ID: 339435
Sample Name: 3PD4931.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 02:39:35
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

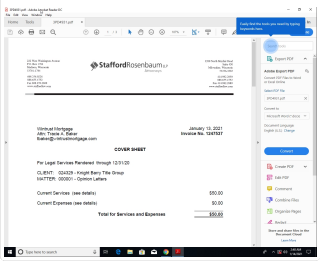
Analysis Report 3PD4931.pdf

Overview

General Information

Sample Name:	3PD4931.pdf
Analysis ID:	339435
MD5:	edc2cd81fc270db..
SHA1:	44986311a4415c..
SHA256:	6abd92aab60b58..

Most interesting Screenshot:



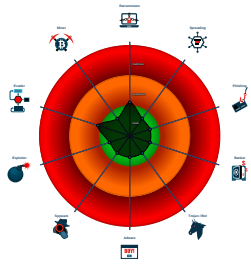
Detection

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

Signatures

- Contains functionality to access load…
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 4156 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\3PD4931.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5544 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\3PD4931.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5388 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6292 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1708,1282318598042692567,6584645183887421796,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=16114704440535557804 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6316 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=1708,1282318598042692567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17658040393359851026 --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=17658040393359851026 --renderer-client-id=2 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6400 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=1708,1282318598042692567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1535626254935326759 --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=1535626254935326759 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6452 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=1708,1282318598042692567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10496770992156748853 --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=10496770992156748853 --renderer-client-id=5 --mojo-platform-channel-handle=1872 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6856 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=1708,1282318598042692567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16098587735302563493 --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=16098587735302563493 --renderer-client-id=6 --mojo-platform-channel-handle=2296 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

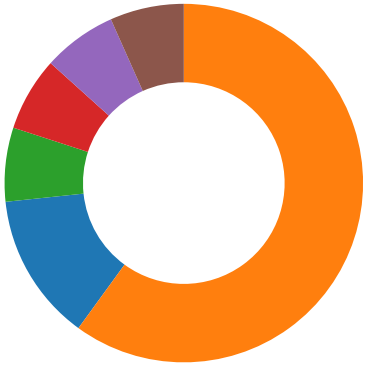
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

