ID: 358577
Sample Name:
CTR00068CP1PDF.PDF
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 21:35:05
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

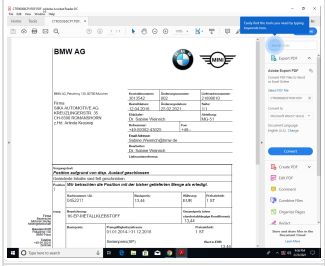
Analysis Report CTR00068CP1PDF.PDF

Overview

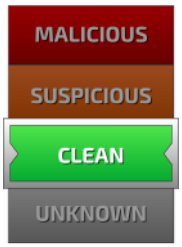
General Information

Sample Name:	CTR00068CP1PDF.PDF
Analysis ID:	358577
MD5:	e224bcfaa02a888.
SHA1:	599a043fa6f27fe…
SHA256:	2db74b42a9f7442.
Infos:	

Most interesting Screenshot:



Detection



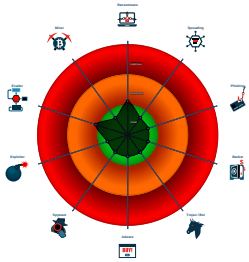
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Contains functionality to access load…

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 672 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\CTR00068CP1PDF.PDF' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6040 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\CTR00068CP1PDF.PDF' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 3288 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6152 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=1700,144647073828735727 9,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3630556925514522147 --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=3630556925514522147 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6184 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1700,1446470738287357279,6939926539180054600,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8690066333002460602 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6232 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,144647073828735727 9,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2706402308431694826 --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=2706402308431694826 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6372 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=1700,144647073828735727 9,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10726678641985929267 --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=10726678641985929267 --renderer-client-id=5 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6600 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=1700,144647073828735727 9,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14471897307288007299 --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=14471897307288007299 --renderer-client-id=6 --mojo-platform-channel-handle=2144 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

