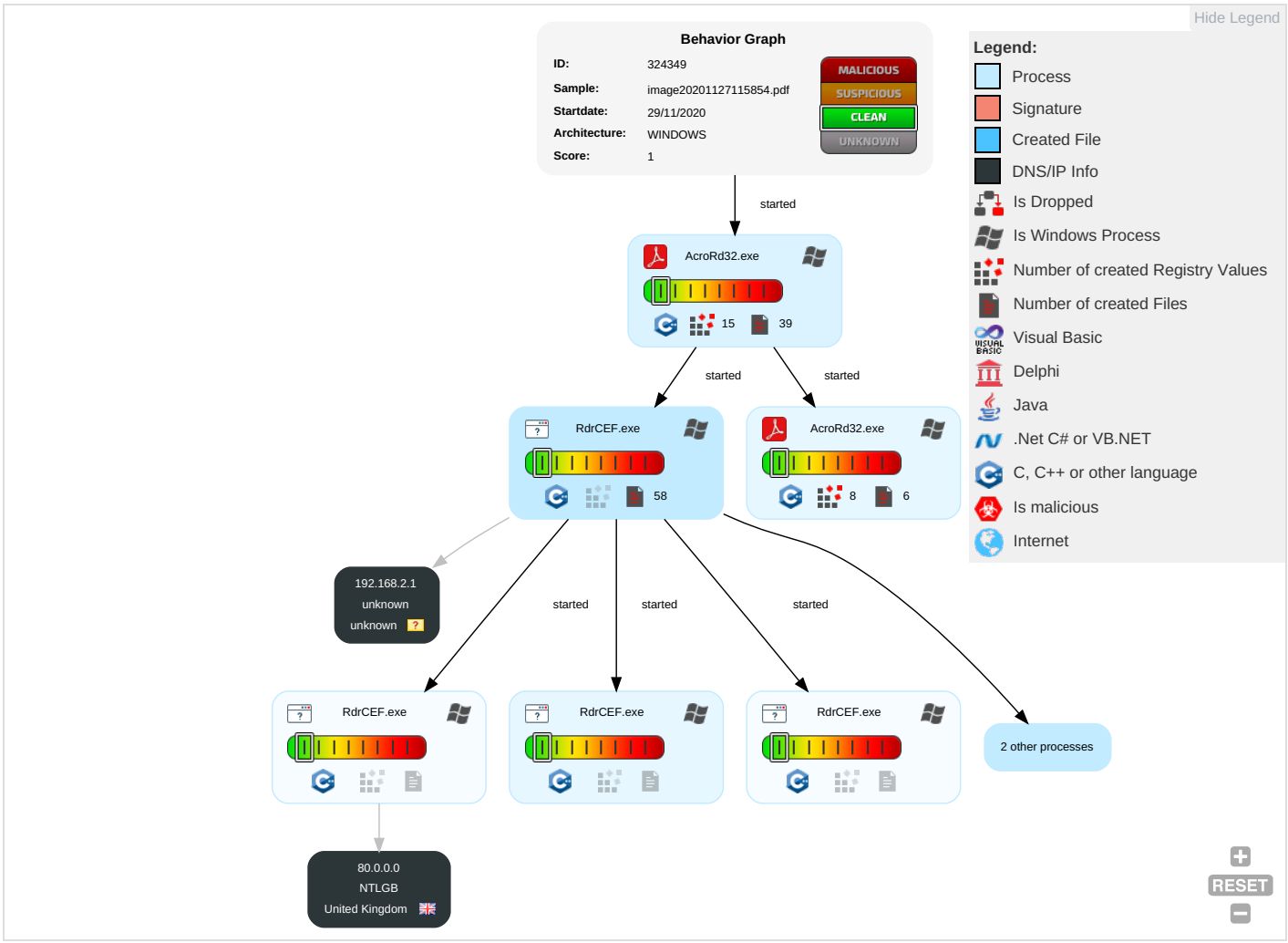
Click to jump to signature section

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process 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	File and Directory 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

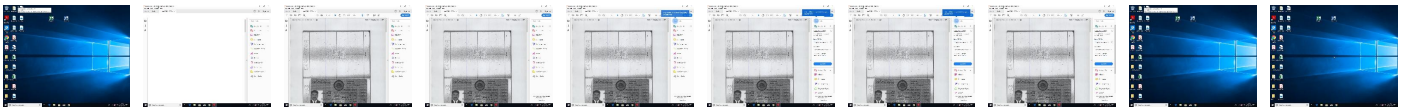
Behavior Graph

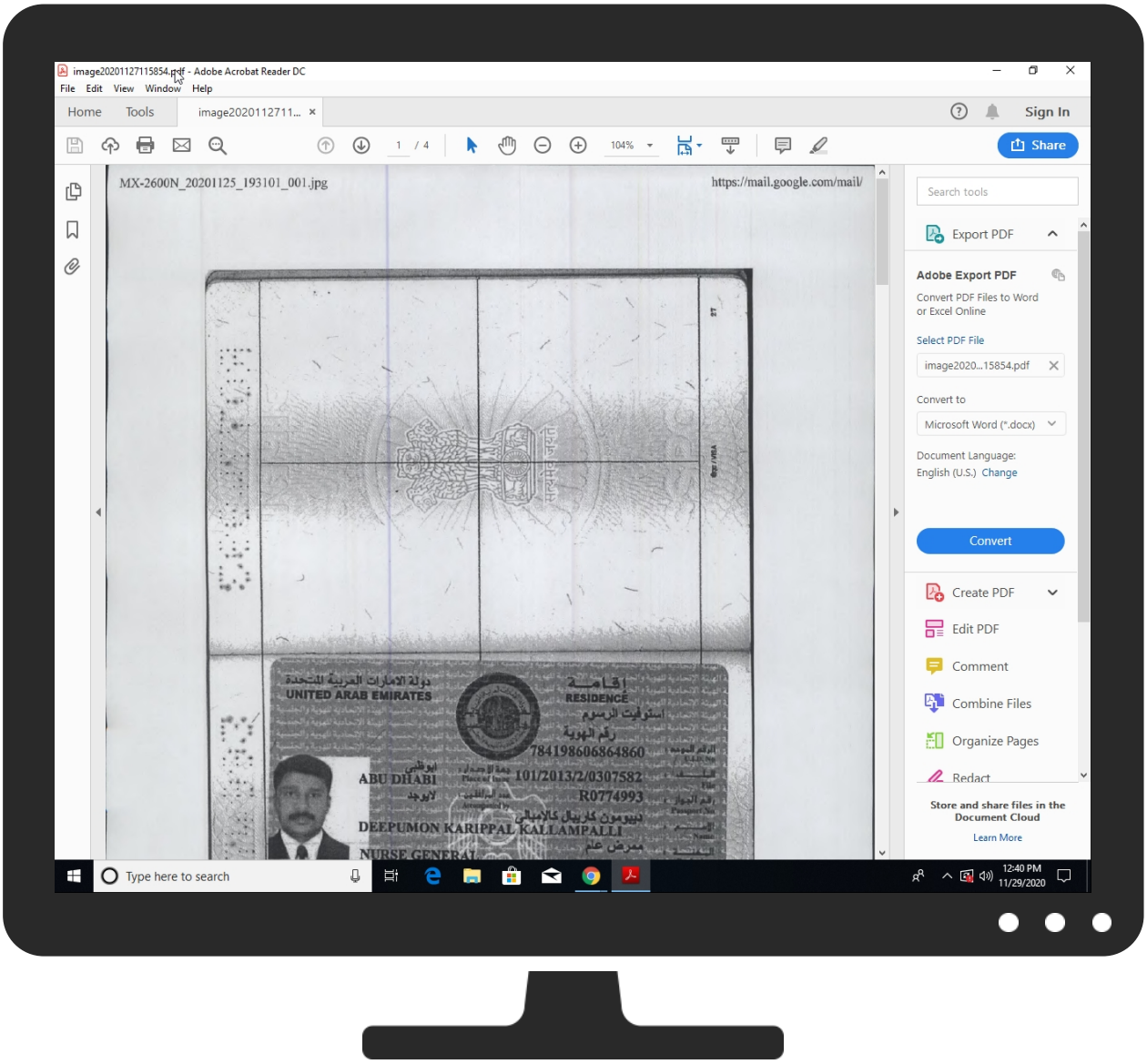


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/H	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/R	0%	Avira URL Cloud	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://ns.useplus.org/ldf/xmp/1.0/	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://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://iptc.org/std/Iptc4xmpExt/2008-02-29/M	0%	Avira URL Cloud	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://https://api.echosign.com4	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://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://cipa.jp/exif/1.0/)u	0%	Avira URL Cloud	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/Upload/j	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://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.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.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	