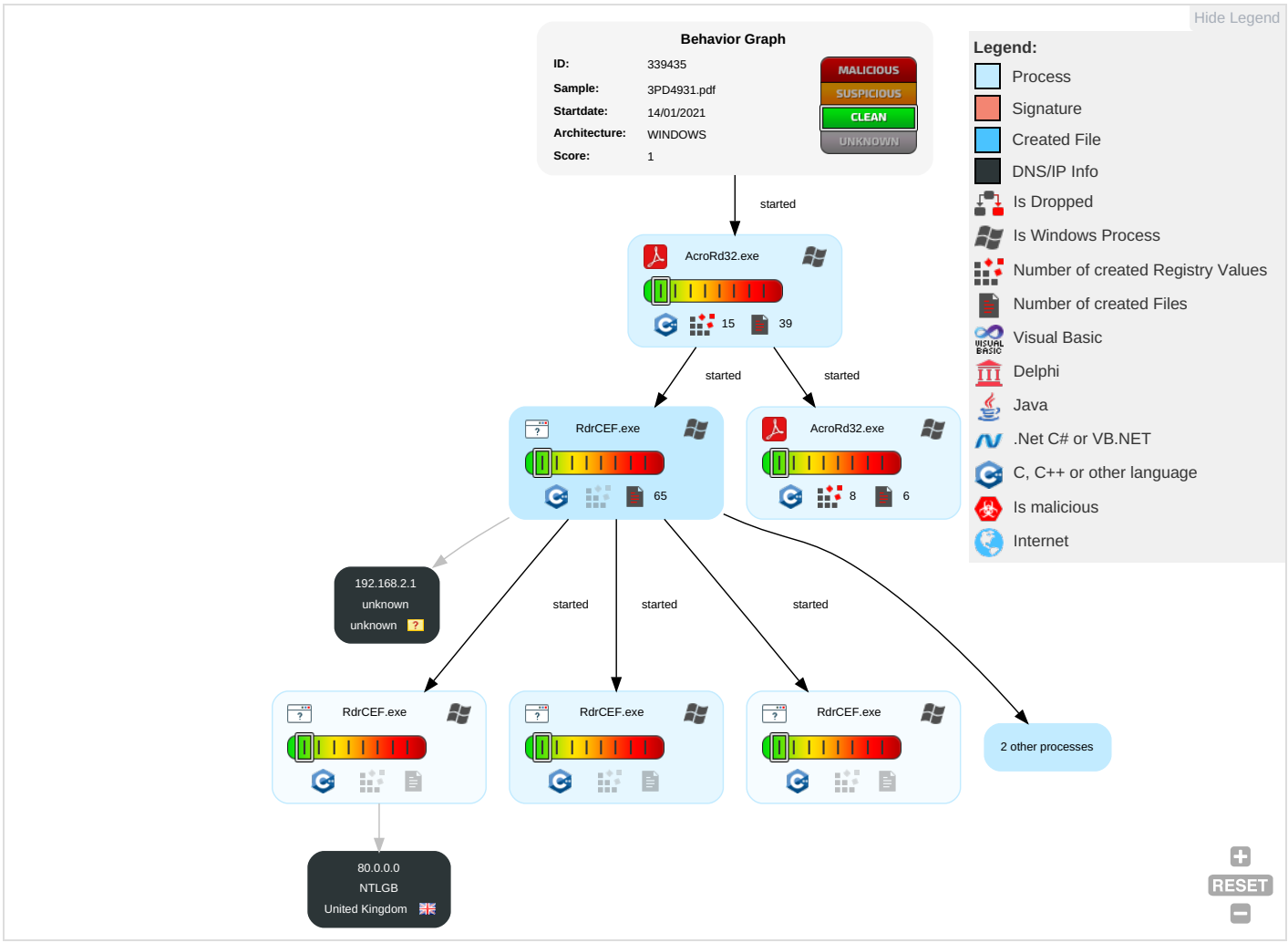
Click to jump to signature section

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

Mitre Att&ck Matrix

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

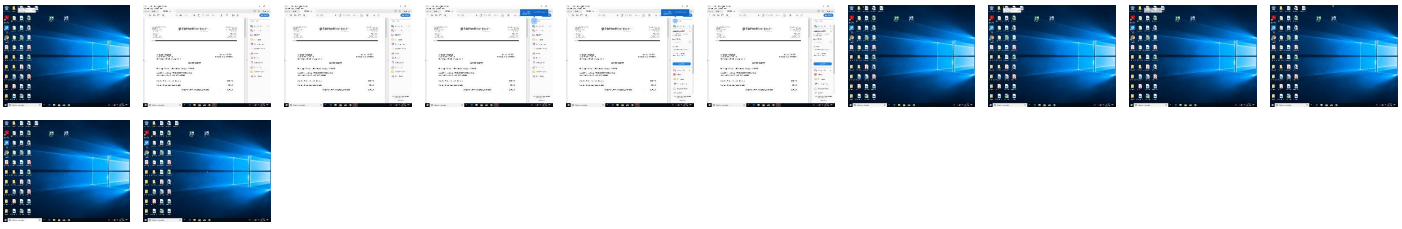
Behavior Graph

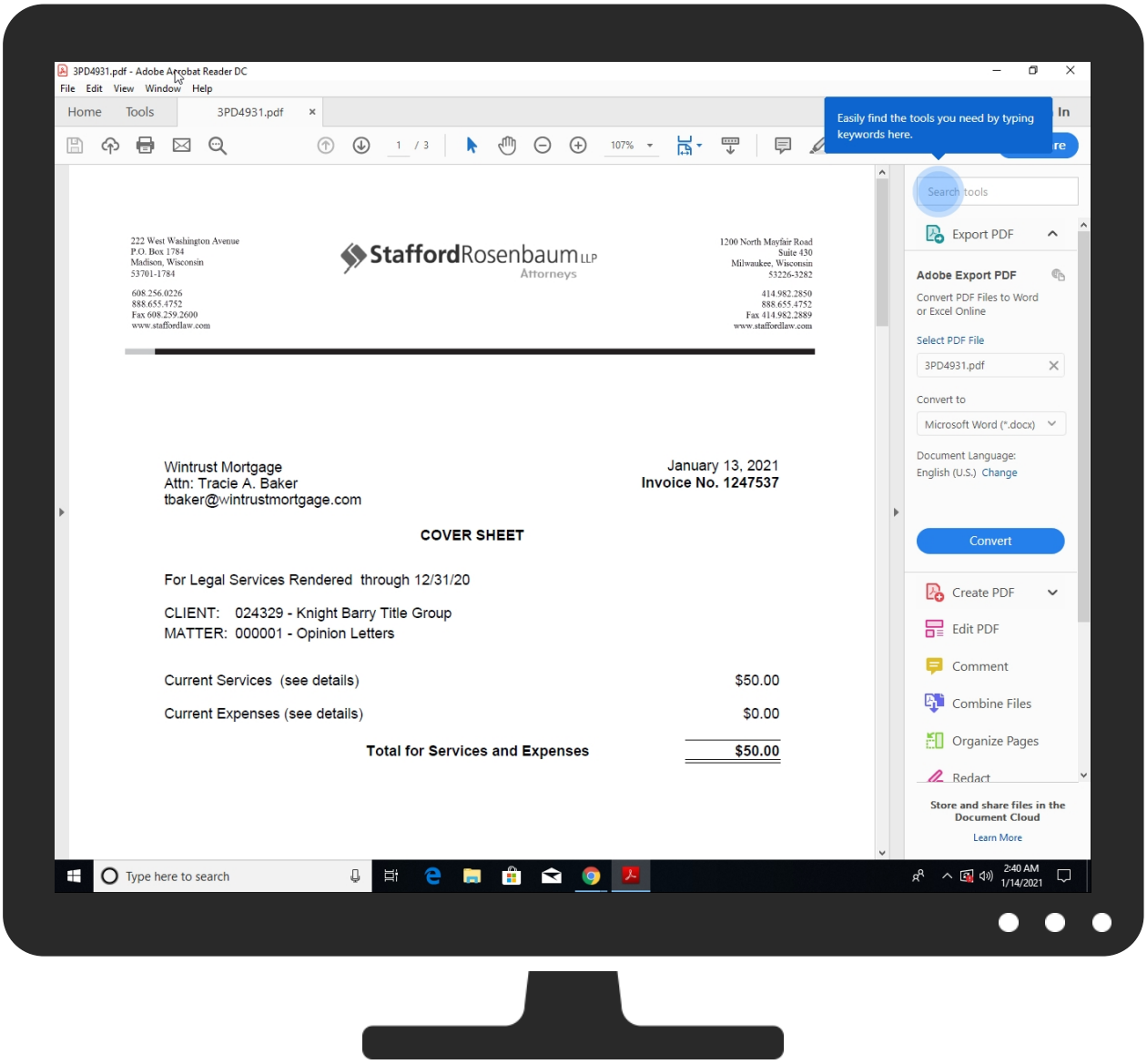


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
3PD4931.pdf	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/6I	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/(15)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/(15)	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/(15)	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.adobe.c	0%	URL Reputation	safe	
http://www.adobe.c	0%	URL Reputation	safe	
http://www.adobe.c	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/P	0%	Avira URL Cloud	safe	
http://https://ims-na1.adobelogin.comN	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/1F	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comength	0%	Avira URL Cloud	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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/?	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.adobe.c9	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/c	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

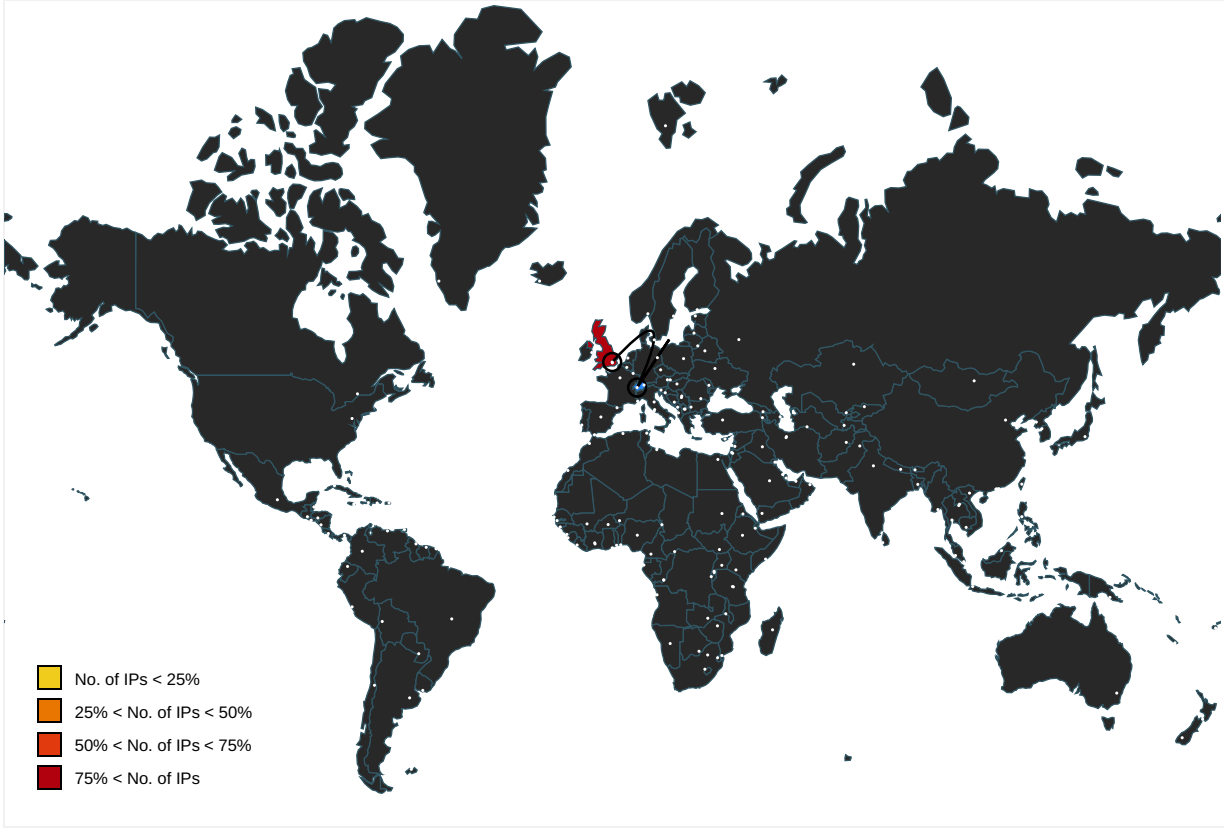
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.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/C	AcroRd32.exe, 00000001.00000002.391707436.000000000B7DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#B2u:	AcroRd32.exe, 00000001.00000002.390110089.000000000AF5B000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#j	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/6I	AcroRd32.exe, 00000001.00000002.391707436.000000000B7DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/-29/m#	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/(15)	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.adobe.c	AcroRd32.exe, 00000001.00000002.394894832.000000000DC7C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/P	AcroRd32.exe, 00000001.00000002.392037923.000000000B836000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ims-na1.adobelogin.comN	AcroRd32.exe, 00000001.00000002.382206477.0000000009410000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://www.npes.org/pdfx/ns/id/1F	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.394523907.000000000D8D9000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.391707436.000000000B7DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.391131335.000000000B6D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.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, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comRL	AcroRd32.exe, 00000001.00000002.394523907.000000000D8D9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comength	AcroRd32.exe, 00000001.00000002.394523907.000000000D8D9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/field#c	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/?	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.392037923.000000000B836000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.382206477.0000000009410000.00000004.00000001.sdmp	false		high
http://www.adobe.c9	AcroRd32.exe, 00000001.00000002.394894832.000000000DC7C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/c	AcroRd32.exe, 00000001.00000002.391950316.000000000B810000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.376595261.0000000007AF0000.00000002.00000001.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:	339435
Start date:	14.01.2021
Start time:	02:39:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3PD4931.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 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 40.88.32.150, 2.20.142.203, 2.20.143.130, 92.122.146.26, 2.20.84.85, 51.104.139.180, 2.20.142.210, 2.20.142.209, 20.54.26.129, 51.104.144.132, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, 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, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.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
02:40:34	API Interceptor	8x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSIjf0v9YP9XHTo1mHg1DdlnrlGItn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	
	http://https://bouthilletteparizeau-my.sharepoint.com/:b:/g/personal/jproulx_bpa_ca/EYQbKRRM1_VEjGeslLjc5GwB075qH34FcIdpShYIw3DxFA?e=4%3abltg7p&at=9	Get hash	malicious	Browse	
	ds7002.lnk	Get hash	malicious	Browse	
	http://https://townemortgage-my.sharepoint.com/:b:/p/cislami/ETa8xXdrX-FKtlaSfOphTioBLICbx4muhejuoDN0jK0wqw?e=4%3aBnR24e&at=9	Get hash	malicious	Browse	
	iwqOx.pdf	Get hash	malicious	Browse	
	http://https://jcpconsulting-my.sharepoint.com/:b:/g/personal/maireads_jcpconsulting_co_uk/ERfHfSCzdwpCiQXDqtKNHKkBnVvlszs3rd1CSU_-rQLUlg?e=0TY6UC	Get hash	malicious	Browse	
	purchase.pdf.exe	Get hash	malicious	Browse	
	fOlUD.pdf	Get hash	malicious	Browse	
	aPJ75.pdf	Get hash	malicious	Browse	
	http://search.hdirectionsandmap.com	Get hash	malicious	Browse	
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHIfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPIY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHIfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPIY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	
	nyEdi.pdf	Get hash	malicious	Browse	
	CHoyU.pdf	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	2EB0.tmp.exe	Get hash	malicious	Browse	• 80.0.0.0
	muddydoc.exe	Get hash	malicious	Browse	• 80.0.0.0
	RQMofd68Ad.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 80.0.0.0
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 80.0.0.0
	utox.exe	Get hash	malicious	Browse	• 82.27.253.120
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSIjf0v9YP9XHTo1mHg1DdlnrlGItn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	• 80.0.0.0
	NormhjTcQb.exe	Get hash	malicious	Browse	• 82.1.160.234
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	• 80.0.0.0
	http://https://bouthilletteparizeau-my.sharepoint.com/:b:/g/personal/jproulx_bpa_ca/EYQbKRRM1_VEjGeslLjc5GwB075qH34FcIdpShYIw3DxFA?e=4%3abltg7p&at=9	Get hash	malicious	Browse	• 80.0.0.0
	ds7002.lnk	Get hash	malicious	Browse	• 80.0.0.0
	http://https://townemortgage-my.sharepoint.com/:b:/p/cislami/ETa8xXdrX-FKtlaSfOphTioBLICbx4muhejuoDN0jK0wqw?e=4%3aBnR24e&at=9	Get hash	malicious	Browse	• 80.0.0.0
	xJbFpiVs1l	Get hash	malicious	Browse	• 82.30.74.138
	SecuriteInfo.com.Variant.Razy.803156.13117.exe	Get hash	malicious	Browse	• 81.106.72.253