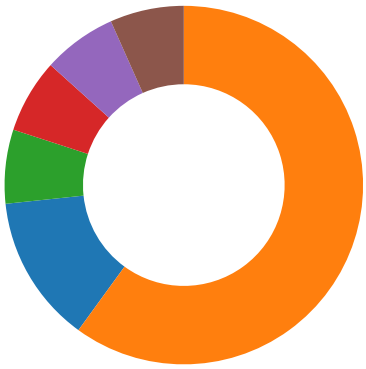
Yara Overview

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

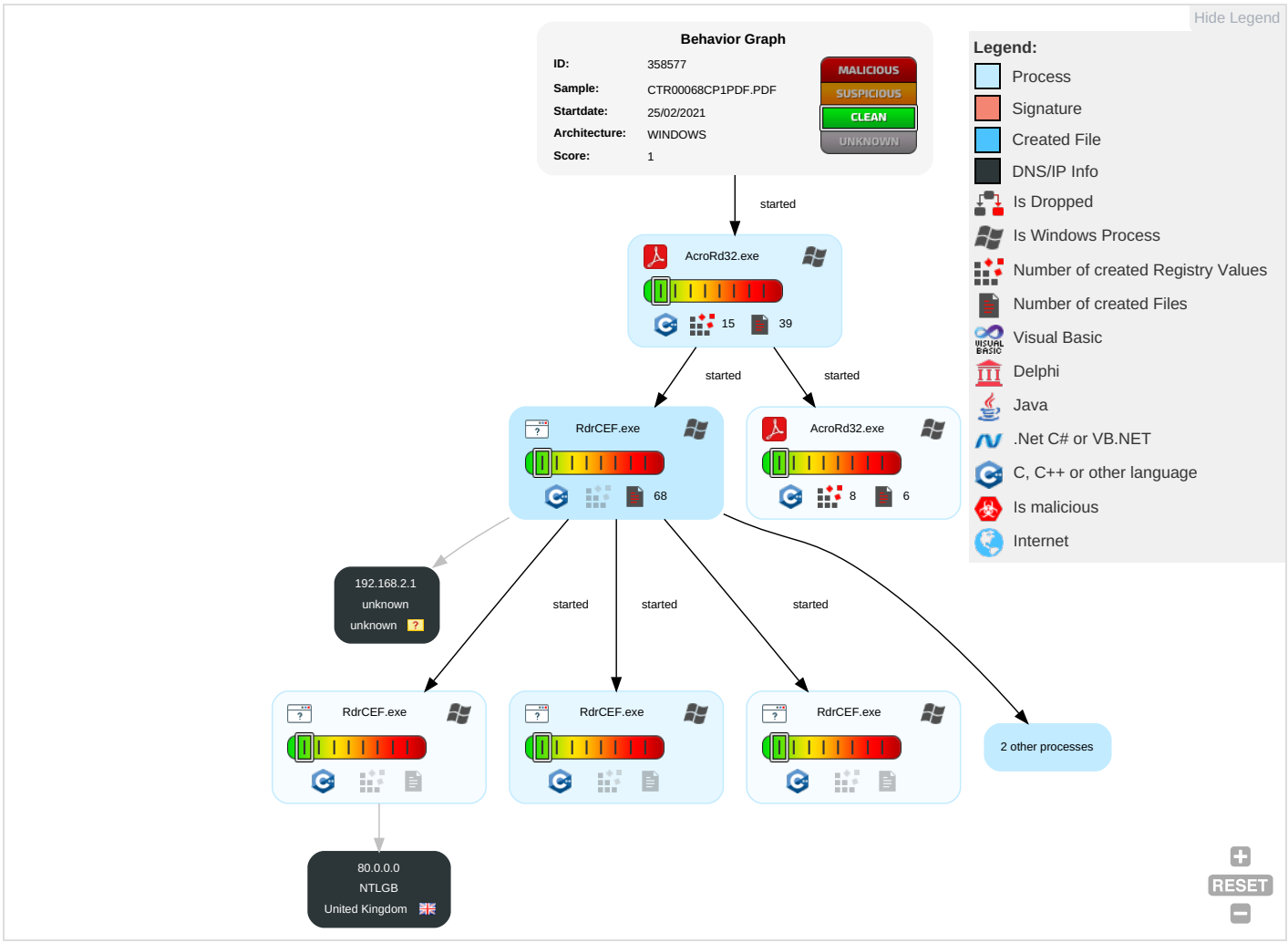
Click to jump to signature section

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

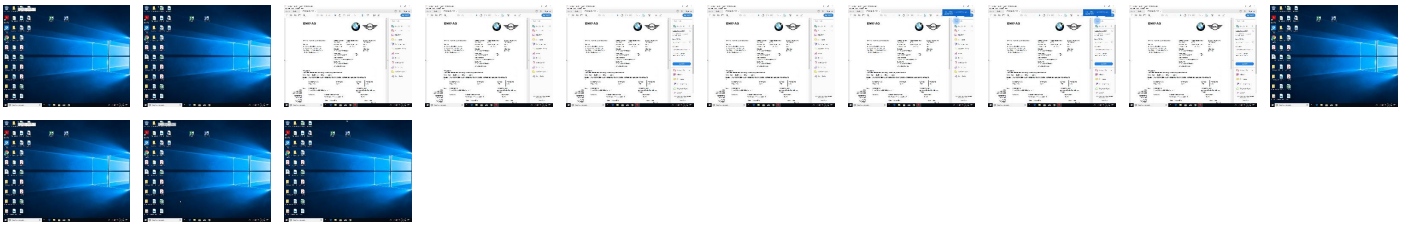
Behavior Graph

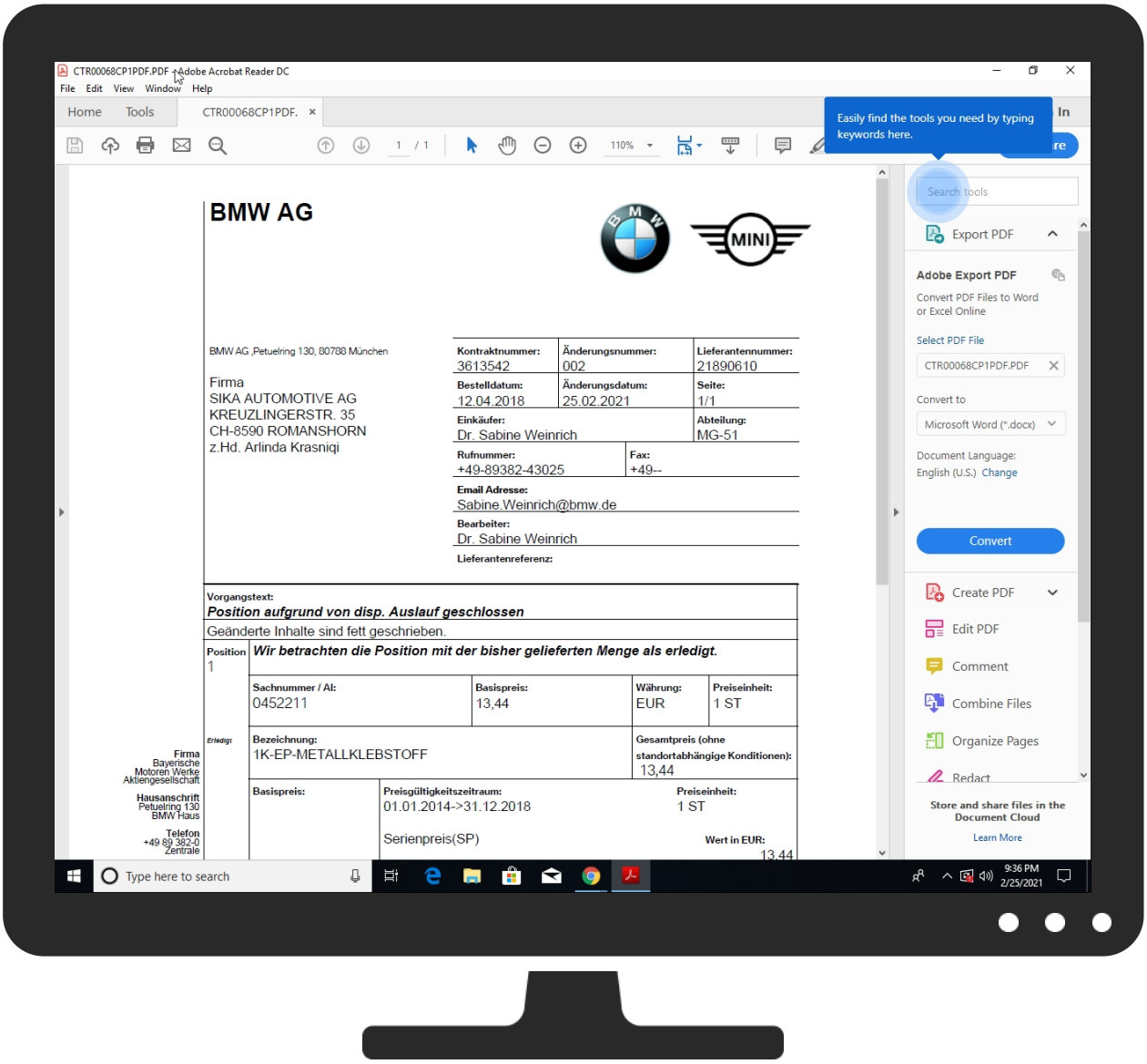


Screenshots

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
CTR00068CP1PDF.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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/Ch	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/1.0/2(	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/g	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://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/wh	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/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://api.echosign.comd	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/J	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/265	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/r	0%	Avira URL Cloud	safe	
http://www.bmwgroup.comH;	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://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/41h	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/k	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://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.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://https://api.echosign.comocessId	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

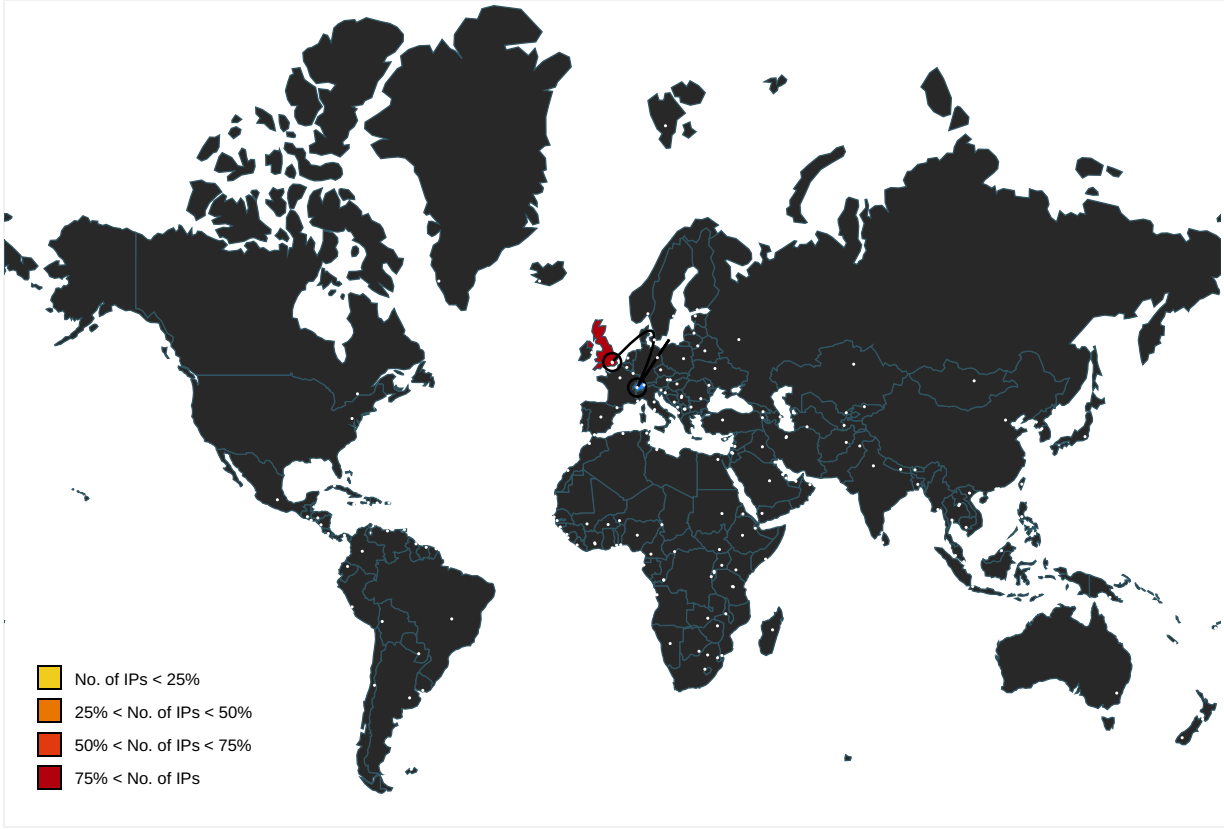
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/Ch	AcroRd32.exe, 00000001.00000002.370040068.000000000B52F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cipa.jp/exif/1.0/1.0/2(	AcroRd32.exe, 00000001.00000002.370433136.000000000B702000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/g	AcroRd32.exe, 00000001.00000002.370286659.000000000B641000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.370433136.000000000B702000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.357026055.0000000007C40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.357026055.0000000007C40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.370433136.000000000B702000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/wh	AcroRd32.exe, 00000001.00000002.370040068.000000000B52F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.370433136.000000000B702000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.357026055.0000000007C40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/type#5	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comd	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/J	AcroRd32.exe, 00000001.00000002.370286659.000000000B641000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.bmwgroup.com	AcroRd32.exe, 00000001.00000002.370286659.000000000B641000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/265	AcroRd32.exe, 00000001.00000002.370286659.000000000B641000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.370608654.000000000B77B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfe/ns/id/0..	AcroRd32.exe, 00000001.0000000 2.370433136.000000000B702000.0 0000004.00000001.sdmp	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/r	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bmwgroup.comH;	AcroRd32.exe, 00000001.0000000 2.370353839.000000000B695000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.0000000 2.370040068.000000000B52F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.0000000 2.370433136.000000000B702000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.0000000 2.357026055.0000000007C40000.0 0000002.00000001.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, 00000001.0000000 2.357026055.0000000007C40000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/41h	AcroRd32.exe, 00000001.0000000 2.370040068.000000000B52F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.useplus.org/ldf/xmp/1.0/k	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.0000000 2.357026055.0000000007C40000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema##	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.0000000 2.370286659.000000000B641000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.0000000 2.357026055.0000000007C40000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.0000000 2.360686606.0000000009420000.0 0000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/extension/1	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.0000000 2.357026055.0000000007C40000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comocessId	AcroRd32.exe, 00000001.0000000 2.370608654.000000000B77B000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: 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 Emerald
Analysis ID:	358577
Start date:	25.02.2021
Start time:	21:35:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CTR00068CP1PDF.PDF
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 40.88.32.150, 104.43.139.144, 13.64.90.137, 104.42.151.234, 13.88.21.125, 23.32.238.123, 23.32.238.113, 23.32.238.129, 23.54.113.182, 51.104.139.180, 184.30.20.56, 67.27.159.254, 8.241.121.126, 67.27.157.254, 67.27.233.254, 67.26.75.254, 20.54.26.129, 51.11.168.160, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:35:54	API Interceptor	12x 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	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	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	
	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-WnHuSljf0v9YP9XHTo1mHg1DdlnrlGltn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	vUp5vjYOoL.exe	Get hash	malicious	Browse	• 80.0.0.0
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	• 80.0.0.0
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 80.0.0.0
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 82.12.157.95
	wEcncyxrEe	Get hash	malicious	Browse	• 213.48.143.199
	Swift.pdf.jar	Get hash	malicious	Browse	• 80.0.0.0
	0001.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495.jar	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 80.0.0.0
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	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