Domains and IPs

Contacted Domains

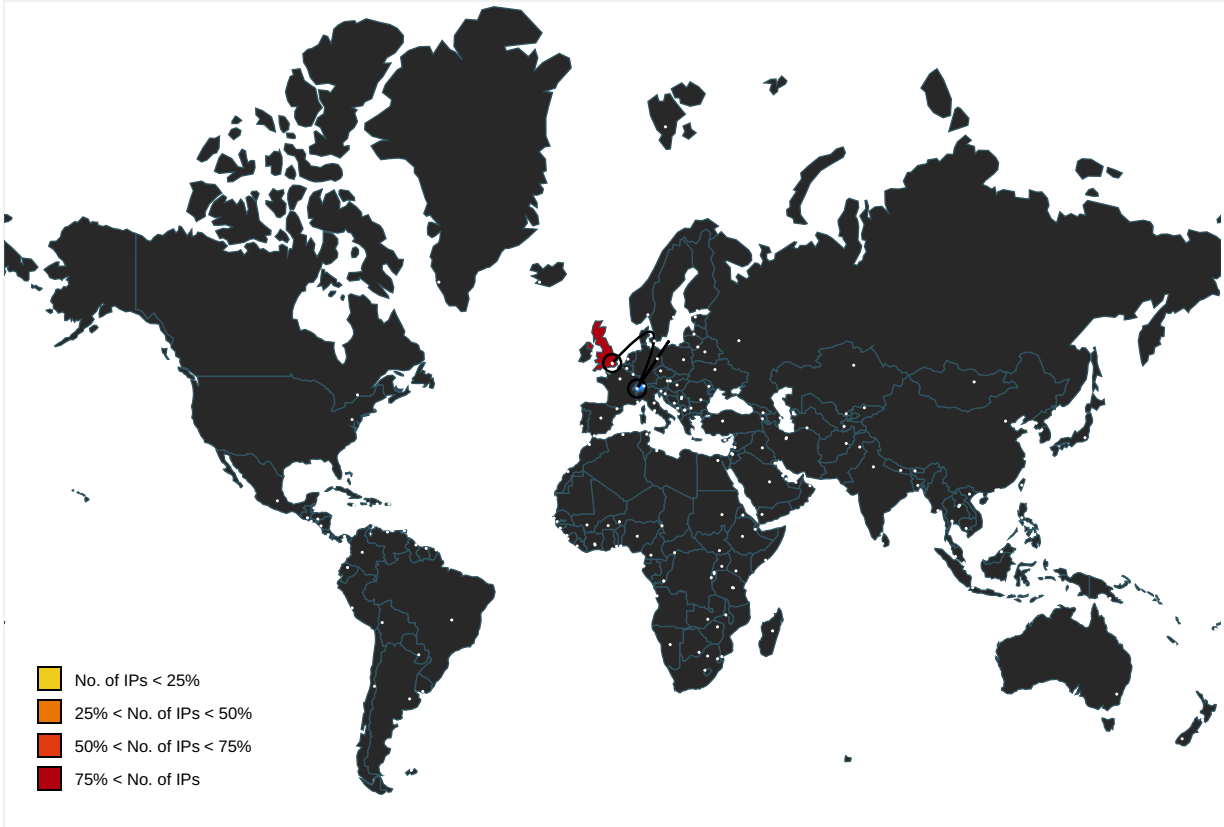
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/)	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/H	AcroRd32.exe, 00000001.00000002.421374200.000000000985F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/R	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/M	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.com4	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.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, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#5	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/)u	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.421374200.000000000985F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/j	AcroRd32.exe, 00000001.00000002.421374200.000000000985F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000003.414207794.00000000194E7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/extension/h	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/o	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#D	AcroRd32.exe, 00000001.00000003.413979974.000000001AE96000.00000004.00000001.sdmp	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.429093036.000000000C740000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.421103497.00000000096A0000.00000004.00000001.sdmp	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.416902612.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	324349
Start date:	29.11.2020
Start time:	12:38:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	image20201127115854.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:	27
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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 2.20.143.130, 2.20.142.203, 92.122.146.26, 51.104.146.109, 104.79.90.110, 67.27.235.126, 8.248.121.254, 8.248.147.254, 8.248.117.254, 67.27.233.126, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.132.208.181 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.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, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:39:18	API Interceptor	11x 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	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	EnklyRDCVr.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
File Type:	data
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.673927541741363
Encrypted:	false
SSDEEP:	12:vDRM912LZiEzffDRM9NYaLZiExHDRM9y398aLZiE:7XUE3KUE5XVUE
MD5:	FEEBA60E050B4BFA6519B7A4A1DEE82F
SHA1:	DC8F8C6B0661B9AA65E373E3258C34CB65C373BD
SHA-256:	8E7004C062C45F7FFC7AA49077E6385130B7CF0D6F33D3B169D646D494110CC2
SHA-512:	E1B2B2E26EEBB0E1A5AF950B8AB3A940E573F9226BF95A38F47A59E0C8BC962F4659CEDBCC023308FD815F479999499D7C8784C38A7AA66F1A41926D80750511
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .}>j,../....."#.Du.^....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..P.,../....."#.D.).....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.... ...,y.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .?4.,../....."#.D.|l....A....d.{v.^.G...d.W.:...P..k%..A..Eo..... ...A..Eo.....e$.....