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sDSRBJGFaW.exe	Get hash	malicious	Browse	• 81.106.72.253
	Advice.xls	Get hash	malicious	Browse	• 81.106.72.253
	iwqOx.pdf	Get hash	malicious	Browse	• 80.0.0.0
	pty10	Get hash	malicious	Browse	• 217.137.225.123
	http://https://jcpconsulting-my.sharepoint.com/:b:/g/personal/maireads_jcpconsulting_co_uk/ERfHfSCzdwpCiQXDqtKNHKkBnVvlszs3rd1CSU_-rQLUlg?e=0TY6UC	Get hash	malicious	Browse	• 80.0.0.0
	purchase.pdf.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):	5.668389602293913
Encrypted:	false
SSDEEP:	12:vDRM9zeZiEnDRM94GZiE8DRM9ajsLeZiE:7OEDZTEKfcbE
MD5:	D96CB2AEA11974711CAD860B30131FE8
SHA1:	33E0755284CD8A37F5FDCD80BD49468D43B6EAD3
SHA-256:	24CC77A9510011A2124342F87C2ACA020D93A71BBF323E10A5A58C8DB4BE283B
SHA-512:	8102BCD24A8E544B62C598B7125371535FD0FC5C65BE83AC5EAB1E8F5EE58E80F124F95B21F2F4E6261218503EFE00D14FD231EEC7C58DBE64DFDE6FDAB9DA7A
Malicious:	false
Reputation:	low
Preview:	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.....B7.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .1..,p./....."#.Dp.Q....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 ...o,p./....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....P.....

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):	5.5900920672982135
Encrypted:	false
SSDEEP:	12:V9zkpq9PQC9zij9PQC9zVo9PQ/69zYi9PQ:XzkI9PQ+zm9PQ+zVo9PQezYi9PQ
MD5:	43C4560C4F4B219AA77065A62006B9CB
SHA1:	39D436254B1B4649F294DA89B9001CEE4A6345FE
SHA-256:	EF13CC819F8AA50DDE870D2A0A4225E78C18564901857C0656570F964F6C41E8
SHA-512:	2BF930B2DD7AF95CA01E096FFC6DF72052D002D28D2E21DF2156B8211D9C17F39FBA427A5CB2F3D179877197795C2754D702A91A609367BA06D70E06D4CA1C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..4.+p./....."#.D.nG....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....L.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .m..+p./....."#.D.U.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....Pd.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....,p./....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....#1h.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...^,p./....."#.D.(e....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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Size (bytes):	738
Entropy (8bit):	5.574586423046823
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAF6vlUo6jiyeRVFAFjVFAFZJyvlUo6jUyeRVFAFjVFAFydvlUo6je:tB4v4oSBCB4v4bQSBQB4v4ESB2f
MD5:	8A209FC9B088A5DF0F0879D8E0D74457
SHA1:	88958AB320CDB81127DB5AC25A40F2564EEB953C
SHA-256:	56CB1DC564921089B0185FDAB25121D2F0097B3F8494069B9596B7657A44C49C
SHA-512:	AC52C8870396856CF006BA070A41F7B739627C2E72CB334E9DFC05DE232A42975911473132F4E7341B17DBE15CF11049E6EC8F817DF796021BBD9B13850E8CEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....+p./....."#.DyY.....A..hvDO.N.t@...n.*..... ....A..Eo.....A..Eo.....W.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....,p./....."#.D".O....A..hvDO.N.t@....n.*..... ....A..Eo.....A..Eo.....>VI.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .!.n,p./....."#.D0.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....%2.....

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):	5.619463219877738
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RshV8p0iWulHyA1TK6tc:IbRkiDm+pFWuss
MD5:	A99BF2E1D977163AF9962805AB9A3F17
SHA1:	0ABD27381A42CE7A6349C0132F3A4809EFAA5D95
SHA-256:	7C9229E129F6D9312F73F908CCDBE541FE44331F4A9BE4127E14157BC7E852F3
SHA-512:	5F986C277F4E803603E6AAB2E4A18AF4DD0F0CF6308FA4B4AC8E38C6933136C80A9F09409A06FF9F5A7EB517EFD99BDB5A1F05753D2D4630FE3EF82A4F40275
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..C ,p./....."#.D..^....A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....ez.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.53896115128606
Encrypted:	false
SSDEEP:	12:pyixRuhbARV41TEx/zyixRuLV7RV41TE:NL4xExT24xE
MD5:	B450FAE8CA0BB1D56F3D3BE7E8355204
SHA1:	A6105693D36C4F2A91BBD8A8D9495918AF87DE67
SHA-256:	FF2FFACA4912902B83432DE346AAE469D5A646F3D19E5DB6B700223D60016334
SHA-512:	82A0364091CC9B9FDDFDB6B40B93E1C87D19842336DA540021D1096B75159847142E444B716809F193BB3AE494887BBB9B5927BC6ECE1C7F7584A1E165B1EAD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....+p./....."#.D.....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....#Yn.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...o,p./....."#.D.`.....Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....PL.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.617021984801141
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQF1e3GLZIl6P41TK6t/YvYOFLvEWdhwjQyWALZIl6P41TK6t6:0RhkWg3GLZCQRhkNLZCw
MD5:	A8C32B427C4B3778C7E844766F26AB20
SHA1:	CA4B64F3B05D061B3F042E5354EC457F5F4BC4ED
SHA-256:	CE03247AEBCC2442CF5F99F990A726E8C585C35DC7F59CF5D747A69F1451C340
SHA-512:	D4ED7FA0A3312DA06F43E65D3A61C3234F1026A8967A9B966810C91503A1AC07F9159A1D3E97BF96E1C09713E9E256C793434776EA12483F06D99D0E8168EC0E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....+p./....."#.DbL.....A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....o.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .Lxj,p./....."#.D?.....A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....]