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):	820
Entropy (8bit):	5.6824698661360875
Encrypted:	false
SSDEEP:	12:vDRM96rVZiEBnDRM9+akZiEq+tlhDRM9f9eZiEPDRM9thZiE:7yEBDuEq+X1OJEbq6E
MD5:	19C1AD59EDE473C9F03A4FB8D037177B
SHA1:	9BB3529072F5118A5FDEB7E95BA1AD96C4DA799F
SHA-256:	39EB09CFA4CA0018439959A5E97275A4D142CB97544C9531E16C0F54912B2097
SHA-512:	2BBCD3FC1004C33C6DC7C52DE14A9D8ADB386C381A8E8BC2F11169313CD0D543D39B9FCFA7F9AA720A3293A3A5E044A9A28983B69B06ACA722602BC0488C9 6C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../...."#.D../"..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... YM.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../...."#.DY..1"..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....M.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ./...../...."#.D..1"..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 ...../...."#.D.:~2"..A....d.{v.^.G...d.W.:...P..k%.. A..Eo.....A..Eo.....s.....

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):	5.636096945146175
Encrypted:	false
SSDEEP:	12:V9zUQZ9PQIP9zTgLeZ9PQS99zHp4m9PQR9zrh9PQXKl:XzjZ9PQIFz0LeZ9PQezHWm9PQbzN9PQO
MD5:	8CE8725F4937D56D0AA6C7728AB0E22C
SHA1:	0151BB24548057F47CDA9F6DF11DE2778D00B2B5
SHA-256:	477DC2823D681E8C4D051D28B470629D19F737C08C8D48E898D38D0111E0B240
SHA-512:	C934D8B8F411FDABA909CDA6E02AD25EBB0C2842C4645770889E5BE289915EF80AE1A090369A3EB26859AF5687B6B9215FBB2BD60AFE4A62DD5AA82E9ABDB C08
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../...."#.D../"..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....>.....0\r..m.....,....._keyhttps://rna-r esource.acrobat.com/init.js ..kp.../...."#.D.g'1"..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....OV.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js . ..../...."#.D...1"..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....>Mi.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .D.../...."#.D..42"..A.1.x.'.v I..*|Z..o...+.4....0..A..Eo.....A..Eo.....C.I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.643654336098051
Encrypted:	false
SSDEEP:	24:tB4v4KSBqB4v4IRsRjSBSB4v45SB7/vB4v4bT0SB:nMFSBqMFR8SBCMySBVMYQSB
MD5:	CEE8CDDD727DD56C592320E74757D49A
SHA1:	5A37490B42B3024B2A16A7897FF8B831747A5C99
SHA-256:	FEF4E849F055AED637E5A039ECF7B998DD3ABB2091130D0634CC8E0E4C90205F
SHA-512:	D0F6E329DBBACC896B6F0F30A1CBA084CB44C2BBA64B54ADE583643C37E117FD85C97DDB989619BA47B97D93C5C0984C6F1A1D8197984BEDAAE563390FD93 89
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
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 ...../....."#.DB|./"..A..hvDO.N.t@....n.*..... ....A..Eo.....A..Eo.....m.Z.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..j..../....."#.D.I.1"..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....>.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ."...../....."#.D9..1"..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....S.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .u{..../....."#.D<.x2"..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....KP'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	464
Entropy (8bit):	5.650751799883201
Encrypted:	false
SSDEEP:	12:IbRkiDaXIEllIn34WusskbRkiD8IsXWuss:OpD8l/CpD8n
MD5:	30036709752631F0B5D2FA111BD3D890
SHA1:	6CF3B501E61A231299DBB5973639690176C6DA1E
SHA-256:	6CABDBE34E0CDEBC2308ED6ECDCE1ABCC66C4CB9F1870AAF8C9B500D2FAE3A13
SHA-512:	AA5BE2694F69216F681E41C985D5D3B0FCE53A5B38E6E509D77E41FC78832135ACB6FE5353ED7B094634D47B7CA08F1A690A7B80A457751D0D50301515EAB6D
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 ..r".../....."#.D../"..A..8 P..a...R..Y....7.@..2Dm{. .A..Eo.....A..Eo.....2.....0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...../....."# .D.I.2"..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....[.'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	420
Entropy (8bit):	5.588470026126778
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu/LznPVyh9PT41TK6tqf2+yiXYOFLvEWd7VIGXVuIVyhS:pyixRuJLbPV41TE8yixRuSV41TE
MD5:	9D6A8800D3F94BE14257ECF3A98E5119
SHA1:	2C1A7ADE8B3EFA7C697F7A42FFF6D2D380FCA4DC
SHA-256:	9D561317A3ECE636888925412DEE70DB75461071479940858AA019A9A4DE80EA
SHA-512:	ADCA1686274E2AFBD35DD81A3C9732E7DD55415DC40E137553685316798651FC711EE5CEB6A35CE5BD19926324827A73CE4EEE872C8F156F67D22F97004E42D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...../....."#.D...1"..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo..... {F.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..6..../....."#.D.|y2"..Ak.Q.....-_..y.....O...>..1....A..Eo..... .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.6456991708593165
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQfIhEkNLZIl6P41TK6thvYOFLvEWdhwjQ9gyyy4gNLZIl6P41Tj:0RhkhhBLZCRRhkGyGLZC9
MD5:	8CE1E797F0F09038B8D3E16E6F651E7C
SHA1:	32ECFC5CACB3AC2AE8AC8ACCF4FAEF27C1947138
SHA-256:	C416E9C76B188BDBC23D1EA91F1B7D03AAD5C3C201888036AD33AE95222DB8F5
SHA-512:	D86C9A719F3A2560CF3A2C19B1181D2ECCF9CB06118F7CD9DD281112CE63F49B01B7BCE4BE71D91EF21A29C5707BED443FCE6B9CA52431D235EBAB13A7E9D C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...~.../....."#.D..c1"..A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....G.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .o..../....."#.D..e2"..A.].>....uUf..N...k.....c..l.A.. Eo.....A..Eo.....S..M.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.606822441690248
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQ/mQla6g1TK6tG2JYOFLvEWdGQRQOdQOsPdXq96g1TK6tE:2RHRQCoa1NRHRQCRsNq912
MD5:	B92136FD0CEDB0BABB7FFEBBB3F7D43A
SHA1:	85F71A1F967F91AA999B5FB181AEB15592EEAAFB
SHA-256:	B713008D9BDE7D0FFEB4720A8A8400D4D73D14A468971DF32006F069B8D91D26
SHA-512:	1700F3F7B5B65170C225A52CB3A444E632AAA980DC070CE4426617D722BCC19C3E97BAC954B61049F754CAEC51CB11D94787422382FA8E987C7F3B0BDFB3E4D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .J...../....."#.D...1"..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....K.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..u..../....."#.D..x2"..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....*w[.....

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):	5.613492078966523
Encrypted:	false
SSDEEP:	12:Z5MAIMuR/EF5MqlLMuR/ELO5M7kMuR/EH5Ms6MuR/E:ZSAJuR/EFS3uR/ELOSZuR/EHSsTuR/E
MD5:	530926B1BB9207CC53E8A452AFC50506
SHA1:	E2E2AC16A70B4DAE71DBC95E303F3CB86548C884
SHA-256:	F39490D778416981A385463A4BFA9C4AC13BB668C5FA33A8EBC614A1FDCBE91F
SHA-512:	D5196A594B6367B1E186C16270D197F9E3E6D26DB6EBF663BA9FD7BD78922E0987BF61459944AD543B0980039342B9ECF422CF00815AAD2DD934DC1D6866296
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...../....."#.D.../"..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo....."..A.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..op.../....."#.D.}'1"..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....S.,.....0\r..m.....3....<lb..._keyhttps://rna-resource.acrobat.com/base_uris.js .:..../....."#.Dn.1"..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....7.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...../....."#.D'.42"..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....Y.....