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):	5.64601676617792
Encrypted:	false
SSDEEP:	12:V9zLHq7m99PQU39zJ199PQJ9zOG/ND99PQd9zd2Mlm99PQ:XzT9PQUNzh9PQzzOGj9PQ/zdFg9PQ
MD5:	06B0FA52A7CE5E81D0F7EA351E049839
SHA1:	C434FB7CE2B06C48126CADE59CB9A5D55F2DF5CA
SHA-256:	B42DD640144BBC300E7FC6AEF90EA3A1E432743EF96C54ABEFBC554DB5537246
SHA-512:	35E11903FA379F3A4ABC73FA946DCD94591019DDE4B3D319C2F82CBEA4FE23F08CC78E5EDA2B685B85508A5D17D358B2D218ACF5DCEFCABF721D18FD1E7E0 AF8
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .d..,../....."#.D.#.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....Kd.....0\r..m.....,....._keyh ttps://rna-resource.acrobat.com/init.js ...W,../....."#.D.(.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....Y.'.....0\r..m.....,....._keyhttps://rna-resource.acrobat.c om/init.js .e...../....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....W.N.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....,../....."#.D.$ ....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	738
Entropy (8bit):	5.605418563120102
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFeYQcblUo6jGyeRVFAFjVFAFBAblUo6jrWTyeRVFAFjVFAF/PRb2:tB4v4DSBOB4v4aSBydB4v4JSB
MD5:	5A332402F97929E676373FD8A5B258BC
SHA1:	7B49C4CBB946BC1F89409F4363F145A1BF763CAD
SHA-256:	E3FD3BF28C51E060869C68ED726EEE984D97CB5613058759C5028AA1806BE272
SHA-512:	0C5315991D8F451A1C72B56BEEAC3F277E8129562C9EADBB980C87A6DFADAFEBAF6B764EEFF3E793E28497B539CAB1E2D5F963466EBE02A71A3F9386B0E3ED B0
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 ..h,../....."#.D..X....A..hvDO.N.t@.... .n.*..... ....A..Eo.....A..Eo.....n.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/home-view /selector.js .M!.,../....."#.D.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....E./.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracke d-send/js/plugins/tracked-send/js/home-view/selector.js ...,../....."#.D..f....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....vD.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.660753046929362
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsc9dlkUSiWulHyA1TK6t6:IbRkiD/ndXWussk
MD5:	001BC8C69332E6716463D7247FC0571E
SHA1:	1E75A62E04F71979AC31134FB5C32E0E85E73252
SHA-256:	326BC9E3FE716CC05B1A214D063412762B7FE42F78EEA30CD81C067BE70790E3
SHA-512:	8CA953EACE9EDD5271E9828610E9127BAF6BF5EF7630FB840A10D726211BA44B22CBB499CCCE305066E7552F497FF0CE776AB8C9178B8CAF063C2CF0658A75A 9
Malicious:	false
Preview:	0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .M..,../....."#.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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Entropy (8bit):	5.584266172935865
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVubEck7VVyh9PT41TK6ty4+yiXYOFLvEWd7VIGXVu6PJJm:pyixRuVEpVV41TEU3yixRui280V41TE
MD5:	25B491D6D9020ECDB32E9D823423285F
SHA1:	9E59ECC36590A6BA06A8E5040B133761B18A6D0F
SHA-256:	51538039B80D2177B78AB57C6EF3B6785F667C820C6D4DC2CE5EE256B4993A56
SHA-512:	FF80EB6C9CF30DFFD0FADEE14E34EC809CAC9030654C5415EF66CEDD65633732AA3EC0AC74F8E9A806F64C4F739A2BEB63B076986DA4BA05924162E60175DE AB
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..mi,../....."#.D..Y....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....t.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...,../....."#.D.pg....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):	648
Entropy (8bit):	5.705466248864061
Encrypted:	false
SSDEEP:	12:0Rhkz9QGLZC9Rhk6d/bLZCpkRhkak4SLZC:0fMLc9ffRLcef3SLc
MD5:	5652557B9CA5F1AA21DDA91F79B80548
SHA1:	AC2BB78C12E38D20AE51815AD041FD375AFC813A
SHA-256:	2DA6CA1A84B0DB457409873BB0EAC6CFDEFB937933CCD623EB50DDF2A5AD9745
SHA-512:	FC459B3524818F441BF14CAB8BDCD048741965813253E1BD89C58AE5C3D87E3DCF0F2B371376BBDE58D496353BB2DEE51C34A9EA9F75DC27557C268DFE6F51 7
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .O.0,../....."#.D..d....A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....%.6.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...e,../....."#.D..C....A.].>....uUf..N...k.....c..l.A.. Eo.....A..Eo.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...,../....."#.D[.W....A.].>....uUf..N...k... ...c..l.A..Eo.....A..Eo.....L.....

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):	5.556892380916859
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQU3dt6g1TK6tyEJYOFLvEWdGQRQOdQY/EJI6g1TK6tWH:2RHRQChD19RHRQC1EJI1
MD5:	B30B2DC3CF55215FF81450A867F132B7
SHA1:	73D02BC258C53925F85BDA69091739605B2C71B6
SHA-256:	970BF84B91CCB8AC846A972FC24D1B27DACA49CEF6DAD2EC81DD28D4EB2AE28B
SHA-512:	6C69BB53C31C82EA6E0EEF672F54E84FA7508C32FD297CAB52CB4570C2C2C26984437CB3BCC1FDC6367B698E2FCC900F19EC7DF979C980F787F45EADDCEA6 53
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .C.i,../....."#.DP4Y....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....3E".....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .T..,../....."#.D.g....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..... .....A..Eo.....|Lu.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	716
Entropy (8bit):	5.667239769647621
Encrypted:	false
SSDEEP:	12:Z5MVchMuR/EA5MT20IUMuR/El5MuL/c3hMuR/Etr5M22EXqrMuR/E:ZS6muR/EASZINuR/ElSuL7uR/EBS23a0
MD5:	FC39A05A20358E6ED8149C1AEC1A62DD
SHA1:	054ED984CD2D27AE0901464DF5400421FEB9337F
SHA-256:	8B38CD94ADE869A7D87A87DD204D0E6207739E3D152CF627FC8F24BA4F1564A0
SHA-512:	6F6A956D37E7B0A251861A2AC5695C071AF7F29C04E695B47CE6563BED92104D4821E3DE8AB5D56ECABAD84559A21332FB9348758CCA14FDC7FEE33EB8D034 3
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .R...,../....."#.D;9.....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 ..3W,../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....YE".....0\r..m.....3....<lb.. .._keyhttps://rna-resource.acrobat.com/base_uris.js .\...,../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....I1#.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..,../....."#.D..$....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....

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):	5.579747614367353
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuJq0i9wm0bbsIDMGH41TK6tkl:XfRM29KsIZE6
MD5:	6DA9DD8FECBFFFDEAAAEA8C52B558B17
SHA1:	92C7A5AE81355ECB9462F7969FB83B00D6B8E6C3
SHA-256:	7B3B7EDCE4C6CDDD50342F3C40C459E16D82428EB688D85F3733776BE7C9D6B0
SHA-512:	115589A45D656874B9EC2E551AA139C495DB979154779A501D2F0B0C4B2743C9EEBBC59EFA1AB5911E89DE585784FB6C190A2BB20EB9563C51ABB1758EB04E21
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ...p,../....."#.D#ir....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):	5.566955357558725
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtubw974+by0zBUKSAA1TK6tl4fPYOFLvEWdtu92qlD+by0zBUKSn:pRiw974+be0RA94be
MD5:	FC15E78CD4C6042FBE3AF20503E9C072
SHA1:	6CECF5F627B0A2D1910527C7285B282F6FCA48C3
SHA-256:	94C97DCFC20DDBDE10BB87022B744C3D78D272C0F501E22FE6B1471CB4505CB1
SHA-512:	C55476A9D9FB72EFF6E0DF43EEA2FFD2B98FAC60758E2B24216C091E8C61E277764DC0BA07C362F56DC1F07B6573FE2BAE1FC980D9091763D8996B0DF6016C46
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .`.j,../....."#.D..Y....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....N.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..\.,../....."#.Da.g....AQ..E.=....=h`t..t..3%A.F$ ..w..A..Eo.....A..Eo.....<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	708
Entropy (8bit):	5.614958032057476
Encrypted:	false
SSDEEP:	12:KkXxKMSCvqXftUlQokXxKMSCvIS3tUlRakXxKMSCvGCk/o0tUlbkXxKMSCvletUz:KkXxiCCPWjkXxiCVWRakXxiCQlWbkXxB
MD5:	7B34A6DB27F8561DD6201E9F78EC1B67
SHA1:	9C161B0F3F82060D09442DA4CACE2E9C5A396A37
SHA-256:	0E89EE100D13A7DED1A9A0FB94B5C44B3AD212B8AD5F8778FFA942451FF2113A
SHA-512:	9D709C732B98E4269FA13670070079857CC91547866238A0BC3C2CC114B148EBDAA4495A0984ADDF2FAD602CF17B088D3BFA4FC24686CF04B3122C9CC652FB8
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .9...,../....."#.Dn2.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....\{.X.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ..0W,../....."#.D.A.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....G2.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .n..,../....."#.D.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....H.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .Y..,../....."#.D..$....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Z.....

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):	5.632576616863116
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
SSDEEP:	12:5h6OLBWXxIkEzh6OLp9TEkjhh6OL6/SkYh6OLZ9rk:5h6th9Ezh6ojhh6TYh6l
MD5:	74A8BAF14BFC8A096F4D8B8EDD41A965
SHA1:	56E6092105EB936E84BAA1BF7509CBAD6DD84DB7
SHA-256:	D0AA1A322D5422BB78C82707DAF57F4534AEBC32AC335638EBBF6EDE6447366E
SHA-512:	E4933F82A1516FE3BFAD25E3D1E5D70D16042EA4323994CF2488F61CB2DAD592C6A340E5F5CA83559079987F8A29C1495D61D312702E279742DB800FFC9A3DB3
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....,../....."#.DNc.....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....B.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...b,../....."#.D.26....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....4\7.....0\r..m.....;...I....._keyht tps://rna-resource.acrobat.com/static/js/desktop.js ....,../....."#.D^.....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....w..4.....0\r..m.....;...I....._keyhttps://rna-resou rce.acrobat.com/static/js/desktop.js .D..,../....."#.DjNI....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....?.u.....