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.507359053357327
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQx8S9lV6g1TK6t698JYOFLvEWdGQRQOdQ/BIV6g1TK6t5VH:2RHRQCk81I4RHRQC481H
MD5:	DA7561DAEE6EF710AB0203BE86D2E453
SHA1:	F0A0745204DED05CBCB015FC92C35322660C280D
SHA-256:	9E4A0EAB971279F834881B12C5DB28781F2365EDCD43C4D2E975347EC30EC6D3
SHA-512:	11626818B33D3FE20E461FF944DE9C7AE35DA29B055B2F049A166A1024AC217BA3371C317612B581CF87034E02EF76BC30E710E85599CABD6BB17D4584D3B49(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .O..+p./....."#.D.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....`4.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...o,p./....."#.D.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....Ka.p.....

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):	5.594530253588081
Encrypted:	false
SSDEEP:	12:Z5M0lYLMuR/EQr5MAJMuR/Eu5M3PJJMuR/EKB5MPRMuR/Eit:ZS0lYouR/E2SPuR/EuS38uR/EKBSP2uV
MD5:	F5C517B3632E8458961069FEA3145FF6
SHA1:	C23268B1527C062867C13FE9E5822CACC3CE3827
SHA-256:	DBCC0C95381C5B1B9724CB7A03DDF91BEE1C97369E2287C22BC00E0D2C4F4570
SHA-512:	4292C1B2E86832EA12243C803A175A8C395BBDAD43A71F20EC9677BBB968B4FF34A50CB46010DF95A92294EBEC84603B28C18263D8B7D9FF02E33E41C200E17
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .5=.+p./....."#.D..G....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 ...+p./....."#.Dyt.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....O.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....,p./....."#.D.~.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....o?.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...^,p./....."#.D.Te....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):	5.583573650450309
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAurllPc1nSm0bbsIDMGH41TK6tLz:XfRMuLKsIZERz
MD5:	A64973852496269CCC7EE23FC51F6B92
SHA1:	45F057C90C551A71933393A45D46235C824D6065
SHA-256:	20D346D7BC759AB8A4C544EF062F2E34781258A9B553773BB408641BD01220EA
SHA-512:	7313B95D141355AEFA290FD70C2EED57C3D018A5E2EBBDE978E7C0956AE898F75D92E5560709E4965A7A89BEC564E55B92CB0F851775F85A4A1D0DD9DD7764(D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .5..,p./....."#.D.....A..`.....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....J.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Entropy (8bit):	5.497134532335113
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtum6uby0zBUKSAA1TK6tD+4fPYOFLvEWdtuEZHYby0zBUKSAA1TV:pRUubehRRQbe
MD5:	7B0DE5643406C2DFFAE66CCF99A645EF
SHA1:	B2A68D72E2611A4329F45E2D436B7C04D668A0DF
SHA-256:	751EAE3BF306F0941F4CA5A55777D4337E84823F98D94BCC71EC23CD0AA63C29
SHA-512:	88BB19048F81E31703770B14B41622E5A2D00451EB0D0FA5564878515060CBCE728F8D90BB6A5B5361FD5F2591BC5AE022317DB18701E95934BE7C745A2BAFAA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..c.+p./....."#.D.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo...../.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..o,p./....."#.D.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....5.....

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):	5.530890969976863
Encrypted:	false
SSDEEP:	12:KkXxKMSCvBcDytUlnkXxKMSCvwGtUlbLkXxKMSCv+s1NctUlskXxKMSCvI3l3tUg:KkXxiCJcOWnkXxiC4GW3kXxiC/DcWskk
MD5:	65C90E9A7077CC530612DAA8C7891DC3
SHA1:	B40DA13374C1C2FA2F6CC2571C07C921F2C619F4
SHA-256:	4022038AF346526FBE984AC983FD9A7B0C411E005AA4B01AD2CC848342D5B3ED
SHA-512:	7E1802CEA4F465C59B6A784A15443EE7211291F96739256E4C8BD2AB9FEAF658FD643F7ACE05DB54440DBE4D2DDC57A156B868BECF7EE1D90C7859D3D00CAF 9F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..8.+p./....."#.D,.G....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....NF.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js .^..+p./....."#.Dnk.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0\r..m.....1.....5...._ke yhttps://rna-resource.acrobat.com/plugins.js ....,p./....."#.D2s.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .?.^,p./....."#.D.Be....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....rt.....

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):	5.6025199201680564
Encrypted:	false
SSDEEP:	12:5h6OLPYqkmJh6OL2Giqkz4hh6OLJ2akbh6OLGskrN:5h6AY/mJh62i/z4hh6A2vbh6jrN
MD5:	D11A1EDFC4535AAC29FC7C44AC3DEF00
SHA1:	9C61D4DCF69D1E759D6480D59AA331984FA83B15
SHA-256:	D2319EDF552127204CADA56831545664F7099C49EF7EB162544BE25D939FD964
SHA-512:	66BB23BD6E9867AB940B6E84A430BDDE61EFC11DF3F1FCF32AEA65266B24FDB5B416CDEA2D8307C3DCC0C1AC61F1A680C8897DB83CD126AB1FAA6AE9124C 224
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .w..+p./....."#.Dz.6....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 ...+p./....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....C.....0\r..m.....;...I....._keyhtt ps://rna-resource.acrobat.com/static/js/desktop.js ....,p./....."#.D.:....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....!hl.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .`.g,p./....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....e.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	732
Entropy (8bit):	5.624828858314464
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFPdnwSeKaTLnDcRVFAFjVFAFMwSeKaTLnqeRVFAFjVFAFE91wSeKa3:UB4v4VnwzXLnAB4v4MwzXLnlB4v4EXwf
MD5:	510BE0540C58543D1249A4F60CCA53C8
SHA1:	1EC9236D6B9DFD39150043408DA97F23DB2352DC
SHA-256:	507C299F4D3B1523BE9FD6150564A1713CAD6A47B82FE47013410CEEC0691B30
SHA-512:	DE11FA68842E47D32D1BBB4A49BBF85881BDA909D833F9353CD1498AF36A7789A214E12EB94178B2D95829B61CC165E3382608400179C13605458F730BD42540
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
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 .y..+p./....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....p.....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 .-..,p./....."#.D.=T....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....-.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...o,p./....."#.D.>.....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):	5.485275797682893
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQji65GFCaa+41TK6tl5l:NRMHdy5Gda+EB
MD5:	12DB1648730BAF34A6A0BA419C9893E1
SHA1:	62F558F9505BCA438D2878103DB4054F38F5D5C6
SHA-256:	C22E086F5E0DB6CAA69C658233BD08A5042D02E35DE84F0DE4F1DD5C2C842922
SHA-512:	D91061F2E90CD651D858939DA57BA015FD870CCF5AB65409B7A390B50715DB9485F8EE2444354D58CFF783192BC05AB13B0AB2A6E193C8E60C90679C0FFAB31
Malicious:	false
Preview:	0\r..m.....R....L...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ....,p./....."#.D._.....A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....di.....

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):	5.52711285437214
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXup9c/oPb11TK6tNEs2VYOFLvEWdvBIEGdeXu7cS011Tk:BsR2EsetGXsR2Ese4cx
MD5:	BDF6F98D38A7BF165E19B114B2639A47
SHA1:	89810E5C786616530333BD9887DF419C4080D588
SHA-256:	B643BF2B51D01915E373944DAD50C58D6A329A08FFB98E1B54A7154117BD7089
SHA-512:	8D6412436D8DBAEFE0CB37E0B7D596A49579C66E77ADD967D189A0FC17F8F5BD96AE8C53546EE657EC31AF054E415718E59B3FA3149DDE3DECB25EE93F171330
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ....+p./....."#.D.*.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....K.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..<n,p./....."#.D.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....Z.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.6282442189920925
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQZc8Fq1B7OhKlvA1TK6tHMaVYOFLvEWdwAPCQT3YoB7OhKlvO:RbR16GC1BJkpbR16aIoBJk
MD5:	AEE298114137A1D5640982B3AFDAD825
SHA1:	59EA58C9DCDCBF0CE8C4AF7DBFF8C86C77B21711
SHA-256:	75049E0485F33346EF20450CBC9A1FDB53EE1F987EC189EF0FB3155E6F5F2905
SHA-512:	68BD6915B6D3DFDC3B29663B6E681D424E814838A91A27F144A5DCFC031D171BDF8FEED36476E57AB6BED55E7BF83FAAA3F1BC8B40CF43A6B4AAC1EEE9216D45
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ....+p./....."#.D.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....y.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .Qtj,p./....."#.Dp.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....fk..... .