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):	5.619127404676773
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuwMqinSm0bbsIDMGH41TK6t:XfRMvRKsIZE
MD5:	42AD0347302F4228381D4348590720BC
SHA1:	68518EF17CFB02B9F40DB6E60D22A06A8F9DB01C
SHA-256:	FDB2FECB8F8D5433B5DBF05DED1AB8A0BB300B55A126E95AA9443B232099540B
SHA-512:	C8422D697F20EF3ACC06D6A6D2EFFC9C5D0B4BC43B09028C419BFFBECE4BBF70825F5645EF548E509849ADA5079DB5BE92CEEA5861723FED93ACBEA58A1B952E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ..n..../....."#.D<..1"..A..`....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....DC.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.58498830328987
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuMzCVMby0zBUKSAA1TK6tf4fPYOFLvEWdtuN4PxMby0zBUKSAAI:pRfuSbeyRs4P+besH
MD5:	0B42AF2F9705B09F3A71DCD239B3D669
SHA1:	8C6966A3EE212FAFE268A23E5BF0D82782DE5300
SHA-256:	ADFE1EA2707CF16108E6A938EDC2BB3DB581982058C0ADB820F4EABF2FE2D0CC

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
SHA-512:	2C6469446AEC6205D124B0DAAFD3987CF761D65C5BF6EB31D3795F574C2684CBCB87503714B889BAB323FC53E0F51FD35FF1ED690E69563FB5E3E22F7B4A1E5
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...../....."#.D.'.1"..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....[.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .[...../....."#.D.x2"..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....L.....

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):	5.59789842914692
Encrypted:	false
SSDEEP:	12:KkXxKMSCvbBxIvtUlRkXxKMSCv8vtUlqkXxKMSCvykFvtUlPkXxKMSCvUvtUl:KkXxiC1xIvWRkXxiC0vWqkXxiCKSvWPS
MD5:	EA536E1180C0A2DC9449F2F4C698A058
SHA1:	DB1F406FF9E9A2292293DF5734DDD25BC46981FE
SHA-256:	4A7EE966E80C16B26553CA3D8EB7D3B630043EEC71A403EBD252987CF80A410D
SHA-512:	3F228ABEAFE79E9D9F5D33DD82ADD581ED34589C5CAB3FFFC471B90D75DAB3E32E94A1427E4E1139F022B0FC5B9947DADA2C7583427BB5883B262F21B93A74A8
Malicious:	false
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ...../....."#.D.../"..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....I.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ..np.../....."#.D.v'1"..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....dl@.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .I..../....."#.D0.1"..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 ...../....."#.D..42"..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....q{.....

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):	5.643706273682197
Encrypted:	false
SSDEEP:	12:5h6OL8KZkch6OLq5koBh6OL/Zkah6OL7X5k:5h6t9ch6nW2h6zah6X
MD5:	9869BB19A69BA039D101978A8E3619B9
SHA1:	34C5D2D26D995EB241A1E2637A6F7EF2ABAB2E29
SHA-256:	13905BE5619D1805893798C4BE2F4659968B4003016C9DDE09FF378B1E661361
SHA-512:	F1C8003373C4DCBF866FABE49606BA78F3AB450B71FA933A77F6403A8C0F386B01C940B40F9054DD655AA2FCFDE28F19C8F6C8743D8DF076E7D49ECAB0C5B48
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .H...../....."#.D.A./"..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....bD.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...{.../....."#.D..U1"..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....5.j.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...../....."#.D.'.1"..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....9.6.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..%.../....."#.DCYY2"..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....Og.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.659718151735316
Encrypted:	false
SSDEEP:	24:UB4v4fwzXLnbB4v4twzXLnZB4v4pwzXLnUB4v4JkwzXLnL:8MJbnFMPbnjMDbn8MWbn
MD5:	8F993A9CF02382F6F6436DB96F9B42A5
SHA1:	581F80AA5068276203A4372852E6FB5F82D2DD2C
SHA-256:	105121813521DB63EEC0516463C0E6A39920C26497B2F1A6E3F7E94AF69DEAE7
SHA-512:	A022A515F6C176FA06E068DF121BDDA7B07B405DE6A5ABDA3A8C3BDB8C6AA1C2A9E38098DB9AB077F47056A414CD8D0A77C408C6E250A1888E4F59E514B3BDD
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..<.../....."#.D5../"..A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....!;g.....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 ...../....."#.D.1"..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 .QC.../....."#.D.x.1"..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....!.t.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .T8.../....."#.D5.|2"..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):	5.569278151349627
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQR7XpNz5GFCaa+41TK6ts/:NRMHd6DpNz5Gda+Eq
MD5:	D88363CC76F7D74FC1894A7FF213364A
SHA1:	98615DC6EF39B3DCEC197E92A27D19F0B05EFF8F
SHA-256:	8CF5F63BC3B8FC3466E3B9080C9D23622F802368F4837D1A5CCD2D8C95FC7EB3
SHA-512:	E280F1BF7CF4B0978686800F6DBF0C7D25F0CF0E2C0281555B5A24DDE9C8EFBEAC4BAB03B366F5A3362BD7B28233D0225A750DDE02FEA91751FC11149DDA93D
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ...../....."#.D. .1"..A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....p..6.....

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):	5.5877249047419015
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXudl4511TK6tVjvs2VYOFLvEWdvBIEGdeXuissll8zP15:BsR2EseUQjjUsR2EseZk
MD5:	22FAC3773B4350402E77FF7618F63F5F
SHA1:	B8C4E907BF74DDDFF5F1349A36A0209CB6D0CB0C
SHA-256:	072D3593DE8A86EB9EE620F5A39FCFCCEBEBA2A1744B34288337210C974929D8
SHA-512:	5893EEDEDB7ACEE23D22BA28B1FD75F0C2843F6F7575C720B142F72B60A3CEEF48A58BC6097D07590354CCA44DF49E256C4EB9C932EBC218EC896FF1D8BB2C9
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..?..../....."#.D.C.1"..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....S.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...../....."#.D..x2"..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....Z?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):	5.67904912162304
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ3EkH64B7OhKlvA1TK6tIaVYOFLvEWdwAPCQD/gyLu4B7OhKe:RbR16UEY64BJktbR16CgX4BJk
MD5:	D4695E9BB1BF2B287FFDFAA60EBB4181
SHA1:	507ECEC99B0DB0A666D66C16F057914B0701E985
SHA-256:	6CF265470F15866E73716B4C9A99B05746F6760AA37B23029F9BA6BAEAECD86F
SHA-512:	A6CD7A70377C6A0085A4B060C31E332D45F02EA87AE4A9F36FC413FA08319929E35CC8E60C2094E44814CB70FB2AD211DCB6360CBF79EAF2C596A7972CF8B58D
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...~.../....."#.Db.c1"..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....l.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D..e2"..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....p.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.61571569947488
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuyVEQdFt1TK6tpYl2s2gEYOFLvEWdGQRQVux0rl86lgnQL:B2geRHRQfE0TYT2geRHRQPnl00
MD5:	2D5AE76EC7F0DE88D19DC34EF3CE871B
SHA1:	44FCFAC22E7E6B5461A1942A7BF88E8572BF1677
SHA-256:	5171924D36D37F6B2DF1F499A27303D144B68F56B2CB9B32DFD9AC15E8188DDF
SHA-512:	314741D077A2300A9E9A861DC026F006FBA0633A6B80421D12614F9850E0797C03FDFD70A3BB45962A20658A964EE2DEF68680356B04C08919D2FC14DA850851

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...../....."#.D4g.1"..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....4.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .>...../....."#.Dx.x2"..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	824
Entropy (8bit):	5.664963873046301
Encrypted:	false
SSDEEP:	12:WyeRldBit1wGyeRl0l3Ot1w/yeRlHat1wdJ0yeRlyUEt1w:WJ1YfwGJ0efw/JPafwdJ0JqNfw
MD5:	87E234E09E0AD148F18E76EA6D470A8D
SHA1:	1A5ECF72A32A54A4BF7882C7495449582F995FB6
SHA-256:	FFA7973FD48B09D2EA264C9553ED3E165255CF33867C4CF1F4D769A2D6842383
SHA-512:	521CEE552745A9B078B576E7F6154F01CA1CE363CD44F68887BA40C8C995070416277B2FCF46510DD8D5CC0575C64F6BC3BEDC2971F2176432536E4162037C33
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js . \..../....."#.D&../"..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo....Q.e.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...|.../....."#.D..[1"..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...../....."#.D...1"..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....]......0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...../....."#.D..^2"..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....cz.....