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:	modified
Size (bytes):	732
Entropy (8bit):	5.660422341205291
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFGq2wSeKaTLnSXeRVFAFjVFAFfXNVUwSeKaTLnoRVFAFjVFAFKXZ6a:UB4v4swzXLnSXeB4v4vUwzXLnoB4v4la
MD5:	E14C63BEEFB55B470CEC4C5588A10DD7
SHA1:	4D3B7DFC417C269450D617AA23FB8C7EC6E2BD45
SHA-256:	B09150379B70AC775930179B80AF90459226FC782CA67B11A82ED4F5DC4B49DB
SHA-512:	C0E304CC638235D4292B7FC0F53022DA244F6A8EACEE65B0A395CEE1989C4BC9365DF0D1393A63E4CA80F7B2FC31CC6AED99974E6F5C3674DF249DA168C457 7
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 .>.i,../....."#.D..`....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/p lugin.js ...,../....."#.D.....A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....x'[D.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-sen d/js/plugins/tracked-send/js/home-view/plugin.js .[..,../....."#.D..i....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....

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):	5.545961023005628
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQl+l/xt5GFCaa+41TK6t:NRMHd+a/xt5Gda+E
MD5:	B9E82C5D65F875519C4F47E40ECE33DC
SHA1:	797B8DD148A39B2B0259FED52385A3B042EF4739
SHA-256:	95EE894F835B977607F8781028365D5C4CA5D5364BB81C5F475DDF481D08FC84
SHA-512:	5824CE73EEFC4D776C4EE63E643F2C92480E2A7DD3A1BE32D6686DAE6ABC2EDA62FB6C65F8FEBED45404F18C35D8F041FA8C9A6B6606117D57D02B1A766293 CB
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ...q,../....."#.D.r....A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo .....X.....

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
Entropy (8bit):	5.555711219897526
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXugq/E5P11TK6ttCs2VYOFLvEWdvBIEGdeXuK1/FQP11m:BsR2EseNqwvFsR2EsefFQV7o
MD5:	9C5426F8850283FBA9BA4DCE54A18712
SHA1:	7F9E8E6F195A43DAD6C822A4E582A524A1E61185
SHA-256:	F17466ADD227E2377FD908765C8F790DD34B164723375077C4C40957DC7CF83F
SHA-512:	B2078FC14C455D9BA9BD55200020530E07D0CF6C0CE9464EAD4C1B04387C398D5CFACB254D75C573FE8DEC7349AF3CFAF9F7FC4AD3FD826CE64C9C387906D 1F
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .I.h,../....."#.D..X....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....Gx.~.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .x..,../....."#.D..g....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):	606
Entropy (8bit):	5.7152682224967934
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ91/MfV+B7OhKlvA1TK6tc8aVYOFLvEWdwAPCQM/wk+B7OhKe:RbR16A9M6JkGbR161/4Jk7bR16o9JJk
MD5:	C2FC2132BB0B91F9390528ACD6B99E69
SHA1:	9A371FFBFD94C5D54D3102EB21F12D5659AEDFD8
SHA-256:	6DACB2D4FE857BAFB81E1836C9537A0BE0CF54B865F14A5419CE73E2E3BF5D29
SHA-512:	70C315D689F9573F7640DA5824CD4C9A7A48F0B07D3B50E3315DD09FA7D487CFABD47950942E8522A163815B495B9BF9D62D00C423305EFA10E42E13E9352EDI
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .I>0,../....."#.D..c....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....)O}..... .0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .D.e,../....."#.DY.C....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... j.B.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .%..,../....."#.D..V....A..4T].....Tw.....(..b...EO....9.A..Eo..... A..Eo.....J.....

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):	5.590496211250686
Encrypted:	false
SSDEEP:	12:B2geRHRQ6XcZj0JpR2geRHRQbucUKrj0:B2gerQhZj0JpR2gerQN1rj0
MD5:	97B56221A4BE1B2AA85312C8F4E52A69
SHA1:	635284D5A87D44BD894FB89BA848BF4AB745F458
SHA-256:	D9A72C4E1D09704DDEA74DCD34ECACA12E328F8C0ABCDEC654A1930DF6FB6127
SHA-512:	D73AC31871C16A9EB232FD56600C30AC7D6961768FD21783BC0D882F4AA2B1FC87167BC1AA737A602090C46FCD5A2C1AE7A0EB0EC440CB4F8CB52484245378 D
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...h,../....."#.D..X....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....it.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .z..,../....."#.D..f....A@..{o]...9o|..qY....T....{..u.b..A..Eo .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	824
Entropy (8bit):	5.677258061405141
Encrypted:	false
SSDEEP:	12:WyeRlql/Gvt1wMyeRlqX1Et1w5KmyeRl9G/nEt1wKEyeRl7ot1wg:WJC+fwMJjfw5KmJwMfwvJUfw
MD5:	DABC7F02B88831D14F549525E2AEB84B
SHA1:	35E2EB8B13078AB20BF6E4A24730A22FFE82ED7D
SHA-256:	3D5F6CD384CAED3F9F07A16A5296C6F0CE972711F52922D3B38DF22FBDE6B734
SHA-512:	94B34EB78D6A0D60498F71CE6F67436EBE0404F4039B905AAA794A48BE6FF9548CDB232ED5493904CF23112E81A040DC775FA6C4873C8071250EF848D10B9715
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..;,../....."#.DG.S....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..d.!.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...d,../....."#.D..<....A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....J^.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..{,,../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....,.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...,../....."#.DEcQ....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):	654
Entropy (8bit):	5.620443435970398
Encrypted:	false
SSDEEP:	12:wRhh23kIjwK+EFqRhp/oljwK+EhRhA+EVDjwK+Eq:wfhLDEYfm6DEhfr+IDE
MD5:	249A9946B046430155F9B6C5A0DAFFD6
SHA1:	AF4562045C1B620B37D2322B529F777BA4765E0C
SHA-256:	6BF43745CB0584D60EA9E7C60D5EA15296EF77FF0B888D499CABC40875225486

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
SHA-512:	E870BDE8C7FED1493DC29CA686E460EA488DA5CECF4811E7BDC30B67AA6F7EE40B4FF890DEC65430B6DFF5868666EC8135DE13E3BC6874AA03A6710BBEC7E30E
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ../,../....."#.DK.b....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .ede,../....."#.DweC....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....<.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...,../....."#.D.V....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....1..L.....

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):	5.67049127829456
Encrypted:	false
SSDEEP:	12:/RrROk/o//qlfLEORrROk/79XAfLENRrROk/G/9wfLEf7XRrROk/dqW9fLEa:/PJ/o6l4OPJ/y4NPJ/GFw4jXPJ/dp4
MD5:	01C27A10F9B216CA0AD9787CFC015D59
SHA1:	82CEAB1942E527CA68AA2A2BEFD0B3F08153A000
SHA-256:	0696958166FEAAFB0C15E69F91D3490F96C0C72C782BA61F5379F4FA370161C2
SHA-512:	34573934BCAE3A48C0AF95C35F98C6A6381BD744572745219E9E206D605700B3209CCA1A2514AEB4A95C789B16B21D5849666676249CA6ADA333FC6CFD329E97
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..),.,../....."#.D.aS....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....;.=.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...d,../....."#.D..<....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....&.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .Nn.,../....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....K.V.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...,../....."#.D.MQ....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....K.}.....

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):	5.640229024634905
Encrypted:	false
SSDEEP:	12:xqTbtECPLnfjqTmUw5CPLnUqT0qdCPLn2jqTqwCPLn:AyMnOgMnL1MnZDMn
MD5:	22E647DE0377F2F4FE77F09161E67131
SHA1:	B2D23CC7DA27C95E1FE384DE805AD2F3BCF72185
SHA-256:	EF18C66499DC8EE9D6268212D0146288B3774597AC8C855F695027E0E375B25A
SHA-512:	2B6CDFE41995FE4B06437C7FE717DD4A7335AFB9C80D03CE90A795C6A61E08AD4910559034ECE53EB772DA1A17B445C008218CC8AB248071579EA78144466BEB
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....,../....."#.DD6.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....R.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .g.b,../....."#.D-&6....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....:....f....._kx.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....,../....."#.Dm.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....t.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .=..,../....."#.D.HI....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.664990033256374
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuiX0R/sEJ41TK6tce52YOFLvEWdMAu3tXpsEJ41TK6t3E52YOF5:zRM4X0R/sDGRM19psDZBRM6OXYWsD
MD5:	5C2B4F5A90FCEA4F73213243E04FCA6A
SHA1:	AF0BF838E43F00874FB674E43B082BE431BDDBAE
SHA-256:	6895AA1BBDF0303662924A397D53F20FB9AF0A23B5D76E440B744859279D0E4F
SHA-512:	B2FED56BD47F2CDB443726668EFED0AE26D9982CD1D5232D3B626C655528DE69E8872E43B8A92753BCDD40C4B5F441D23FD9FCCBDEB7C72837DCB1214808469
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...h,../....."#.D..X....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....u0.F.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .8.,../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....vR.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .j..,../....."#.D.3g....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....h9.....

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):	630
Entropy (8bit):	5.6070916645614215
Encrypted:	false
SSDEEP:	12:6lJRs2qKVoMeClJRfEnRoMrilJRrFVoMQ:YzoM9VCoMrQ3VoMQ
MD5:	D0FE520B4FD2FA5B598A7BA2DA5687F2
SHA1:	2B6CCA95F43B386F4DA4AEA64C7EBAA942E9DFFF
SHA-256:	2B7F0F17D2D8A759A8DBB5C7E2628C8CF746A7641614E963760B92361759CA96
SHA-512:	F1B4242AA63B5D908A625D81C36BA7D9592BAA5ED37AAB02F4276C8917E0573EFDFA0418A96D7A1F86BABF6AB19D84B39B26B30910F90203B908F6FC5D64B04B
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..hi,../....."#.D..X....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....'.....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .M.,../....."#.D.B.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..o.,../....."#.D.Qg....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....Ge8.....

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):	5.669655125213974
Encrypted:	false
SSDEEP:	12:F8hRrROk/z8un2h8hRrROk/2sJn2HN8hRrROk/lRG/kZ23//8hRrROk/pCs2:UPJ/Yun2lPJ/92cPJ/nGcZ2PqPJ/4s2
MD5:	6C90BD0FBD4D61D1370337B263E054FA
SHA1:	611F403CDA9282CC8B70584D3163E288B157612D
SHA-256:	EC5F048F526F0B5507F078820D6527D3E050D2AD30A8C9EDDF77FB604F35D727
SHA-512:	F3E068CFF116CA14FD540EB10DE162B9BF2168180E7DE64CFD170DB33D87D969FF2DC588420AB51F59EDEA3BDD5327B0F57D77C8791EAC98CAF0929C811C68A7
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .:.,../....."#.D.R....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....S.+.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .N.d,../....."#.D..<....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....3!.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....,../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....i.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .. .,../....."#.D.AQ....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....F.....

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):	5.73075807791946
Encrypted:	false
SSDEEP:	24:ehC7JICXh2PJICthEYaJICvhyJb9pJIC:e05XwtteY+vQXz
MD5:	D5A01A962DFFBD111A875F5D6277289E
SHA1:	B807625CEBCA21CF1A54150BC545BDAE202C2314
SHA-256:	5FC788839F074B5428FC088E4FFB93D99C8A99DF993CA4EA8DCC89B8F308A172
SHA-512:	267DF150FFE673E40D851AC65B254C63DF4B4CA705EFC3BBB4FE7105E678B90823A8DF5C10DB68567631F1902A3F8A29639E095AD23F0451D32957DF810CDF2
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..L.,../....."#.D..T....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .(4d,../....."#.D..<....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....E.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .T..,../....."#.D!".....A.;"./N_.,.:C..2....9L.H..3:...A..Eo.....A..Eo.....?.).....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....,../....."#.D..Q....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....xoa.....

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):	5.65549487904394
Encrypted:	false
SSDEEP:	12:0RqXZ/ReNR6CyKReXRC/tReHCRfXgHHRew9:0UJ8NsXIiHClo
MD5:	7F89A31F189B1156A416A79E59071CF3

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
SHA1:	59B0F0445290E1EB0378CD5BEC9CCEB92859EE05
SHA-256:	1606A581DA1B31BAA31619EDF9CFF1C9608426C7E1C369AA90F70FEDE2A7F249
SHA-512:	F2DB47954C463694EF77014C353D1C9365222FCA265929026D5667B6C29281951F248AAB6C158E1BEF453AC9471C8608EE7338E6435E0971EEE4121074E8F9D0
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .a..,../....."#.D.v.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....(.J.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...c,../....."#.D!.<....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....Y"V.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....,../....."#.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....I/.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....,../....."#.D..Q....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....@.0.....

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):	5.665999555487122
Encrypted:	false
SSDEEP:	12:6JJKuIIYJJKJ6+l/FILBJJK3rI9JJKU2OIwH:6JI+YJIJoLBJIU9JIxY
MD5:	86DBF318286E431954B260438B61A47F
SHA1:	FEEDDC51C9A2C0593CAEB9B583BC09B754D934FA
SHA-256:	11E127FC7F9FDEF99C57CF0DB27B1FC9AA49E9F510CECEF9C13409AE68DAEDB6
SHA-512:	9AFDE8512E5BCE1E023EF1300B63A85CDD02E85094A3A6E6B2150BB63D23E4F0B03DE5B7EA579B5CC6B82FF0AA8388EEB95FB5907D2866D9B6605D9A6EDBA892
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....,../....."#.D.(....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....H.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .r.Y,../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....c.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....,../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....%Sj.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .1..,../....."#.DN+4....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....T.>.....

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):	5.655881771966278
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvue0yghUDLYtmOZn1TK6t6zEWYOFLvEWdBJvvuza/N5hUDLYtmD:xRBJNLdDcFZLMvRBJpNcDcFZLg
MD5:	D042F071A6D5471365FFCABE3E860217
SHA1:	6BF724D49924EB601AA87001E0CCA51CD92170C5
SHA-256:	E97316CF80455316A17B35A3675486F13E84C134A2AF1C5715B996B67E889B6F
SHA-512:	B98BD15433CFEF32836A360F6174A559235A1922B4B6A52D8E770006F22077626ACCA28A7438048A7D65633D07F5F1B7397335996E451FF3C2575977AA2D2451
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...h,../....."#.D[.X....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....*C.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ....,../....."#.D..g....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....C.....

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):	5.663342934283703
Encrypted:	false
SSDEEP:	12:BPH4eUczCPHb2GcMmPHLJ+l/gc6PH4CHEc:BPHfUcOPHb7cvPHLMlYc6PHHHEc
MD5:	8866F14F7E2C569221D1E6318917584B
SHA1:	D5D518BAA6A2F0CFD58905863E6F9251CF9BBB35
SHA-256:	6FC6B8EAF35178A5EDE4C69ECE8CF114A1C075F7665466D49E0F3DC27D268CC2
SHA-512:	5E7322F3F438994C84B53FB2E43377C6815760AF29276E8B844DC7F6269F3C1C7F78F2CE7505BAA9A4DEA87CB312CB5BDDA6C55B894C036D1B3B7E08AA4E82A7
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....,../....."#.D=e.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....3..A.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..5W,../....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....r%b.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .d$.,../....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .B.,../....."#.D..$....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.608114771672931
Encrypted:	false
SSDEEP:	12:bJRT9yJ+9uer0mBJRT9h//er0YJRT9S2Zcr0:9NgJ+o3m/NH3ONk2R
MD5:	BB97D97CCC02CE2B48DD82030D770AAB
SHA1:	EC32B28E63056D2BBF18E67F7493A996D10BB6A3
SHA-256:	8FDEA3B75AFE602B5835E4507BB01D07F5BECAC850D64F35438A9B04E773D4D9
SHA-512:	43FBA84DEA2B0702070DA2DE864D9FF1F7DA2ACE7EB05269FAA59AFA5B3095462CF2F305F02612420CBEFFFF700CB295F7814E61AEFA5FBCFD1C52E5A3BF49 5C
Malicious:	false
Preview:	0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .u.0,../....."#.D..k....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo. .....?.....0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .\.e,../....."#.Dl.I....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... .....A..Eo.....0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....,../....."#.DgDZ....A...M....m+lS..e.....<7.U.P8* .0K.A..Eo.....A..Eo.....a.e*.....

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):	5.588615229007747
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQdAhjBRCh/41TK6tBOQt6EYOFLvEWdccAHQaw1/Tmyk1QjQ:XRc988Di/ELvRc9CTe2Di/E8
MD5:	E440C584477767B9CFCD44178BB50B75
SHA1:	57A1C3372CC5F72A852E19A20B4D0E770CB977D7
SHA-256:	6CF0740500247DDFAA82216AF063BBA7AE1F68E8D2DD3B9EBE142BB43664A178
SHA-512:	E9595068349C5802E25BA899A7CBE566F7D3E358DB11572B18E4739D02756FE79571CA2B2E46670AEFE709F6564B5ED2B07CE298E9201FE316C2F2BE32A4FF46
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...i,../....."#.D.c....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.. ....s.K.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .P..,../....."#.D/jn....APJm...0x.x..RD...BB!@5..<..]....A..Eo..... .....A..Eo.....a.n.....

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):	5.631815269597018
Encrypted:	false
SSDEEP:	12:bs6xRkixULlF4n4js6xRkiCll/NHTZLlF4n:brxpWoQrxpCllFzZo
MD5:	E48315C8E83E0DE5C6F6735288900EEA
SHA1:	9966AA89494EE9A44E74651A04F5C9B0FDD112B6
SHA-256:	13528878C14B64B44227FCBFF916BCEB5E5BBB40CFB9F2E57BACACE5FC262E3C
SHA-512:	83B9CC26A48A45E086DCC830FFB53D4BA950F0AF1E02B145D254D79537FDABD94780F6F69DBA372A71BB877376E17B3F5ED97B281794D08B399F28DECFC47BA 0
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...1,../....."#.D.\o....A.P...#4..l....5...5..).w.. .h.~..A..Eo. .....A..Eo.....$.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .q.,../....."#.D..... A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....$M.M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.54240560649493
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuZEELqY941TK6tDdehYOFLvEWd/aFuNXOUvY941TK6tq:WRAEL19EVd+RDXOF9E8
MD5:	3C01AB4FB351EF19CEC0F23768F2C833
SHA1:	FF61167F4C7F538E7DBDCB01D8D5E04E629D5587
SHA-256:	3B1C39B4EFDC91588A77DCAA640127585E4A7DFA859808F4B43789B5A05952CC
SHA-512:	13D22DD50EB46180336123421302CE1EA26D08CA35C38A8B29B34B2209AF3E944B4E6CE1AA4BC81F4BC174D6EB86F14810413F6A2E79CF82B61820426828B7F4

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .W.j,../....."#.D..Y....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..i.,../....."#.D..g....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.569574512483093
Encrypted:	false
SSDEEP:	12:2DRuR29doB9Vd2kemDRuRcXtYoB9Vd2k:8IbdTeMpbdT
MD5:	892E3381A7756B94B72834592F78232B
SHA1:	B302271C799114A6C2FD0A3B53EEA6503F840791
SHA-256:	AD3A982B076BD81C5A1FCAED229AF66AA6411E1EC96567F1BCD93215C807C17E
SHA-512:	D46D897FC29C2CE526B4FE5DEBBE970F9756B7EB0CDEB9A97BA815DD9C8E7816EC99FB27C0935D3306ECC0736214BAF0653C0BAA480A752F3CD87441A61E0 0F
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...j,../....."#.D.Y....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo... ...wDi.....0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .%H.,../....."#.D..g....A..y.$..$.v5j...T...z.]..._S....A..Eo..... .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.651988695229455
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QCJq8C1GFouA424r1TK6tXkqYOFLvEWd8CAd9QwXpouA424l:+RQTq8McrnlRQRlrnh8RQPuVrnf
MD5:	34AFF7B76B1061179F6D704D342EBBD6
SHA1:	325AD35D1EF756A3B6954B5EEB493CB60DFF97FB
SHA-256:	6D81889DA7A6B1D2644B266F94BFA107C62B4B409ED035462849A730080670B6
SHA-512:	FD8C2820087806B0C66E8388964F36FE1FA010C39F633028453E21CADE1DECC3743753FF0BB20D3E6FF769541C5D93D4FFCF5D452DB2C32329FEDD4A594D733
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..yj,../....."#.D.gd....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 .%.,../....."#.D.z.....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 .U7.,../....."#.D[.n....A#..@..k(v.8g..5.~_....]Pj.*..6.A.. Eo.....A..Eo.....[u.....

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):	630
Entropy (8bit):	5.5834395145226745
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuNxscyC8n1TK6tboXXYOFLvEWdENUAuJl/B7yC8n1TK6t4MJ:xhRTnxz7QmhRTLl/B77QchRT5Ysqg7Q
MD5:	71437AA73020F8F922B582460D72498B
SHA1:	6D9CD9DB73E4FB3F2F169C597F2F40E5F13653B1
SHA-256:	6E9A15CB3CA1007DC6ADEE6088E90222FBC68B849CD271C40DD59BDEEF40FE8F
SHA-512:	30F8533461A7ED74A790E1198F22CFB80C234EE23896FA8FC61619294E114E090DE1B95C2B523C6DDD06AEA3E220A79E3C15AB20B46022DCC2208105320726BA
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ../,../....."#.DS.b....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....Z+. .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..ae,../....."#.D.NC....A8.../...;.\\o....1.....+..A..Eo.....A..Eo... ....y.[.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ....,./....."#.D..V....A8.../...;.\\o....1.....+..A..Eo..... A..Eo.....i+.....

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):	5.630867526323791

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Encrypted:	false
SSDEEP:	12:nRrROk/Vc/FwmZRrROk/ViqYPm1yOfRrROk/Vrl/7wVmboRrROk/VgLPm:nPJ/0FZPJ/AO4OfPJ//DwgboPJ/r
MD5:	DD182559D73DBC248FD3D358D19C3FC7
SHA1:	DA7C5EB595DA73BB7E62FBC0F43492D22204AA52
SHA-256:	8C7BD143E18B56E73AE725C9E89C727FA004A012F59476F302C4310C9DA6F86C
SHA-512:	1ACD8B36AFE66634E18D0F186E6797ACC365BFB3486FABFFD549B060DD588C99CBE8F3B59C55EEA33A68C2F33C5459D2170EA95568E852FB1660B9453F0EEA 0
Malicious:	false
Preview:	0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..b.,../....."#.D.eT....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....X.3D.....0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .)Ld,../....."#.D..<....A ./.ev.....N~..6. b.....$.j;:C...A..Eo.....A..Eo.....N.....0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....,../....."#.Dr6... ..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 . .t.,../....."#.D.Q....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....sGA.....