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):	5.587545792403011
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
SSDEEP:	6:ms2gEYOFLvEWdGQRQVul8ywnLQdFt1TK6tQs2gEYOFLvEWdGQRQVugQdFt1TK6t:B2geRHRQAbwL092geRHRQf0
MD5:	3B414CF69DB35B3FA49589045A005C75
SHA1:	4B243B58E282A900BBB56E89E019D59E84068C5C
SHA-256:	13269A7AFAA9919689C284938209D8384EA191ED5B415C70975C136C0DDFC2B6
SHA-512:	F9D16E47509BB3D426A3B495454CC0BD780DECBC1E1AAEFBFD4EE8F6213ED0C9E48524A449419EE273D329FC81E001ED97AB7157DF21F6974A1658226721664
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .J..+p./....."#.D.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..:n,p./....."#.D.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....0.....

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):	5.653227879151244
Encrypted:	false
SSDEEP:	12:WyeRlONt1wl/MyeRlif5t1w/9/MyeRlxWqt1wxyeRlxt1w:WJefwl0Jqf5fw/90JpWqfwxJJfw
MD5:	9F62380078E145CD604B37F6B375A534
SHA1:	24270BCBAD28B5533CB15FAE457D75D439D8C589
SHA-256:	13CE52D45DC8B64B018BFC60AFD15777D3D1A859DEC5EBC461649EDBFAE7CB0F
SHA-512:	CBA9E468A551B8443A0EC8E4FFCE77E5D798EEFD8FA3FBF68D2D0F470B096D2BCEB6E7CEF88333F54ADDD23044018C9F8E9E8E59FCD299BD1D21F8E683AB185F
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..(.+p./....."#.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 ..$.+p./....."#.D|.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....).f.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ....,p./....."#.DV.C....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 .4.h,p./....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....+).....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.542664597470618
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyupVjRqwK+41TK6tB/EnYOFLvEWdhwyu41vIqwK+41TK6tp:wRhScwK+ESRhJ1vhwK+E
MD5:	FBCCF5B17B07603F06BBC553F41B934B
SHA1:	CA23D5A80CEF1A7AF924658E5E4AFFF9E2A59911
SHA-256:	4720CAAC664F5E3CA308A1022784B7879126A83825C79F08DDBD56DC8D7076C1
SHA-512:	2EFDEE9A06F6FADD9F53A47576CB2C90758F1BA1882A3E3682043F1A52E0FA8F697B1C3FCA28A89DACC2CA69EF4911CB7DF64C95395E025A222E984F1B89513A
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..g.+p./....."#.D.z.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....a?.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .1"j,p./....."#.D+.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....v..?.....

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):	5.6012043191818135
Encrypted:	false
SSDEEP:	12:/RrROk/+fLEmRrROk/WpfLE4RrROk/eIfLE0lRrROk/ofLE:/PJ/+4mPJ/Wp44PJ/H4oPJ/o4
MD5:	DAD3AE76C8D9E68C02BB3DF4EB0874C7
SHA1:	DAE9861E36FCD934AD619BBF5B1F3661E4AFFE90
SHA-256:	4CC08801ADA9D775792DC51681483D088C22955168F7892E9EDA33F1578D7775
SHA-512:	ACB751E53E0E5C6E4DCB05B6E957CECA0564C7547B85AE143C8C2AA0D98577C2F4DD0FC7855E60B04C8C1B9A117484A44A9616744681B954CAEDDCF5E5F5A52
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....+p./....."#.D.^<....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....c.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....+p./....."#.Dg.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....&k.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .. ..,p./....."#.D/.C....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....S.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..h,p./....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	744
Entropy (8bit):	5.573208012190657
Encrypted:	false
SSDEEP:	12:xqT86oCPLnXAqTtxZQCPLnnBqTo+NCPLn5/rqTLxCPLn:ANoMnnBzQMnnQbMn5WPxMn
MD5:	7E8BC9BE5CE1F2E906A9E0F776411C59
SHA1:	F72E533DCC734869A78610FD5422DAE2887AA6FC
SHA-256:	465450C931DC608888BA23886A86C2B886A5844615B03F4A1184673AB7DCF658
SHA-512:	C213E9DEA1304FFE997EC72EAC520095C3650579557A130EB28EE35A852075EA0F33564DABC9C4C7457A737AA35814C980D8E48823695589A0122AE1B2BC28E7
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...+p./....."#.D..6....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .i..+p./....."#.Dr.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....,p./....."#.D.\....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,p./....."#.D<....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....e#.....

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):	5.623699281541974
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuO/RWsEJ41TK6tR252YOFLvEWdMAuiyCDWsEJ41TK6tnZNM52Ym:zRMJsDzjRMqCsDBZRMbStusD
MD5:	06240011520035 60BD8D0EF5D01AC148
SHA1:	C18BC0F2E9B1F9D2F3AAF9F9F72E2265BD7A892E
SHA-256:	3AD5C05545856C45ADD0F95865ECDE0EAB679E5BFCDD7E4E06A173C0B37882C4
SHA-512:	12082E73A332A3F83DD07A1A05EE7F58C9E50739C5BE8BBCC234110BCF92FB575289E2D6896BC90B32C4A02C50299BA34D9696DE683C9332E24A3C285AA7C0D F
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....+p./....."#.D.w.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....,p./....."#.D..O....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..>n,p./....."#.D.*.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo....XV.....

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):	5.593998194872934
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAu+cucqMESFong1TK6t1YilPYOFLvEWd8CAdAu6lSSFongv:6lJRpAFoMplJRF7FoMaclJRcFoMbAt
MD5:	CBD125919FBCDB778703F06B0218639C
SHA1:	E9D1572936998AA64EF4383DD65DD464E5FC4ED0
SHA-256:	957D63BC5F1BAA19FC1456F17CC397D5041E7E0E09A6D31DC00D5C1DD56E0EB3
SHA-512:	1452A23B46BE81620428009461AD80F8A3BFB09014B1375230E1EFF42D1D702F626DDEBD367C0A595B74874A84099F21605CE6ADADC820FB4BC2B1D1E98CCED
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...+p./....."#.D.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....&6.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .J..,p./....."#.D..O....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....R.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..@n,p./....."#.D.@.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....m.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Entropy (8bit):	5.605528470059793
Encrypted:	false
SSDEEP:	12:F8hRrROk/bje2m8hRrROk/Re2R8hRrROk/fie2c8hRrROk/cce2f:UPJ/G27PJ/E24PJ/h29PJ/I2f
MD5:	750629E2EAE67AFE8F3E36AF64E902F2
SHA1:	7DE9DD1AA74C6E971DD9703CC7421E3E41A531DB
SHA-256:	E83FE7A0F0BD6A892F4D8CF444FCAB9B6988FBA596B2BE57F5DC1FE224E58237
SHA-512:	FEAE65BAB42C01C3DF123006D29CAE2A901F75EEF3BEC84EBA830642939F1D6AE32673F11A757C05ADF244EB89A064D03F50962ED2991A825A702F52C1B1683
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....+p./....."#.D..;....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....BK.n.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .Z..+p./....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....a.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .^..,p./..... "#.DJ.C....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....{X.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..lh,p./....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....A.....

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):	5.66139703946498
Encrypted:	false
SSDEEP:	12:ehRc+ZFirNJICiGhRcu0lS9irNJICXhRcErNJICshRcjrNJIC:ehVMJICiGhLh9GJICXh3JICshiJIC
MD5:	751A942BA6066AC03C64CDDBAB3C2BA9
SHA1:	98ACD57F1A82E76AA6751FC63A1C7CD11F3A6942
SHA-256:	7664957334EBDA73894CC40585BF8CCBDB1AA1AD69DAEA8FE11117CE82964F59
SHA-512:	B4667CBA72F034E01D5ADDE8EBB5899E7CC90BB404E4185A4D631AB26802B90F989C0F4C7CEA572FE1F89E1F160F7218CF098C4BD80A6358CFA1465BDE1F60 8
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..*.+p./....."#.D..<....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....I/.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..&.+p./....."#.D.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....t.x.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .X..,p./....."#.D..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 .y.h,p./....."#.D?;.....A.;"./N_.,.:C..2 ....9L.H...3:...A..Eo.....A..Eo.....v.....