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):	5.580226187125152
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuX+oUrqwK+41TK6tnXMnYOFLvEWdhwyuqxJqrqwK+41TK6tbe:wRhO+lGwK+EURhZqGwK+EB
MD5:	BAF9E419AC2D11559DF2CF0D746BF912
SHA1:	E24D3685A7F8A5E86A9EF0F1AD38ACADFFF9770D
SHA-256:	B13742686F896B21EA64A5A474292616B5296803D22DF62F96E8400463D79FAB
SHA-512:	54A4A0F5A617D945FA0F995A42442580B9184DE25977C17EE0BA496DDE9A390B1B305C85C508F68B7D901EB14EF5F20FA57F4CFCAC4ECA86DD9041600E2F258
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .O>~.../....."#.D.Zc1"..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....{8.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..K..../....."#.D\<e2"..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	920
Entropy (8bit):	5.639950992808038
Encrypted:	false
SSDEEP:	12:/RrROk/8kfLEnmRrROk/Q5fLEaNRrROk/SfLEWVRrROk/9dgVpfLE:/PJ/8k4mPJ/q4aNPJ/S4WPJ/YVp4
MD5:	7CFF840A6B1C9B8BEF7B8CCC8BA805D0
SHA1:	639608D99CE91F550A9F4CA2104D0E0CD9A19F45
SHA-256:	D967873CE920C7FD721D704CAB2EF95D7F78C2DC624FD4E9846DFBCD846C9FCD
SHA-512:	3730B96DBD1D8DEBA7963B033F57A4B8DB947C28B22D659A4EB36A2962AC1814261A17E05949D57F3BE676EED65DBACBB0290CF48C3D66A363B0B8131C3176F
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..2..../....."#.D.../"..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....jW.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...|.../....."#.D..[1"..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....t{.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...../....."#.DQ..1"..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....W.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .o...../....."#.D.^2"..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....<..r.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Size (bytes):	744
Entropy (8bit):	5.640276699075347
Encrypted:	false
SSDEEP:	12:xqTLKCPLn+qTsCPLnDqTspjCPLnRqTTCPLnb:A3KMnRwMnGYtMngvMn
MD5:	86BEF0C79D8076548BC7EB0C6C4E44E7
SHA1:	C6758E03B1B1BE223A8C935CCD547EF935CC650D
SHA-256:	78C5C1FB7466540150A4FDBAA5C5AF00A7F439656C7BC8472A653700D72DD71F
SHA-512:	7981147497B4676CB13A9D18F4290911DF43D1D0575D0590ABA3E1482CD9D68DDB03C57CD58A56A62C0934A97D050CF30C8C7BBC554108E7D0823A7F6BE8CA
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .p...../...."#.D.9./"..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....G:5.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .C.{.../...."#.D..U1"..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Z.M.....0\r..m.....:....f....._key https://rna-resource.acrobat.com/static/js/config.js .r..../...."#.DX..1"..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....<.....0\r..m.....:....f....._keyhttps://rna-res ource.acrobat.com/static/js/config.js ...../...."#.D.RY2"..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Xa.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	828
Entropy (8bit):	5.628180105966192
Encrypted:	false
SSDEEP:	12:zRMxMsDJcRM0lODIsD5RM1JIsDjBBRMKlzyZsD:zenDJc7l27D507DjXjeGD
MD5:	DC66CD5245C2E63C16A4BC27072EAFB7
SHA1:	C92B5128FDC808F2BB38682ACD4DE1779BDBAE9D
SHA-256:	125E05421DF42A1488066D5A4AF3B1AA18EC0D9CCA3876779722F1C70E0BD864
SHA-512:	CD6A8135E80F2A0A968FF4223A82CF9181EFA2E530B2581FF3CE65951FAD221AB21B620C81756A82F2585EFB38416EE57061C30005F2E0E53DAB0F8A3173A9C3
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../...."#.D.F./"..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....z..... ....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .'J..../...."#.DA}.1"..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 .i...../...."#.DsL.1"..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.... ....X.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../...."#.D&.x2"..A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo....._..P.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	840
Entropy (8bit):	5.640850462086998
Encrypted:	false
SSDEEP:	12:6lJRVSTFoMdlUlJRWlFoM6ClJRIFoMHqlJRWSFoM:Y7STFoMnyslFoM6w+FoMHo4SFoM
MD5:	21C782D8F3EE08AB70AC69F700ED2B4A
SHA1:	272E62B92EA002DC2E13EB5F98B206A8F236A6F1
SHA-256:	252B902878B49D622691D4D7AC362D3461126D3D7C3D703293219C042AAAFC6A
SHA-512:	FD4B14F36B91026F88275F804FD725F31C23EA5A99EC504714E065CE579B2D30C5880AB773C6CD89ABECEA0BDC4DFA7390B598555EAC45D1E6AEAAB72934E6 01
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../...."#.D.a./"..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo .....%_.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..K..../...."#.Dd..1"..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..... .....A..Eo.....f~.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../...."#.D.i.1"..Ac}.H7M=M..-.....Ix..R.l. ..}Rl.$q.A..Eo.....A..Eo.....]..... .0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .f...../...."#.D..y2"..Ac}.H7M=M..- .....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	892
Entropy (8bit):	5.652789226758764
Encrypted:	false
SSDEEP:	12:F8hRrROk/dve2c8hRrROk/Jwve228hRrROk/wyITe2h8hRrROk/zde2TR:UPJ/Y29PJ/n2LPJ/wyp2IPJ/s2T
MD5:	6881DF9A059DCFB9379D86C1C0B704F3
SHA1:	8BD646111747D67B1EDE6EC0ECBAA7E9707B903F
SHA-256:	1D04D56EB8C3CDA88F350C38142A9EE299B29279E2D62D5CE257D7C23A405C98
SHA-512:	FEAC4AD9DA608B57268E1535268C7A2BE63F041700548F63A951A3D940DAE14486B86B7C01FF8F2E97BA50D0432353D9D1A2507C69263B2A9A9A0C719CBE6EC
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .@'..../....."#.D.../"..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....%.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..|.../....."#.D..[1"..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....wb.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..}..../....."#.D.m.1"..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 ...../....."#.D.P^2"..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....gC.....

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):	5.7313042796456415
Encrypted:	false
SSDEEP:	12:ehRc+vrNJICLuhRcq+lrNJICghRcerNJICThRcM/IV/qrNJIC:ehLJICahhKJICghBJICThfAVGJIC
MD5:	6E5F544AEC80349B35552ADD4F1E54E8
SHA1:	49F913FCC53C6E447627F47EB4B2D8AE3E0D94B0
SHA-256:	2D02479FA60FB71F2A0B238C997BF21D4F72E0FB41AFCF098A00D8569F20B163
SHA-512:	D1A38E2A547FC904EBCBB7F9BE4E0DB473F8F6E5C5FD3938F766D3C53D4FD2A99962AF664EEC8386DE03C72A86C2075321D3346EB45F2B7F38BAF79C042490 1
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..]..../....."#.D|../"..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....}.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...|.../....."#.D,+\1"..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....&.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...../....."#.D...1"..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...../....."#.D..^2"..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....d.....

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):	5.60778349941718
Encrypted:	false
SSDEEP:	12:0RYZRe5SR+dvZRedRGV7ZRemRC3ScZReJx:0z5SBdkIm4ihJ
MD5:	0F5BE3D1A3D466838312BEB4AEDAFF9B
SHA1:	E0355515F8B847B3DBFFE3E89B7F5D620B0DA290
SHA-256:	F3D30385A7FCD6FAD950EF9C25BFB7B75FF3B85A38C13747FB416F67DD1EC324
SHA-512:	E3177F73FE3494B4525F00ED21442625F42F50938DC236C26C3223413F7CF2273A65550E193EA56FCB06B077763A0546ED6A2FC8ACEC06DE0C9EDB61F833F134
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...../....."#.D!v./"..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....m."......0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...|.../....."#.D.[[1"..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 .@g..../....."#.D...1"..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....e8d3.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...../....."#.D..]2"..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....2v.E.....