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):	5.58977913427434
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWudJqnxAdm9741TK6tTmFEZ/lXYOFLvEWdccAWuyIs2xAdma:qxRczESdu7EAFoxRcEIs2Sdu7E
MD5:	B0BDB42116E0E45940C065011680A331
SHA1:	F4D4E64A3B721714814A18B97135A5929A972C31
SHA-256:	AF03E59572A1DF3E8826F6D82A0DF5C274729E98CB52A5B9BB2DA41BCCFFC72F
SHA-512:	C6BDC35FC4F8A5F5808D9763FCC134AD27199D5DB28C4896092FFEA0A34ADA152A583ADA2D6D8E78A8005A2B78DFAB3B91EF0B0E948A52A8A3E89243D44149 4
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...h,../....."#.D'.X....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....{~.C.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .q..,../....."#.D.f....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo..... .....A..Eo.....[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.639125110112249
Encrypted:	false
SSDEEP:	12:2R1iriLO8R1Ull/8kbL0HeR1XqoFYqLC:23LO8zkbL0HeTL
MD5:	EEA9A50C3299DED1242D900B210ABA4C
SHA1:	917271CEA1823900919E13B12A98E89210E36D4F
SHA-256:	A42DF63D23EA6AC705933127C38BC2AD3F2C53EA874A01AE179B0BACCDEF3906
SHA-512:	09DFF10BB64817066CC242D6268288247D38F9B3B7560B4303F4F21BC7480FD7F445F249E68FF9F83E668B109F6B5AF8DE906F1DC0957F34CF1E55F3654F0BFB
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .../,../....."#.Dp._....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ..H.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..Ie,../....."#.D.0C....A.....k....F..D..O.n;[.1m.....=..A..Eo..... ..A..Eo.....t.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..^.,../....."#.D.{V....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):	5.6895675722963155
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQmqX4s2zhcsBXIh1TK6tk3PXYOFLvEWdBJvYQEXmECtm2zhm:mxRBJQwos2DB0WxRBJQpXutm2DB01
MD5:	A5FFD457FC8B7CE9CCCAB75979C81A7C
SHA1:	EF113102B1D0AD2EF03832821703DF21184DFB39
SHA-256:	B79977C06CE97C4EBD6FDC00156CCC9440DB3B71E91F1A9C3ABCAA7EA21D5455
SHA-512:	D48E9D9A795B2FBE82FB479CEC9BD29B793AEAFD86A0440C4F62CB052B20A9A9EFE1F2D75D762BF93C52BF99A9397BDC52A4FBBB0F464C7271661F7B493F4E 47
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..=j,../....."#.D..Z....A...k..`..N3.... ..d..$[....{.A..Eo.....A..Eo.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...,../....."#.D..g....A...k..`..N3.... ..d..$[....{.A..Eo.....A..Eo.....N.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.645702667809178
Encrypted:	false
SSDEEP:	12:3RrROk/sy/TvcqFRrROk/s2yMcbVRrROk/s/l/Xc8RrROk/scyYc:3PJ/h0qFPJ/ubVPJ/+lE8PJ/qd
MD5:	A7789E6A5C5B6AAA995D9B17CE0FC729
SHA1:	745406246F193F11F45492505201FF0EFB026027
SHA-256:	F1E1D66956C01C3010BA40AB560FC8535BECC12CC53E2D47AB97B5193C41AEC9
SHA-512:	9003723253F7FA2553497427FD62EDF8FF7A1AACBED978B7335BB74413250263EED9849196CEBF384EE55BB9BE250930A0552858E9D286A0EB268CA3A36B2F85
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..{.,../....."#.D.PY....A.....9Q].8O.z....=.:.N.{....N{.A..Eo.....A..Eo.....oo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..bd,../....."#.Dw.=....A.....9Q].8O.z....=.:.N.{....N{.A..Eo.....A..Eo.....%.I.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....,../....."#.D.x.....A.....9Q].8O.z....=.:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..u.,../....."#.D..Q....A.....9Q].8O.z....=.:.N.{....N{.A..Eo.....A..Eo.....Cp.....

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):	5.291241044535032
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPWAMEAQue+VCwPcMoO57YAthQA4kHQ1:h1zZ4+dsp6jAMEjayXObthrVHS
MD5:	9BDB0821B177F6E87E65EB04BB79DE11
SHA1:	03E908E8A2424F3E424F27DE3CE9567300224095
SHA-256:	2C6A987F3D4A7DA04D79E0EA2F9E4FB7257C3CA4CBD3D0BFA0DF3F1B6653CB17
SHA-512:	D975B414793E2778A37AC13C40800C1EBA0184DB72C47632EFB1BB41CF1CBD3C633E980C31CCDD3AD3089D1A97C721BCBEACE3CF625CC4C93BE7260D220FI AF5
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):	289
Entropy (8bit):	5.140208018425578
Encrypted:	false
SSDEEP:	6:aWlq9+q2PWXp+N2nKuAl9OmbnIFUtwxW+WZmwyxWtFE539VkwOWXp+N2nKuAl9Oe:a4q9+vaHAahFUtwxlW/yxo+539V5fHAR
MD5:	7459635D11D680BF0401A8F51E5AE895
SHA1:	92ADDC36FFEEE182501A07FA5CCCBF56B4A619E2
SHA-256:	38D9F9B44B25E8B2F4DBB57BEAE59FBCC0AF598A39801665A28F570B68804DE8
SHA-512:	48AB600E5A38DB800B6A3ECC45BC7063C83E0993DCC38C638FF36B7E74897477060084C73FE8D8D01DDBCE74A3420436B27774EB431698389C9F9C955D0B756
Malicious:	false
Preview:	2020/11/29-12:39:23.899 aec Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2020/11/29-12:39:23.908 aec Recovering log #3.2020/11/29-12:39:23.909 aec 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):	1703936
Entropy (8bit):	0.009971064856787025

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9smWi9smWiAsmWhCzsmWhCr+smWhCr+smWhCr+smWhCrDsmWhCDY:YTUTPQPQPQPvnovnovno
MD5:	C90F4316CF868652B2443BBC1772416D
SHA1:	4EA162D75917A065154BCD605395647C09F995CD
SHA-256:	0F658E222C89EE4EED8A4012AD95C61A7B58C6C60EB0706DBDD778324F583211
SHA-512:	4D94DD18134931107DC30C79F6780840191A9C55C987AC61AB635B585C12A4D0B9805B3851690D1383333ABBA94EE8AC2DE53FC54FB8454594E67CB3B96072D
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129203919Z-269.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):	5.592935716802893
Encrypted:	false
SSDEEP:	1536:GSzYWmGFNyDXl+M/AxOkZCzeXa+x/cihO3Cgr/zFVjlZhGD0y4V+NknpxeQGpTX+:tk5aNA0M/AxOO5Xa+SihO3r/zTlZhI0N
MD5:	E9B4675C17D2A1C0CAAA95C45BC5ABB2
SHA1:	B66D900B70C560F4FF358C0233914AE2DB1E0EE9
SHA-256:	7F8FD520F604B69F47D02EA5C9D7F8B7320F34272E1E05CD6FDF3CBBD626C67B
SHA-512:	7A433433629AB99D7E1C1002D7B60355D136FE2821BD45DE580CAEA1E9A09E419A29396A81B767157B7B3D88D435A11D972E945938ADCE842953EFA5A2523CA
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):	3.3868591381003808
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQMOhFVCsL49IVXEBodRBkR3MOhAVCs749IVXEBodRBkl3MOh1X:iGedRB8edRBSedRBFedRBj
MD5:	3DEBE17EEB360504AEED46F6629E7479
SHA1:	FD1C0A5086C8DEEC2431B2C4D79DBAA51C3BA879
SHA-256:	9970605BE55274E3247D5788CFE67C11F58A18BF8B7562B3D87A3971463D033E
SHA-512:	5521E0A327217B45167BA2A175FC7B69D2666ED2416A61A2FC90F028B7AE03862B09DA979D854404E3DC09822F847470221304AF4F9F7116F0654A9BA9FF58A5
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):	3.2011312565296026
Encrypted:	false
SSDEEP:	96:97OhFVCPa949IVXEBodRBk5MOhFVCsNLR49IVXEBodRBk23MOhAVCsvod49IVXEN:9OiedRBGLGedRBIoCedRBvyedRBy
MD5:	4C5A2CCE877EDE4BF806532AAA6E013B
SHA1:	8629E9E55194EFB30C89032CBC9BFD51B8D8DB80
SHA-256:	D0D19E91ED28F8EDDF98CD35BAB037226C787BA8349AE80E276814DBD4E4A95D
SHA-512:	13794D12D438536D508E96B4A902C6D3E1ACE3ADD6D354D31E5F2F2A485B104522572FA18FD1D7D25E6EB09E3E4BA16D59E07B0F965DADF3FF8D682FD69E55F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Preview:	.....N..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5976	
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 1.6
Entropy (8bit):	7.999689796115832
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	image20201127115854.pdf
File size:	1164906
MD5:	94481d1abb00f007f14b5bbc4019d1cd
SHA1:	13d999eac4b938ab9d317f0132e9cb6d1a999609
SHA256:	55e4417b68134b55a12293ed82b8e457dd699e57b9658 fc5e71b899ea1d1376
SHA512:	3d2b01bca921b0cac4be11dfad246dd3460f002f1fa3945 a62e40de6172cf5c73092fe9cf099a76eae60b84a1343ee b32d02a8efee1ff7e300af95dbc801fdce
SSDEEP:	24576:6ZwTsFlJqM1wMtOqGGK/K2F7ifVZ4Cv6JNzCe EqAHmX8EY:6wsHJEMtdS/K6ifLdyzCeXiREY
File Content Preview:	%PDF-1.6.%.....%3.4.6 0 obj.<</BitsPerComponent 8/ColorSpace/DeviceRGB/Filter/JPXDecode/Height 3514/Length 360906/Name/ImagePart_0/Subtype/Image/Type/XObject/Width 2490>>.stream.....jP ....ftypjp2 ....jp2 ...Yjp2h....ihdr.....colr.....

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.6
Total Entropy:	7.999690
Total Bytes:	1164906
Stream Entropy:	7.999720
Stream Bytes:	1162530

General

Entropy outside Streams:	5.313698
Bytes outside Streams:	2376
Number of EOF found:	4
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	20
endobj	20
stream	16
endstream	16
xref	0
trailer	0
startxref	4
/Page	0
/Encrypt	0
/ObjStm	4
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

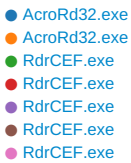
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 12:39:03.862665892 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:03.898356915 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:04.678070068 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:04.713766098 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:05.341758966 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:05.377527952 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:06.300932884 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:06.328169107 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:07.754919052 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:07.782258034 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:08.550985098 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:08.588860035 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:09.241293907 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:09.268496990 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:10.220633984 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:10.256547928 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:11.091169119 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:11.118218899 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:11.945031881 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:11.972232103 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:12.742749929 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:12.769957066 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:13.466279984 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:13.501890898 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:14.470990896 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:14.498246908 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:15.530603886 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:15.557930946 CET	53	57084	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 12:39:16.325759888 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:16.353087902 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:18.359683990 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:18.386909008 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:20.746179104 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:20.784135103 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:25.993278980 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:26.030800104 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:26.037627935 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:26.074608088 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:26.994585991 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:27.032352924 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:27.041590929 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:27.079343081 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:27.996140003 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:28.032052040 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:28.090564013 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:28.128334999 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:30.040488958 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:30.076334953 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:30.143915892 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:30.179938078 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:34.086868048 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:34.122642994 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:34.197422028 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:34.234704971 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:36.018269062 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:36.045599937 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:42.650954962 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:42.704334974 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:53.929223061 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:53.956556082 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 12:39:56.142685890 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:39:56.186605930 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 12:40:11.086981058 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:40:11.114264965 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 12:40:14.962572098 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:40:15.000147104 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 12:40:45.448460102 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:40:45.475794077 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 12:40:47.505122900 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 12:40:47.540792942 CET	53	61292	8.8.8.8	192.168.2.3

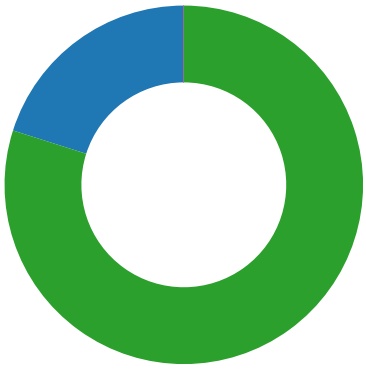
Code Manipulations

Statistics

Behavior



RdrCEF.exe



Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 1004 Parent PID: 5692

General

Start time:	12:39:08
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\image20201127115854.pdf'
Imagebase:	0xaf0000
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	B265C3	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	B4AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5976	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	B3EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock1004.1.2768679314.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	B72657	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	B3EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129203919Z-269.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	B3EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	BB83C8	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	BB83C8	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	BB83C8	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	BB83C8	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	BB83C8	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	BB83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1pudriv_ztm4qu_4m0.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	B3EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	B3EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1f1af6p_ztm4qv_4m0.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	B3EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R18cwe88_ztm4qw_4m0.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	B3EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R19p5xy8_ztm4qx_4m0.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	B3EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rve5sf0_ztm4qy_4m0.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	B3EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5976	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	B7D405	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	B3CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	B3D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	B3D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	B3D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	AFEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	AFEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	AFEA55	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	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/image20201127115854.pdf	success or wait	1	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	image20201127115854.pdf	success or wait	1	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	B4DF69	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 69 6D 61 67 65 32 30 32 30 31 31 32 37 31 31 35 38 35 34 2E 70 64 66 00	success or wait	1	B4DF69	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 32 33 39 31 38 2D 30 38 27 30 30 27 00	success or wait	1	B4DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	1164906	success or wait	1	B4DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	4	success or wait	1	B4DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	B4DF47	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	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	B4DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	B4DF69	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	B4DF69	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	B4DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 5976 Parent PID: 1004

General

Start time:	12:39:09
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\image20201127115854.pdf'
Imagebase:	0xaf0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 5080 Parent PID: 1004

General

Start time:	12:39:18
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:	0xad0000
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	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	BC59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	11	BD83E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	87	BD8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	215	BC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	BC59E2	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	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2176	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	23	BC59E2	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	BC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	56	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	BC59E2	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	BC59E2	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	9	BC59E2	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	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	3	BC59E2	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	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	6	BC59E2	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	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	12	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	BC59E2	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	254	BC59E2	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	BC59E2	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	12	BC59E2	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	3	BC59E2	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	BC59E2	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	BC59E2	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	88	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	3	BC59E2	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	3	BC59E2	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	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	3	BC59E2	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	BC59E2	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	BC59E2	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	24	BC59E2	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	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	BC59E2	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	BC59E2	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	160	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	14	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	1	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	BC59E2	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	324	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	BC59E2	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	BC59E2	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	BC59E2	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	15	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	BC59E2	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	BC59E2	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	BC59E2	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\js\selector.js	unknown	4096	success or wait	15	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	BC59E2	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	BC59E2	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	BC59E2	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	201	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	3	BC59E2	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	149	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	179	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	215	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	BC59E2	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	9	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	23	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	BC59E2	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	11	BC59E2	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	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	BC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	BC59E2	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	98	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	BC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	BC59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	BD83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6148 Parent PID: 5080

General

Start time:	12:39:20
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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3833046004073922652 --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=3833046004073922652 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xad0000
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: 6180 Parent PID: 5080

General

Start time:	12:39:21
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=1704,16962285166967419287,12971905902240953692,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8625267804615807816 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xad0000
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: 6232 Parent PID: 5080

General

Start time:	12:39:26
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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2248485898877757648 --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=2248485898877757648 --renderer-client-id=4 --mojo-platform-channel-handle=1836 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xad0000
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: 6548 Parent PID: 5080

General

Start time:	12:39:27
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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14297594785272241091 --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=14297594785272241091 --renderer-client-id=5 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xad0000
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: 6612 Parent PID: 5080

General

Start time:	12:39:29
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=1704,16962285166967419287,12971905902240953692,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7771386638328599311 --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=7771386638328599311 --renderer-client-id=6 --mojo-platform-channel-handle=2196 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xad0000
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