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):	5.6054926143802
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuVj+/oshLzgm2d/1TK6tZlMOEYOFLvEWdrIhuxZtChLzgm2d/X:0RMZRezkRRIZReJRYJZRer/KRlZRev
MD5:	1D159545DCC88034187F5E1888862628
SHA1:	C75314FC307F3424E94479EDFF8B1D3870B9BE04
SHA-256:	6E64C0610A4A2B194E43AC7443A69BCA5A70906FFCED49463F8D7156764A48F5
SHA-512:	A6C060E58FC77B8F46CF39F7F085B9685AA31DDADB390C97B491B300B7DE71F1CE645EA47B7538B5603C062EE3EB58B8116AE78BCB800B578A8537F33665BC8 F
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....+p./....."#.D.:....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo... ....=.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....+p./....."#.D.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....mT.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...,p./....."#.D.C....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A. .Eo.....A..Eo.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..jh,p./....."#.Ddv.....AZ.Z}Q..4.o....0+..[|..n:*.. U.W.A..Eo.....A..Eo.....(.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	752
Entropy (8bit):	5.5888428112658906
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KDziW2kx56uvp1TK6tReMAElVYOFLvEW1KOskx56uvp1TK6tn+V:6JJKPiwnXJJKQ1CJJKc3JJKRpoK
MD5:	444829C0FBCB51C9F883F706376B287A
SHA1:	FDC8E659377C5F6D99E8617B2060DDB0E3BCB9C4
SHA-256:	864ED385A737C38FE6F23435DF7FDD04CBC615CE8AC9B97C0CA4006CF4FD7BE3

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SHA-512:	C5368B3987FF3027A407ADB828B8E6F9C12C5A8D9D8BD06C5D4003B3F16D8534FFCDBCB09A432A509DAB3C97A9EB0652F780BF9F3680A5BD275A13FE30145E B
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..U.+p./....."#.D2X.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....^#.....0\r ..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....+p./....."#.Dis.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....cy.....0\r..m..... <...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..r.,p./....."#.D*p.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....8R>.....0\r..m.....<...)6. ....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...`,p./....."#.D..t....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....8&.....

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):	5.626182943266345
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuqyNY0yhUDLYtmOZn1TK6tllEWYOFLvEWdBJvvu8JNV93yhUD6:xRBJlY0HDcFZL5LRBJ1JNP3HDcFZL
MD5:	4231EC452E4756B965334D9D66ED987D
SHA1:	189D49530AAEE5588C1591DA5FB561D2484FB7B9
SHA-256:	FC36D6CB8616F5AEF4352F9C60C894C55333640607CE5C79A275CCCDA13F3394
SHA-512:	C235295DA75EB23B2CBD7C450A8640CEC438811EBC84A993553463A350ABD7A9234152693F9929C9F6504775263878796C0EF5DD5AA4707874581C6E30AF9CDE
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .q..+p./....."#.DD.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....+Z.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..=n,p./....."#.D.....A....t.q..W.EZ....1...[.zC.7mD..A.. Eo.....A..Eo.....Z;.....

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):	5.631453107861455
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp73Fc/lARVPu1TK6tnsRPYOFLvEWIa7zp7dSRVPu1TK6tRf2R:BPHQ8cWPHSRcD5PHWMcyPH/rkco
MD5:	EC5C4300402401A50DB7B60080A3C37D
SHA1:	049DE4486CA0D1FD6DC066912DA47706C504C13C
SHA-256:	608DDC274E056682FA428FC4C7A6E46FB0DC45E0249A4A40D61ACB5E0BD480A3
SHA-512:	8F3D456BFF54A60459795F5E50757CC50C643075CDDA44A736F7F53D4D03B8D4627DFEA7BCF6E9E90120ED35ED6E46B0DB87E82DCB0308985CB31A2B53A3FA 4
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..P.+p./....."#.D.@H....A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....6.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....+p./....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo.... .....A..Eo.....U.}.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .m,..p./....."#.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 .h.^,p./....."#.D..e....A... L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0-.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.553843808635296
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QEOGdiM3Y1TK6tIeKPYOFLvEWdENU9QaKlY8DiM3Y1TK6tnl:bJRT9Fr0uzJRT9Q/Dr0
MD5:	3980663670A29A6CDDCB5EB42782F5BD
SHA1:	8BBD008765487EA9502C9C53D784C7F14CFDF42C
SHA-256:	465CEA20C81C2E2FD38BD0E4A8C251DE8B463B484AB10CB6E261239A66DB2B34
SHA-512:	0A004D9B0D9F7768480B8D39B106B694916554C93EA83451225760EF4FAE35C91B2A12C6FE6AACDEFF58D6CE57BFCF1837D2A71C5811827D71F3B433F03E5A4
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....+p./....."#.DA.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo. .....Dc.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .0wj,p./....."#.D|`.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... .....A..Eo.....ui.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.592243727778103
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQYoAQihjBRCh/41TK6tKQt6EYOFLvEWdccAHQtFhN9+IjBO:XRc9jDi/E9Rc9+/N9+IDi/EI
MD5:	C178BD20E4A9F71112CB3223803F3387
SHA1:	70D7FED62A8024E20FEDBA487696722984FAF13F
SHA-256:	9E95441593A730F0640E97E92D1B7613F0CA7870A488E709616B3B5DF4580CF3
SHA-512:	64A0B2458EBA812EE7D5525614B97C601627D50962CE84F60E37761E7ED2067193E453ECB8C33B9A5F90FF3A94C9CC2D375BD7914A39421DD30D2E64DE46E5E
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .}..+p./....."#.D.%.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....7!.S.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .y.o,p./....."#.D~.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....NK7.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.555486626420864
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuObu+ULlF4r1TK6t:bs6xRkihLlF4n
MD5:	9331F1AB377517CB16A2664CFB05BAE9
SHA1:	E977B2A485BB43D81E4E9C599C99405226A4AD09
SHA-256:	3D000B60F01450D8AA49320E908E09D22D3FD0D854D6557DE7E82CADCE32E9A5
SHA-512:	1320692CC5985098EC09C4975D73FD3609B44AF32A60C5415147BFE8DA27AED334E5F4362CEDEA785DD8D75769124829F81C44F68691578C9C93EA339AA7AA8
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....,p./....."#.D.zF....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....)f.....

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):	5.5080917002329075
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuYuT+h941TK6tZuhYOFLvEWd/aFuihT1941TK6tx2:WRqDh9EiRIT19EH2
MD5:	7FDBAD06D5B618130A4A22F674934ABC
SHA1:	6E1E2F5EFF82355DA2B28E3CFCC65E8F93EF4883
SHA-256:	56A36E3D665231D9182501AFFB07DD8FE9197B11B2744EF1BD1A602674C5DA12
SHA-512:	FD2A2532430792EBEC1E63AF58710B7284325A79B483D896B1F2160B3B0EA51EEAD790FB59B958A55FC1CF89E12C03FAE9EB6C4D1FF070CFB60C1E49E8CE7C FE
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..v.+p./....."#.DGw.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....^x.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...o,p./....."#.D".....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....8.....

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):	5.535771713656583
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQDl/DGGJGoBMqVd3G4K41TK6tZ/ER9YOFLvEWd7VIGXOdp:2DRuRex5B9Vd2kQDRuRfGYB9Vd2kb
MD5:	E33F7DCF1B25321044EBD08081B0FE74
SHA1:	1FD950DBADC71DC5CD719B41E5F178E18BC5166E
SHA-256:	D7172685D7FD70B8260A8927ED7B38DEB7E7480642E6C224C6A7F2375CF61517
SHA-512:	FF6EDE5A082F056AA43A340424FF3F5C07C4C3FA7351FA35055F0B0EDFCDA3B82651E069D5DF79FB07CC50F740A08DD32806970D7D80D147A655C3307635679
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..J.+p./....."#.D.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....$.e.....0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .H.o,p./....."#.D.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....w.....

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):	5.618681521437439
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QJ4BFuA424r1TK6tZY/MkqYOFLvEWd8CAd9QBFy+leZNuA4H:+RQWmUrn0URQ2WirnIRQb8rn
MD5:	A8160020297CF50856A4F28C8D000BA4
SHA1:	924BF80D8664F7BC994ADAD26169F04EEF8841F7
SHA-256:	32BFBAAE8390F3073C064F367F2F38DEF26D885A09066911D47F7D24E3139D4C
SHA-512:	3B7CBDE7298342A76276063C815D7FC1B0FFACD9C674B3A6AEEEDA09CCF26C6D8A3D7498BD060B5E5934048896D3F6458345E4CEED38CFFFFE9CD3BA4A8BE B98
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .^/.+p./....."#.D.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ....D`.....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .b..,p./....."#.DH.R....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....Q.,y.....0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...o,p./....."#.DZ.....A#..@..k(v.8g..5.~_....]Pj.*..6.A. .Eo.....A..Eo.....x.d[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.518265918523231
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuEuYGYAyC8n1TK6tZEoXXYOFLvEWdENUAui3jAyC8n1TK6tp:xhRTSA7Qf7hRTwTA7QT
MD5:	65EACD630B04EBA18F1DAF7A6F6C2CA3
SHA1:	D5D00AAAC030AE36F20FC42321E10298E63B094E
SHA-256:	CC26EC65C51CACF7EFED4AB885546FAA007656D548F4824D80240B2DA3B9A243
SHA-512:	EE545B1D8E58D7922C0E6D559BBF2A8DCB0FB4B9BC8EE4EF13BAADA0C087E669D21B45798362DD4B922AD3F95FBA6F4E5699DEEDE6D87D3AB7ADB17F65B5 7A49
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..e.+p./....."#.D.g.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....US .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .. j,p./....."#.D.m.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.. ....u[.c.....