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):	5.663979337398742
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KFqzhkx56uvp1TK6tgtMAElVYOFLvEW1KBE/+Lkx56uvp1TK6t2:6JJKFsKWiJJKBEmEDJJKdBfJJKB/M95
MD5:	3A739770BFED78F46A25B9DF3C8502AC
SHA1:	919A893D8A62A88967BE69B41537E4656D8261D4
SHA-256:	BEA93D55664CED9DCDAD64894462290A90C99E9163802A4079DFAC94B29FE661
SHA-512:	17AECA3F9135A42F465020F03C02946A06E86E85863EA8907C47E93A915B2651D1E36177945574AE4AEFB9479A0D7DF1A61FDBDE2E3B352499DCEFC383333BD
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D.J./"..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....=v.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...r.../....."#.DY.:1"..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....6.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.DxF.1"..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo..... |.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .x...../....."#.D..E2"..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....\'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.68980633839902
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu3nF7fJl3yhUDLYtmOZn1TK6tXXMWYOFLvEWdBJvvunll6yhUS:xRBJ0nFb3HDcFZLBjRBJ06HDcFZL
MD5:	AB8750B8B0207E2D9C1F2086D791EA59
SHA1:	A3F02F6A11272DE1607A4E73B77A9EE299439863
SHA-256:	3F58205EB2AC0DF6C7FCB7A5462E1E956A52B4E317F729F96AD309C20FD3CA2A
SHA-512:	841E504633F7FEEC85B49AE25B2B118646390A2DE2292C1212135972E08B34F27FDF900F3A803F401F29C240B732054EA17F056B3ECB8766A3A36C2B0B2D3BC2
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .8B..../....."#.D.\.1"..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....o..Y.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...../....."#.D!.w2"..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....*s.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	844
Entropy (8bit):	5.622556127151154
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7VI7VPu1TK6tOesRPYOFLvEWIa7zp7iSVPu1TK6tOsRPYOFS:BPHTI7c4ZPHwScTPHPczQPHFQzc
MD5:	DDD21597EFE5FE0151BF3D2F92F3EF01
SHA1:	2D3F7BF1F205D3ADF2277CE1CE3E21813371AF97
SHA-256:	7E2955FA5A1168CCC6965427C763BB06C5B1072C1FDFDDE7A9823E9726DF4C14
SHA-512:	564488405D42B1BE729B8B6D9AA819F78A655300A761EDAB81C4B30A63B9F092982C3E23B45628FB048A4E5F54E08C6B21A4B785B43244A7B76AAF5F0FF84019
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D../"..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....Av.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..{p.../....."#.D.'1"..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....-..H.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D...1"..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....k.1K.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D.+52"..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....u.....

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):	5.622098070971428
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QXUmsMwiM3Y1TK6tf8KPYOFLvEWdENU9Qtpj9kiwiM3Y1TK6t:bJRT9+Hqr0RxJRT9okdr0
MD5:	40BC4CB242D843724416ECE0B307EF49
SHA1:	70C851EE6AC0FF3F5689388702532D355083D691
SHA-256:	B9C116AB8E22ECEB8F331774E9B70C2D42A36F919C88370519337ECD3D724842
SHA-512:	D797E3BEEE3F9059D93B125EBB951D2367354DE066E26213065CB7133D683EBBCE3EEF689DD8EE8FA087CF1E82A0469EB35D1953E4E1B5EDD6321D600D0645 7
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...~.../....."#.D..e1"..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....j.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .]...../....."#.D..j2"..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.642302415474469
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQAIjBRCh/41TK6tvFEQt6EYOFLvEWdccAHQ0brG2jBRCh/t:XRc9iDi/Eh/Rc95PHDi/EI
MD5:	A26364CD065612EF1608F7A6C5A4A4FE
SHA1:	F36636C88928625CFE0C638F906DE30A21D990A6
SHA-256:	E13AACAA2D913CF42F0C34378070F9000A6A993750E2C89692A83B7E7B3B467F
SHA-512:	3F4B6FFFB42D62413448582C2298AF559702A3CFF2EC529215B1FDE756EE736345ADF40D735D4CB2739638568A168DE73B502ADF649BD0A4AD56FAD414F29E2
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...../....."#.Dl..1"..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....z%.b.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..D..../....."#.Dy].2"..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....}

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.616931930745893
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhupPVULlF4r1TK6tRMqs6XYOFLvEWdFCi5mhu2+YAHVUL+:bs6xRkif2LlF4n9s6xRkiA+V2LlF4n
MD5:	BDE45F7B4098BFDC2CB82501C06935DB
SHA1:	E0475A4CB2BC60212044FBEA534F71ED851E8D7D
SHA-256:	E655212562C98A2EA54720B6371E7571834C8668D26F69B6683C2621A94EBE0A
SHA-512:	179F891CA25E5D2351B4EC7CF3D830D8553E0AE32F457ABB0EA73068481683B4362C480507A9299959FA142E8DF1D914B48A11A15B0ABD60036D683740AAFD73
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...../....."#.D.../"..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....s.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .Y...../....."#.D...1".A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....N8w.....

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):	5.573958237693296
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuKUDN941TK6tFMhYOFLvEWd/aFuPbKsN941TK6tK:WRfN9E/YR9hN9E4
MD5:	BC96E52E7653E848BDA2456691AE499C
SHA1:	96BFABF373838F69E8B38E360F25129F4CB9354D
SHA-256:	8196EE45795A171407C18B23E497B2D5E43322E70A68E42CE800AE07EA41740A
SHA-512:	62C6C761C6A8D281B4948B19C3418996B90FE58D85DE9C623A9ECF9C5818C9A4A021D4363AB304340A1C5F2B452728D17719CEC1A8F8C8A09FE6343108BCE22
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...../....."#.D.2.1"..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...../....."#.D`.x2"..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....(.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.589528745785088
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQDaEAXoBMqVd3G4K41TK6tJ+R9YOFLvEWd7VIGXOdQfD6c:2DRuRTE5B9Vd2kzuDRuRo65pB9Vd2kk
MD5:	A931706ABE3C3D017342FB389E185CA9
SHA1:	F350B077E148D740D72BEBEECE7AAB7B57ED0FE5
SHA-256:	BBC8E5D43307A136245B41B4F85B63B91370126C97F62724772DDBB462DD4CF7
SHA-512:	945DAFDD03F362BC49950F2921028EB7FFDEE0550E55E3B174AC864C3AD8FC060F9F16CABE4E675FADEA090D9A22ECAECD52F266CF714CF7154EB76EBF255 20
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .K..../....."#.D...1"..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....`.....0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...../....."#.D.\x2"..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....a._.....

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):	832
Entropy (8bit):	5.643676850295822
Encrypted:	false
SSDEEP:	12:+RQlELrnlRQTFNcrnuRQ7rnG2RQAhrnN:+uqnloNAnuCnG2BVn

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
MD5:	F3EB9F1FE1FC4C70C715DDCEB1F700AF
SHA1:	527B6724BA024CA1D8DA0B07215BD303C5ED25BA
SHA-256:	E4DAEB260635F16E3E17AD15B5BC5BD15D8C193C213F792DE8E967403B7171C9
SHA-512:	7A9EF4B3C06ABFF79F81AE8699F9A778C45086EE53248238F9AD9360B5F89FF8BF31A149AF02FDE3EDC6064F952036CD0E1F7339B591568FC33F3C6D0080D900
Malicious:	false
Preview:	0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .!...../....."#.D.../"..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... ....t.~.....0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...../....."#.D=..1"..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....h.t.....0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ."...../....."#.D.Y.1"..A#..@..k(v.8g..5.~_....]Pj.*..6.A.. Eo.....A..Eo.....0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...../....."#.D...2"..A#..@..k(v.8g..5.~_.. ..]Pj.*..6.A..Eo.....A..Eo.....H.IN.....

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):	5.585615048509062
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuX4AyC8n1TK6txoXXYOFLvEWdENUAujpAyC8n1TK6tq:xhRTuA7QchRTrA7Q
MD5:	47E5FAC3A1484EBADFA9482AB5689F56
SHA1:	52FE14F5E7FCEB39C39F4968AB855D4E13F82BD2
SHA-256:	3AFE72FFC0016A9B59AB3CDA182C23C4A2495ECCDC2560E76A94E5A0D511CCC4
SHA-512:	0C277CB9E847975B98869EB28A3D7FAA58BCF74F18970A63D75746D24FBECFF1CA9E6051D726874716EF26B9FBDD473F94873D79991AF28033239EAE5BB5525C
Malicious:	false
Preview:	0\r..m......R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .y<~.../....."#.DNFc1"..A8.../...;.\\o....1.....+..A..Eo.....A..Eo .....p>.....0\r..m......R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..I..../....."#.D.(e2"..A8.../...;.\\o....1.....+..A..Eo..... ...A..Eo.....3..@.....

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):	5.643771410501772
Encrypted:	false
SSDEEP:	12:nRrROk/VoUHKHKmWRrROk/VuVm4fRrROk/VK9VmRRrROk/VzbmG:nPJ/iUHKHbWPJ/Z4PJ/xRPJ/gG
MD5:	787F2A40CA20CE1027A4B3372239C845
SHA1:	3D6F395D619491BFC61180D52967D2A1A7E6AAEA
SHA-256:	1BF13A75CF7A4AAEEA3FD890139C5446EC78A183BD485185BD00F70245448CEE
SHA-512:	8C9598EA5777599B81996C735FAD45EFD5E231FC107F9730BD7086766BA37A9F40E505F6F3778932C6444D09D609A5C2F4A9A0811B0DD4F5A78EFF347611147B
Malicious:	false
Preview:	0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..v..../....."#.DT../"..A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... ....A..Eo.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...|.../....."#.D.r\1"..A ./.ev.....N~..6.b.....$.j; :C...A..Eo.....A..Eo.....L.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...../....."#.D...1"..A ./.ev.. ....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .v...../.... ."#.D.._2"..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....IM.....

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):	5.594527108403568
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuqMtVAdm9741TK6tTMZ/lXYOFLvEWdccAWuR8S5oxAdm973:qxRc/LAdu7EZgxRcz8S5oAdu7EO
MD5:	1B791B9E44C0B2BE020DACEF987A461C
SHA1:	361A598F259052B23C792A08E96F40F4CB73140D
SHA-256:	6B2062CFB84DB59084499C7B85409614FCC1800DFC259DB4340FB0F6C36286CC
SHA-512:	71B41B001FE70C2D64C7B6CF4F858A2081BF8EFB4BE65A1359A27E42991912F9512B267B44CC861FA53DCBCF636720CE42237513FB711927626E8C550C907434
Malicious:	false
Preview:	0\r..m......R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..g..../....."#.D.:.1"..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....r.....0\r..m......R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...../....."#.D..x2"..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo..... .....A..Eo.....x^.D.....

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):	5.5808239053470645
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuC14Jn1TK6tdMOYOFLvEWdwAPVutHPoAXvkJn1TK6t:2R1N1eL/R14liL
MD5:	C53F8B49D745730C04B6A262CB8FBAAD
SHA1:	2F0C6B48BB1ED3C58C6093EA757D2799DCCB6873
SHA-256:	885FE70000A814B52C45C72B81D6F500C6829B75A68D39E0CB75F2016FC9181A
SHA-512:	5885F416B063BD399179487971113C276A07B379360CD489E53AEBA5C7AF7875C35E209E6BC1C7D52CF5136F076535A6D5529B41DD008ED0E0F0A80F99AC996F
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...~.../....."#.D}.b1"..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ..N.I.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..H..../....."#.D..e2"..A.....k....F..D..O.n;[.1m.....=..A..Eo..... ...A..Eo.....r).....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.686143235991228
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQilbzhcsBXIh1TK6tM+3PXYOFLvEWdBJvYQfL3zhcsBXIh1W:mxRBJQvbDB0DxRBJQE3DB0Y
MD5:	A3BED303451C0698760F309BD830C2DE
SHA1:	01DB9099D27723A0BBE724869EEE6992D8930AF7
SHA-256:	527AA7B289063C2F000E5A491C050BA6919342179EB3E1D9AF408C7832139A55
SHA-512:	769B10037609AF8456DE03DCAF157A24BCCE3DC05BD6EA0F6C67A2FEC6B09065FD54B6AB82CE432AC539C5FDCD5485ACFEB4467B4FD81AF1EF55600616F47 52
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..D..../....."#.D...1"..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....2:. .....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...../....."#.D&8y2"..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.649378963905756
Encrypted:	false
SSDEEP:	12:3RrROk/sAHczRrROk/suNJHcWRrROk/s3yHcqRrROk/sKVw7cHc:3PJ/v8zPJ/jb8WPJ/My8qPJ/3Vww8
MD5:	380C2023549A936145C657644FF28626
SHA1:	5F881B5F58C8C942949BBF67DD4687D5CB1DE9F9
SHA-256:	EA714C3C0D730F21419778BA9EC7933C457C3035766504EDC1CCD4BF3194473F
SHA-512:	0BBE4E9A496F24F5DEE199670E7A0955975C9FD21C36ADE168805A0F47746FBF301207D16AE7BFC8F9537C780A5F45EC553739B7B3DD81188801418806D06B11
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .:...../....."#.Dm../"..A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....6T.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .e.|.../....."#.D.\1"..A.....9 Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....i.|.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...../....."#.D...1"..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-conne ctor-files-select/js/plugin.js ...../....."#.DTq_2"..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
Size (bytes):	2064
Entropy (8bit):	5.30090914016381
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPzuvpL8XMva/GDT7/hfEDPoHUsl:h1zZ4+dsp6Ouv2Efm9E
MD5:	E5BFE51979BE655EACB216C7762441B9
SHA1:	61FD0E9B3674286D4451FD6CEC63F74400C24547
SHA-256:	D3486C7FF3EC17A848C76A67261AA6971B8FFA1BF23F7FC0BC85F6C3A59C342D

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
SHA-512:	D27A8A76D62A0B93B0BBF5CD9AD653FD2D033940FA1DCDE1E01A6F4A76DEABCA675A0BC4834ECEA9C44DF860B57802AFE9176F4B1B411DB3558D89AE66DD3C8
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.....Xoy 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):	5.226042285938778
Encrypted:	false
SSDEEP:	6:mN9ci+i+q2PWXp+N2nKuAl9OmbnIFUtpe9cicZmwPe9ciXVkwOWXp+N2nKuAl9Oe:af+vaHAahFUtpKa/PKRV5fHAaSJ
MD5:	344ABD26E277C55CE57A2B42503EECE3
SHA1:	C3E77BF6D6E95997287F704EA28B39679430AC26
SHA-256:	C558E071C89034D6AFA49C6F5C7FC7BB48279F29BA36B6CEC725C096E4EDF325
SHA-512:	6A50225D753F2ED3AFA56387FF25C668A1195B1D26BF4EC0A6CF45E41C48EEBE0CE6D116839B70545C632D8E96F1A04CC94498B9F3E296948493068714BCF1F5
Malicious:	false
Preview:	2021/02/25-21:35:59.377 159c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/25-21:35:59.378 159c Recovering log #3.2021/02/25-21:35:59.379 159c Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	0.009659826032596219
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDgsMiDgsMiDdsMhCDOsMhCDo+sMhCDo+sMhCDo+sMhCDo+sW:trrCXonononononono
MD5:	21243F04C89A197BB6B7F6F83FC3143C
SHA1:	86C39801641D4689AF8792AFB690A0CADBE81263
SHA-256:	B71EB44A7471A903DEFF3A492C2981A68BFB32AB60A5D162E43364864DE135A3
SHA-512:	F36B2C48C1F0C30494202D6990352BF864F6D0EF073D8981C8033ECEDE9A0B55F90B422110C91DF95B7E714B5F7F1928FA75A64BFC2A9723234A7073AC945316
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2102260535547-203.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.343231782657978
Encrypted:	false
SSDEEP:	96:gM5f8EWNfjMI4G5fMMg0gDAL1cpemaMMMRl3rBSQi1NCtMLWYDv:9UE831lpdNmr
MD5:	0CF0DA4B7C32C2D1A770F91CEAC9B4AC
SHA1:	BF1E0BB7A1AC16723B6A9D9B5298A80196BE8055
SHA-256:	5EB4303CF0AEC6019FC2753C83EA781E5376155DABA4F67262EF54117DD802C7
SHA-512:	B7D741448BD9697EBF27C6F224672FEACC2B36C97AF86A3756E6EF2921CBB605664A58691696898D6DBDF08AFF2D5B87FAE535A01F7CB6C9E7795D8AC684E42
Malicious:	false
Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Category:	modified
Size (bytes):	32768
Entropy (8bit):	3.386929534603047
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQiOhFVCsL49IVXEBodRBkRHiOhAVCs749IVXEBodRBklHiOhN1:iGedRBmedRBcedRBTedRBR
MD5:	95B5209605E9D36F615AE5DACD58CB06
SHA1:	C2A55182751F252CA008C3B33A9619CD7937FEB8
SHA-256:	257813419740679170DBD8651FA14D723160D083D984522D7FDF778B404AA3E2
SHA-512:	B010706FF285E7273D24112CA08E752B56B79998EE7BB64F1EC7D0CC3F39F86E63206958629A093699C6F504F911DD870A4BD762929FFFB5A162676557570939
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):	3.200978674747074
Encrypted:	false
SSDEEP:	96:a7OhFVCPs949IVXEBodRBkHiOhFVCsLLR49IVXEBodRBk+HiOhAVCspd49IVXEBR:aAiedRBkLGedRBWCedRBjyedRBU
MD5:	0C6C6A6CA2FFC71E6D8BE21BAD7696D7
SHA1:	313C27A1608D9B4CEC493448FE35F4A4C7631889
SHA-256:	46686450248FD211972D60C77CE472073B6CB803109D35D991ADAB8265D20E6C
SHA-512:	987760CF0D2D1885983027EDF912E7305864195995383DF0EF6360BD10E5F4FB3CF0E85F1CD23BEBC9F9162697B3AA4404317F772C454807C71F19F493EC67A4
Malicious:	false
Preview:	.....*.....X... h...y.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6040	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

Static File Info

General

File type:	PDF document, version 1.3
Entropy (8bit):	6.860672979041864
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	CTR00068CP1PDF.PDF
File size:	46522

General

MD5:	e224bcfaa02a8881bb45969ad2c19f41
SHA1:	599a043fa6f27fe9353757c59dfc9ffa8ff6a1d3
SHA256:	2db74b42a9f74422079f9a16ca8bc3a1eb89a2704e3ffdda1c41761b9889395d
SHA512:	c76d37197877612bf0fb97b7f545a552510e6408efa7b2e11c952578abde0a5e24a45d28cbc1e7a2bbc8585e9994bbaea8c6d3f09663d946b588d3b5e27f7e59
SSDEEP:	768:xedfcgnZoIz4oTyWaa+k53RB/foW0dljxRR4TIpZMnZyYwHyTHGaFV8pGiLRQ/UI:x7s5haa+S61lTPEYat7sigu
File Content Preview:	%PDF-1.3..%.....%RSTXPDF3 Parameters: DRSTXh..20 obj..<<../Filter 3 0 R../Length 4 0 R..>>..stream..x.....Z..o..|....&u.... ..b.....)../..\.....'..A..?..J...._..=..S....!.$*z.....).$6;...\....."%,AF$37.....d.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.3
Total Entropy:	6.860673
Total Bytes:	46522
Stream Entropy:	7.196278
Stream Bytes:	35616
Entropy outside Streams:	4.753126
Bytes outside Streams:	10906
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	36
endobj	36
stream	5
endstream	5
xref	1
trailer	1
startxref	1
/Page	1
/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

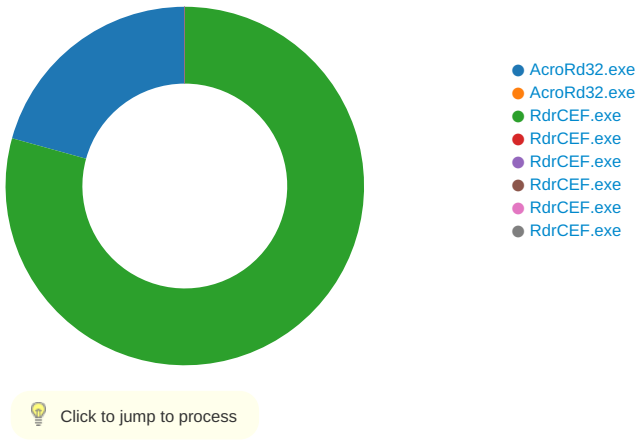
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:35:39.482872963 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:39.531935930 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:40.036221027 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:40.087760925 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:41.280827045 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:41.333540916 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:42.322175980 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:42.374218941 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:43.254157066 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:43.304792881 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:44.526072979 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:44.574549913 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:45.530030012 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:45.581530094 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:46.982670069 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:47.045697927 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:48.150085926 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:48.198791981 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:49.009336948 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:49.058825016 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:50.156282902 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:50.209465027 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:51.063862085 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:51.122073889 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:53.706675053 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:53.755479097 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:56.242297888 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:56.293984890 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 21:35:57.981988907 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:35:58.030746937 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:01.909538031 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:01.914163113 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:01.961561918 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:01.976659060 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:02.907725096 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:02.924577951 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:02.967669964 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:02.983696938 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:03.347894907 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:03.399285078 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:03.914252043 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:03.914307117 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:03.967467070 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:03.973539114 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:05.963804007 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:05.966384888 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:06.021297932 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:06.023646116 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:09.291668892 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:09.340641975 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:09.967922926 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:09.968003988 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:10.017030954 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:10.020095110 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:10.184957981 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:10.233803988 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:11.451567888 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:11.500190973 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:13.219666958 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:13.268610954 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:25.024749041 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:25.086251020 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:35.720828056 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:35.770931959 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:36:36.326442957 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:36.376737118 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:49.210952044 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:49.259946108 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 21:36:52.941642046 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:36:53.003211021 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 21:37:24.247061968 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:37:24.301835060 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 21:37:24.726943016 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:37:24.780040026 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 21:37:26.527466059 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:37:26.604182005 CET	53	56579	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 672 Parent PID: 5820

General

Start time:	21:35:46
Start date:	25/02/2021
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\CTR00068CP1PDF.PDF'
Imagebase:	0x110000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1465C3	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	16AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6040	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	15EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock672.1.2010944208.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	192657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	15EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210226053554Z-203.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	15EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1D83C8	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	1D83C8	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	1D83C8	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	1D83C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1D83C8	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	1D83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rvvdd25_1on4cr8_4ns.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	15EA85	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	15EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1uahzpt_1on4cr9_4ns.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	15EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R146ankv_1on4cra_4ns.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	15EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1qy15j8_1on4crb_4ns.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	15EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R149mjok_1on4crc_4ns.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	15EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6040	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	19D405	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	15CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	15D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	15D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	15D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	11EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	11EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	11EA55	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	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/CTR00068CP1PDF.PDF	success or wait	1	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	CTR00068CP1PDF.PDF	success or wait	1	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	16DF69	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 43 54 52 30 30 30 36 38 43 50 31 50 44 46 2E 50 44 46 00	success or wait	1	16DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 35 32 31 33 35 35 34 2D 30 38 27 30 30 27 00	success or wait	1	16DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	46522	success or wait	1	16DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	16DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	16DF47	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	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	16DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	16DF69	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	16DF69	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	16DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6040 Parent PID: 672

General

Start time:	21:35:47
Start date:	25/02/2021
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\CTR00068CP1PDF.PDF'
Imagebase:	0x110000
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: 3288 Parent PID: 672

General

Start time:	21:35:53
Start date:	25/02/2021
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:	0x10c0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	11B59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	4	11C83E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	98	11C8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	217	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2179	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	7	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	8	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	24	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	4	11B59E2	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	11B59E2	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	11B59E2	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	53	11B59E2	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	11B59E2	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	59	11B59E2	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	11B59E2	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	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	88	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	56	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	60	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	11B59E2	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	18	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	20	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	240	11B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	286	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	11B59E2	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	264	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	49	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	196	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	31	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	169	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	11B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	8	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	11B59E2	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	11B59E2	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	13	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	11B59E2	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	11B59E2	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	326	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	32	11B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	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	11B59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	11C83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6152 Parent PID: 3288

General

Start time:	21:35:56
Start date:	25/02/2021
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=1700,144647073828735 7279,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3630556925514522147 --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=3630556925514522147 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10c0000
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: 6184 Parent PID: 3288

General

Start time:	21:35:57
Start date:	25/02/2021
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=1700,1446470738287357279,6939926539180054600,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8690066333002460602 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x10c0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6232 Parent PID: 3288

General

Start time:	21:35:59
Start date:	25/02/2021
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=1700,144647073828735 7279,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2706402308431694826 --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=2706402308431694826 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10c0000
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: 6372 Parent PID: 3288

General

Start time:	21:36:03

Start date:	25/02/2021
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=1700,144647073828735 7279,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10726678641985929267 --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=10726678641985929267 --renderer-client-id=5 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10c0000
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: 6600 Parent PID: 3288

General

Start time:	21:36:05
Start date:	25/02/2021
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=1700,144647073828735 7279,6939926539180054600,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14471897307288007299 --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=14471897307288007299 --renderer-client-id=6 --mojo-platform-channel-handle=2144 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x10c0000
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