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):	5.640503325567641
Encrypted:	false
SSDEEP:	12:nRrROk/Vr6+mO1RrROk/VwTm9XRrROk/VTFTmlXRrROk/VaJnym:nPJ/+O1PJ/iyFPJ/TylXPJ/8Jnj
MD5:	B5799A5AEFC27071F149CD8F558AFB81
SHA1:	6AF20D0F0B4A90FF20B7A24039DFA31FE61A976D
SHA-256:	5E5E9F138DBB220DB47C2786653CDDFE626E73DF609E5C224CC602D68E68BA72
SHA-512:	199C36651D9CBD30598624FAA2B26F6D2CF3F28EAB77463386862E8ACB4F2E09F97351AB51E8D6D97530F0E9D6966248BB5B9273E4544273977ED3BF3E5954D2
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..T.+p./....."#.D..=....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..*.+p./....."#.D.(.....A ./.ev.....N~..6.b.....$.j; :C...A..Eo.....A..Eo.....s..$.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....,p./....."#.D.'D....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .. .h,p./....."#.D.x.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....AE.....

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):	5.568271346160187
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuk/lxAdm9741TK6t2Z/lXYOFLvEWdccAWul+nlik+Adm97S:qxRcUAdu7EsxRcyZf+Adu7EN/
MD5:	239F30AC94065DA5F86B802770EAC3D7
SHA1:	6860E61630C71A45F1B6DA0FF6F6784DE9F011C4

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
SHA-256:	2DB64D29DCD34A80C2A351FC0264B6DFDDDBAEDB1C902545370579E3251352E3
SHA-512:	2E2A644F80874C93B57A0181181CA62B3500C9F4DD89D4F33A2C892D7651001F9E64CEEB784D9891F6875CD0BFA0BBCF6C69B21FA13BB66970FE55AA25270FE
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....+p./....."#.D.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....D/Q.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .z.n,p./....."#.D].....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....Hb.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.580114883078506
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuEVZtv4Jn1TK6tLltMMOYOFLvEWdwAPVu8+KuN4Jn1TK6tG:2R19ZheLvtMR1j+jULQ
MD5:	07AE54EE720E32EF08C9BE6F566E8818
SHA1:	4C0EA1410C7F26972F3BB660190D8D46B86D6A7F
SHA-256:	7BD46DAD9B66A6198923CFBB27FE33C9C8085B6A460998B8DBC41813DB8E6EC3
SHA-512:	6FFC8DB0F9798224859921B6B9CE7665D4F5A6FA60D6D6B25978D3FCC1A91713287C6E82DD5677464044E92CFA7B54752F7BAC450B322D2AC694913FDA69871
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..b.+p./....."#.D.K.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....~.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .~.j,p./....."#.D.D.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....y.....

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:	modified
Size (bytes):	424
Entropy (8bit):	5.6562746764011935
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ9JBJzhcsBXIh1TK6td/E3PXYOFLvEWdBJvYQvCszhcsBXI7:mxRBJQOfJDB07/AxRBJQKBDB0
MD5:	6A381605C9B2CD94612C58362B0135EF
SHA1:	BC0844F5186D294C92F63BCE8C5A3AD0BB11A7B3
SHA-256:	70A181036B2BDA254F2928B9B931449140A9D56E36C0C0BFACAD70564BD5444E
SHA-512:	2F9C2DE89E6DF5A822255B2A491A23349B7AC50C982D9A655C4247F4CE1C4C74A64DE7DB2452F76ADAA8353D1CF07791783614FAC7C281BEE348F3D5FA0C88B
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .,..+p./....."#.D.$.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....;v.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .3.o,p./....."#.D.'.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....(..X.....

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):	5.624913640869785
Encrypted:	false
SSDEEP:	12:3RrROk/sbtHc1RrROk/siVtHceRrROk/srHcdZRrROk/sM716Hc:3PJ/K81PJ//H8ePJ/I8LPJ/f68
MD5:	0BD88DADBBAE168298A730BF536CDD2F
SHA1:	E03386EB069AC9DB420C860DACF9BF851D11BECB
SHA-256:	814091D93426BF7CE11A8FAB970F9034B5A82CDBB9D0FB5283B12520D26CB745
SHA-512:	39F157F0ED83E861305B7BC76886E04525522A23E7CC96BCC1609FF55AA69D6BF999FD02A3BAF00529293C25B7062CB35E3E6156809DA18A418A78226BBB0FFC
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..V.+p./....."#.D.$>....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 .n+.+p./....."#.D6....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....2.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....,p./....."#.D..D....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....Bp.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...h,p./....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Size (bytes):	2064
Entropy (8bit):	5.3159695148929105
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPWVkzmWLqvYIzFXwC5PBHYMBCCtD3g9/L9/cFG9g3qbN:h1zZ4+dsp607Gr8R9j9Fb0A0Y
MD5:	2D6915CF67EB0B86288ED13E41C81592
SHA1:	86FD1B555730C5FA0659E68633B0BF6319102011
SHA-256:	0582F8A84E676D27924E584D9AF617B2105F957ADBA6D649CDDC5CA38F966588
SHA-512:	FEFAB366CC9DFEC8FFE5602B86A26ABB3DEFFC4DA8B4DBAA7EB69190DAF036627AB79FCB4A9F336CCD614E58A5529436FCB495B281F0DCF37A201CC5D01E7023
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....x..oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.208994619616938
Encrypted:	false
SSDEEP:	6:mbM+q2PWXp+N2nKuAl9OmbnIFUtpruKZZmwPdBMVkwOWXp+N2nKuAl9OmbjLJ:wM+vaHAahFUtpyKZ/PbMV5fHAaSJ
MD5:	C7A14AD218683A8D644F9F6FF81AD131
SHA1:	BBE0E44903F87BA6F1871CBE51BDC6C8882DA068
SHA-256:	51AE6374038500087D344AD18AC69631B547CC0C50065F2DC70A54E2C4FC371B
SHA-512:	27C62A0DFF226A483B22B463522DBE3182DB37A1C0574D4990F297E8B4375A957F19AD253CC5AC2ACD84770B6E4C48317AA5E36F7BA6D2C3485FB384047AF72
Malicious:	false
Preview:	2021/01/14-02:40:42.556 188c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/01/14-02:40:42.563 188c Recovering log #3.2021/01/14-02:40:42.564 188c 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):	1572864
Entropy (8bit):	0.00872536968366379 2
Encrypted:	false
SSDEEP:	48:TGEiaGEiaGEiaGEiCEhC9EhCrQEhCrQEhCrNsMhCr+sMhCDo+sMhCDo+sMhCDo:5IIKnonono
MD5:	932219FA8E3EE188F7590D30BD525EA0
SHA1:	A5A00EE74446A4F6AAD396A733363EB644F9C044
SHA-256:	BF21E3EC0D53A79A948DFD91E4ADD1A8A6DB39F81734AC117E8961A7B578DEFA
SHA-512:	F57F32A6C4E24934E5A2B92FC476448B9CFC32D5F4F1D28E2C6811B744369344092C1BDAF63A616A22C92B2CCA9ACAC8623B93AD4FA93B53A4FBF916409DF18
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210114104035Z-193.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	1.0662403271154774
Encrypted:	false
SSDEEP:	96:B+AfT+JcYYkP45O8n871ApL1MaMeZlMVM2ug2iVQiMM1VgM5U1tMOm4JV/5Baf6g:BPfT+MYbupLmk0VqYfynHo
MD5:	07215956041E31C762493367310E69D5
SHA1:	47FE67035D273C056ABB38F5EC1A43F623CEFCA8
SHA-256:	AB67C01A2DC7CD06365B57BE40DD21FF68DD8FF62533DB28AFAD2AD157610CBE
SHA-512:	8964E7BD526DF8F24D72274A1CA788A4D7A6E0D53D7255215AA9360F6567D834A03356B80FABD126E7CE43A780136F57A86AE26794BEEC41B8D0B0D81FBC957
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210114104035Z-193.bmp	
Preview:	BM.....6...(...u...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):	3.3614444428249173
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBka3OhbVCPL49IVXEBodRBkm3OhOCP749IVXEBodRBkJC03OhBCu:iGedRBoedRBjedRBHedRBK
MD5:	03705418CACAD2C3FC744F7A669C43A2
SHA1:	2E6D4B3FD65D28A6B429D656F1D09AB2BD74A0B9
SHA-256:	8806A2B7F8AEA2BE01CBFBBB7CDD968C49DE74FA3C0BD42AD14B9AAB5B0EDBF9
SHA-512:	EDAAD69137F31A08E0EF0749AF03A2388D2EBA52D8C36857D8F217CADADF04E6D97A8C8D25A1C0F68B943AA433A09F0D78E10F834C061EFC6B52CF23AA0F8E CE
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):	3.17361160017487
Encrypted:	false
SSDEEP:	96:V7OhFVCPB949IVXEBodRBkq3OhbVCP0LR49IVXEBodRBk93OhOCPVd49IVXEBodD:VNiedRBQLGedRBHCedRBZyedRB7
MD5:	BFCF1B7B3FBC3514614DE9171D9D2426
SHA1:	6DF1543A4ACBF9F2F053C9889E1AE9BC9EFC1BC7
SHA-256:	F6192250B047C7FE4F9E22569951C78673EB4EA5088FF1ADDCB50B8FD6F23B44
SHA-512:	0112DA1470CD1BE97FD886A14A75AC24C9EBF011ABC3D9BF3EBC903AA37DE8D75F36F3E43F50CA6FCAA33B0D7CCC7F079DB3B3A846D3FDB6EA6C0EAECB5 F93F
Malicious:	false
Preview:	.....!E..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5544	
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.Na meArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleN ame:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.N ameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-Bold MT.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 1.3
Entropy (8bit):	7.89351432901867
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	3PD4931.pdf
File size:	151374
MD5:	edc2cd81fc270dbf8c0f6b0fb3d825a9
SHA1:	44986311a4415c34c21c332d5efa089c48a37f56
SHA256:	6abd92aab60b58773698cf7fc90527c7c90bcb933d39b13ef10b4c06a9434371
SHA512:	e4f179c3792cc82847561359b08d414e25ebafbff09772ecdb47edd0c051382bbe9131c9f50351d46baf7ecb1455aba4e65797cdfac29a03257ebb26d93e44c5
SSDEEP:	3072:S2B9I6mikftJDBVol2B9I6mikftJDBVoV2B9I6mikftJDBVow:NB9Ig+B3B9Ig+BjB9Ig+BV
File Content Preview:	%PDF-1.3..1 0 obj..<< /Creator <>../CreationDate <443a323032313031313331343537343 8>../Title <>../Author <>../Producer <5265706f72744275696c646572>../Keywords <>../Subject <> >>..endobj..2 0 obj..[/PDF /Text /ImageB /ImageC]..endobj..3 0 obj..<< /Type /Ext

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.3
Total Entropy:	7.893514
Total Bytes:	151374
Stream Entropy:	7.900367
Stream Bytes:	145116
Entropy outside Streams:	4.773014
Bytes outside Streams:	6258
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	22
endobj	22
stream	6
endstream	6
xref	1
trailer	1
startxref	1
/Page	3
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

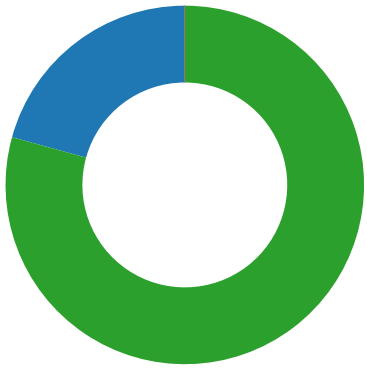
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:40:21.511648893 CET	60831	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:21.570647955 CET	53	60831	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:22.343765974 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:22.403014898 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:23.358392000 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:23.414670944 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:24.334076881 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:24.384959936 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:45.136604071 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:45.137490034 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:45.194202900 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:45.195025921 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:46.137150049 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:46.137182951 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:46.193542004 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:46.194293022 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:47.155179977 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:47.155217886 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:47.211323977 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:47.212918997 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:48.825383902 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:48.873421907 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:49.199927092 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:49.199970961 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:49.256567001 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:49.258378029 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:51.443438053 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:51.491615057 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:52.435286045 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:52.483237028 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:52.649653912 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:52.707609892 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:53.201728106 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:53.201827049 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:53.258094072 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:53.260113001 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:53.344332933 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:53.392172098 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:54.313080072 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:54.372339010 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:55.815589905 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:55.863640070 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:57.398052931 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:57.446023941 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 02:40:58.784709930 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:40:58.832706928 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 02:41:11.755570889 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:41:11.813230991 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 02:41:18.671509981 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:41:18.738754034 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 02:41:34.556268930 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:41:34.606993914 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 02:41:39.485044003 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:41:39.549772978 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 02:41:40.625948906 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:41:40.685940981 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 02:42:09.736186981 CET	60633	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 02:42:09.784326077 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 02:42:11.805543900 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 02:42:11.861820936 CET	53	61292	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 4156 Parent PID: 5708

General

Start time:	02:40:27
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\3PD4931.pdf'
Imagebase:	0x1170000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11A65C3	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	11CAE05	CreateDirectoryW
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	11BEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210114104035Z-193.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	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5544	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	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock4156.1.2804461176.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	11F2657	CreateFileW
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	12383C8	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	12383C8	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	12383C8	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	12383C8	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	12383C8	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	12383C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rxuqp8u_yw8ymm_4a0.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	11BEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1cwtsns_yw8ymn_4a0.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	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1tn0hvh_yw8ymo_4a0.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	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Roe0nc5_yw8ymp_4a0.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	11BEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R15bb9rs_yw8ymq_4a0.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	11BEA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5544	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	11FD405	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	11BCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	11BD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	11BD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	11BD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	117EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	117EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	117EA55	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	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/3PD4931.pdf	success or wait	1	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	3PD4931.pdf	success or wait	1	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	11CDF69	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 33 50 44 34 39 33 31 2E 70 64 66 00	success or wait	1	11CDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 31 31 34 30 32 34 30 33 34 2D 30 38 27 30 30 27 00	success or wait	1	11CDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	151374	success or wait	1	11CDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	3	success or wait	1	11CDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	11CDF47	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	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	11CDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	11CDF69	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	11CDF69	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	11CDF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 5544 Parent PID: 4156

General

Start time:	02:40:28
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\3PD4931.pdf'
Imagebase:	0x1170000
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: 5388 Parent PID: 4156

General

Start time:	02:40:34
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0xb20000
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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	C159E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	8	C283E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	78	C28447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	219	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2178	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	7	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	23	C159E2	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-files\js\plugin.js	unknown	4096	end of file	4	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	24	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	55	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	248	C159E2	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	3	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	3	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	C159E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	15	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	16	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	325	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	31	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	178	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	10	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	C159E2	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	C159E2	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	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	C159E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	C159E2	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	C159E2	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	C159E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	98	C159E2	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	C159E2	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	C159E2	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	C159E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	C283E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6292 Parent PID: 5388

General

Start time:	02:40:36
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1708,1282318598042692567,6584645183887421796,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=16114704440535557804 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xb20000
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: 6316 Parent PID: 5388

General

Start time:	02:40:38
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1708,128231859804269 2567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17658040393359851026 --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=17658040393359851026 --renderer-client-id=2 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb20000
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: 6400 Parent PID: 5388

General

Start time:	02:40:40
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1708,128231859804269 2567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1535626254935326759 --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=1535626254935326759 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb20000
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: 6452 Parent PID: 5388

General

Start time:	02:40:42
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1708,128231859804269 2567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10496770992156748853 --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=10496770992156748853 --renderer-client-id=5 --mojo-platform-channel-handle=1872 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb20000
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: 6856 Parent PID: 5388

General

Start time:	02:40:51
Start date:	14/01/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1708,128231859804269 2567,6584645183887421796,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16098587735302563493 --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=16098587735302563493 --renderer-client-id=6 --mojo-platform-channel-handle=2296 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb20000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis