ID: 392872
Sample Name:
doc13798320210419100501.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 23:12:18
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

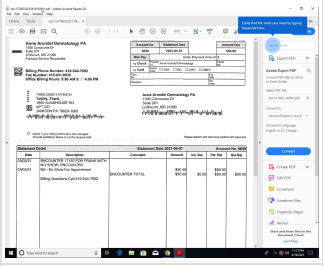
Analysis Report doc13798320210419100501.pdf

Overview

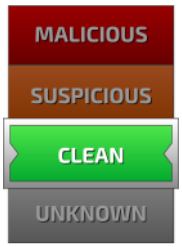
General Information

Sample Name:	doc13798320210419100501.pdf
Analysis ID:	392872
MD5:	3290102a424ad8..
SHA1:	906ed1cf70e333e.
SHA256:	f3cef618295d205..
Infos:	

Most interesting Screenshot:



Detection

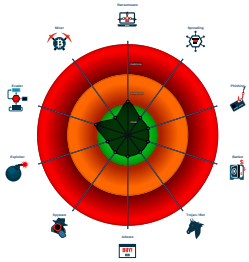


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

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

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 6404 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\doc13798320210419100501.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6476 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\doc13798320210419100501.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6708 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7044 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,1001149262048530690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12742373955121677917 --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=12742373955121677917 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7072 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,1001149262048530690,16326826708203091992,131072 --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=KAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8293892013758276365 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5444 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,1001149262048530690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14988028654324180745 --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=14988028654324180745 --renderer-client-id=4 --mojo-platform-channel-handle=1836 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4644 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,1001149262048530690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1643063119428019652 --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=1643063119428019652 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6164 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,1001149262048530690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16149447064209592232 --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=16149447064209592232 --renderer-client-id=6 --mojo-platform-channel-handle=2176 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

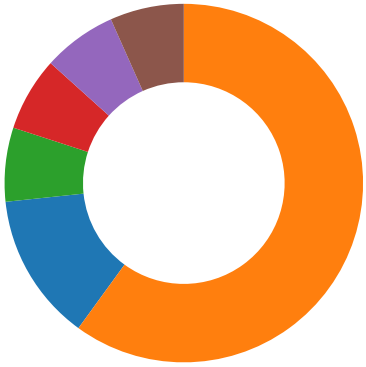
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

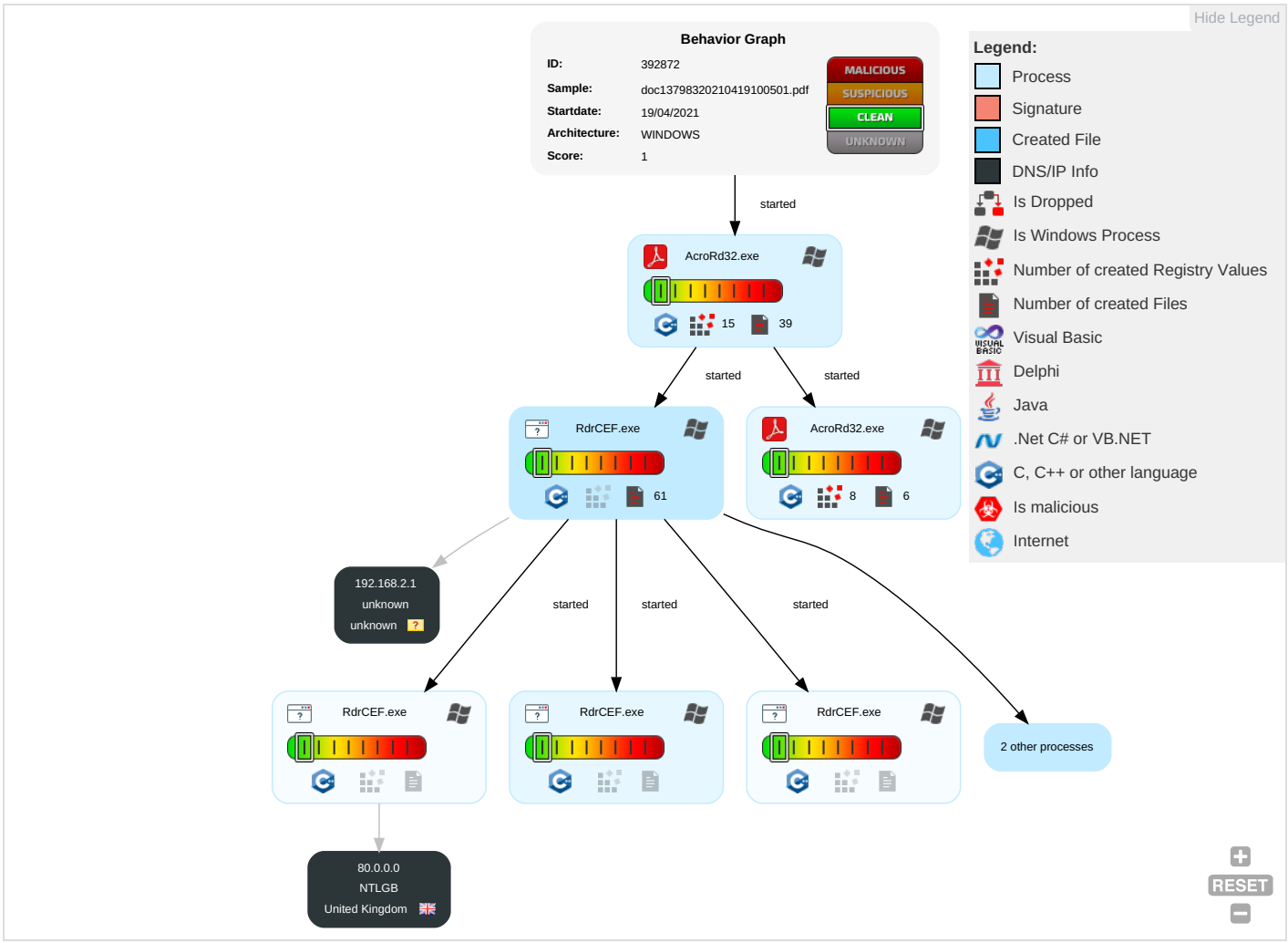
Click to jump to signature section

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

Mitre Att&ck Matrix

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

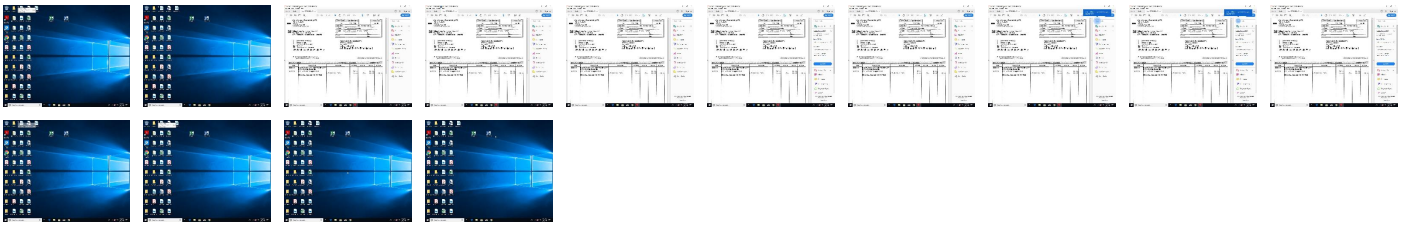
Behavior Graph

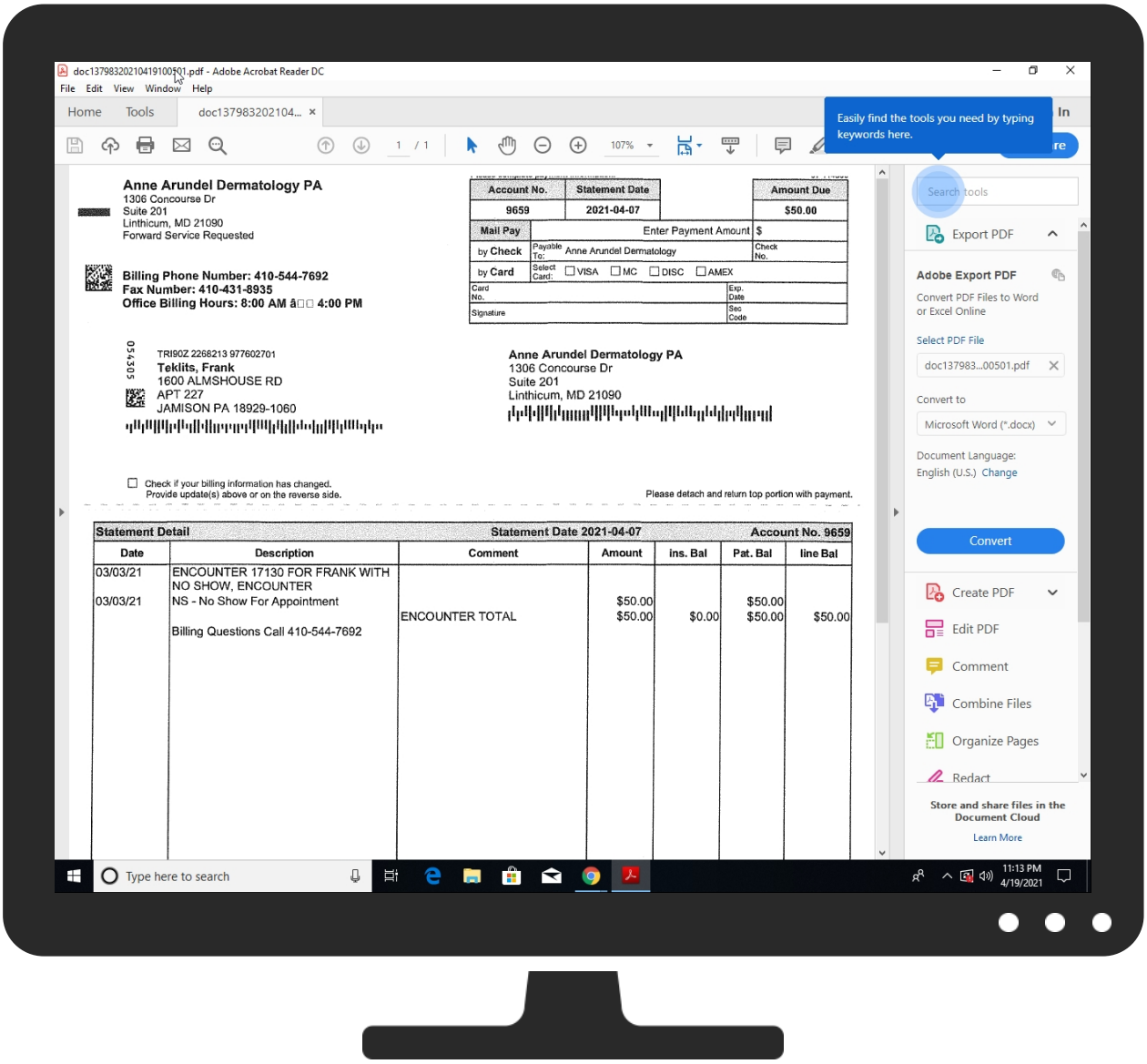


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://cipa.jp/exif/1.0/.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/.0/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/iO	0%	Avira URL Cloud	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://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/Upload/C	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/esbO	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://https://api.echosign.com6	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/U	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/F	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/I	0%	Avira URL Cloud	safe	
http://https://api.echosign.comgs	0%	URL Reputation	safe	
http://https://api.echosign.comgs	0%	URL Reputation	safe	
http://https://api.echosign.comgs	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/o	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://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/y	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/Q;cb	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

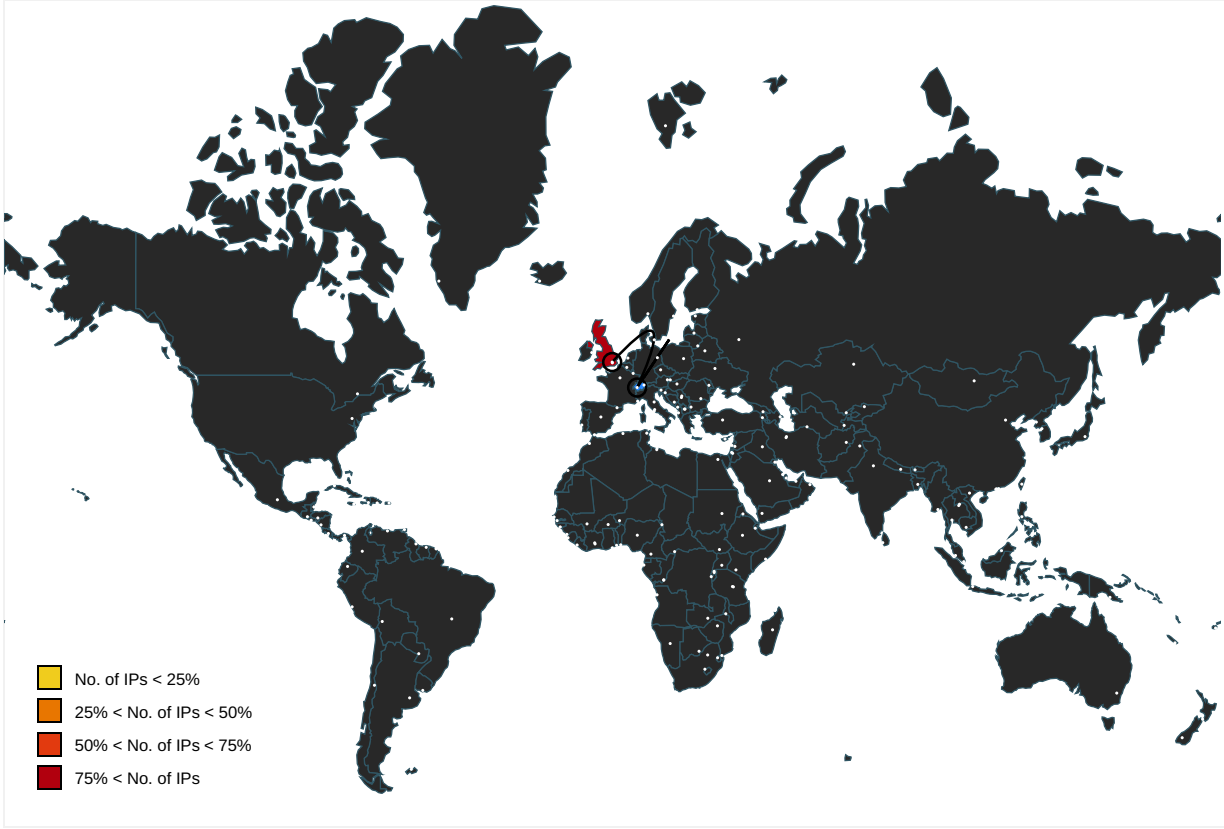
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://cipa.jp/exif/1.0/.0/	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/iO	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C	AcroRd32.exe, 00000001.00000002.380046642.0000000009977000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/field#j)	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/esbO	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://https://api.echosign.com6	AcroRd32.exe, 00000001.00000002.387981455.000000000BB51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.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, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.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, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/U	AcroRd32.exe, 00000001.00000002.380046642.0000000009977000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/F	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cipa.jp/exif/1.0/l	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comgs	AcroRd32.exe, 00000001.00000002.387687035.000000000B92F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/o	AcroRd32.exe, 00000001.00000002.380046642.0000000009977000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.387687035.000000000B92F000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.380046642.0000000009977000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#))Mr	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/y	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.388312297.000000000C9D9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.379828238.00000000097A0000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s	AcroRd32.exe, 00000001.00000002.387449717.000000000B79B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/Q;cb	AcroRd32.exe, 00000001.00000002.387423846.000000000B786000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.375393966.0000000007EC0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392872
Start date:	19.04.2021
Start time:	23:12:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc13798320210419100501.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:	32
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): 104.43.193.48, 52.255.188.83, 13.88.21.125, 23.211.6.115, 23.211.4.250, 23.32.238.129, 23.32.238.123, 52.147.198.201, 20.82.210.154, 23.57.80.111, 92.122.213.247, 92.122.213.194, 93.184.221.240, 51.103.5.159, 20.82.209.183, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.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, wu.azureedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, armmf.adobe.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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
23:13:13	API Interceptor	10x 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	123.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	EiK2ZuecHv.exe	Get hash	malicious	Browse	
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	HunpuKMHQt.exe	Get hash	malicious	Browse	
	JbQoNNPVOk.exe	Get hash	malicious	Browse	
	_vm583573758.htm	Get hash	malicious	Browse	
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	
	message_zdm.html	Get hash	malicious	Browse	
	0000001_Carved.pdf	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	fakeadmin.pdf	Get hash	malicious	Browse	
	x4F1uS8nAq.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	J76uxxiy.exe	Get hash	malicious	Browse	• 86.18.99.199
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	EiK2ZuecHv.exe	Get hash	malicious	Browse	• 80.0.0.0
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	• 80.0.0.0
	#U260f8284.HTML	Get hash	malicious	Browse	• 80.0.0.0
	HunpuKMHQt.exe	Get hash	malicious	Browse	• 80.0.0.0
	1.sh	Get hash	malicious	Browse	• 62.254.90.3
	PDFXCview.exe	Get hash	malicious	Browse	• 82.38.144.251
	JbQoNNPVOk.exe	Get hash	malicious	Browse	• 80.0.0.0
	_vm583573758.htm	Get hash	malicious	Browse	• 80.0.0.0
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	• 80.0.0.0
	message_zdm.html	Get hash	malicious	Browse	• 80.0.0.0
	0000001_Carved.pdf	Get hash	malicious	Browse	• 80.0.0.0
	BWKPI3LiLi.jar	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):	5.712184844304402
Encrypted:	false
SSDEEP:	12:vDRM92zLZiECxDRM96ZBZLZiEF3lhDRM9GBLZiEhQxDRM9z3BBLZiE:7qE2j3CE5l1qEhQlBE
MD5:	943070EDDE70B1127C835CDDCD7CE105
SHA1:	CDD5745215819EF8D0A32375D2E5C99A3C10FED5
SHA-256:	085C0944D7CD0B58C43EEBB5F75E1A30631086FE343FAD61B02913EC421C2768
SHA-512:	57D4EF9BDC99182AA6417068CB77B12F122BDB0497FE2D4149577569E5E3826EDA8E45EF1FBC2346B565E7F8EE04A97B4AF8B642B9BAFE4E975FC66A9725576
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...2.../....."#.D.".?...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .H.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .eR..../....."#.D..A...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A ..Eo.....Z.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .(m..../....."#.D...A...A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....A..Eo.....NzT;.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../....."#.D.C4C...A....d.{v.^.G...d.W.:...P..k%..A. .Eo.....A..Eo.....V.....

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):	5.660936545218893
Encrypted:	false
SSDEEP:	12:V9zHr9PQSlH9zpA99PQN9zEKk9PQ19z/Z9PQ:XzL9PQSnz89PQvzEt9PQ3z/Z9PQ
MD5:	C5A9F587AF05A9367BDB88D34EE294CD
SHA1:	ADAA12E2743669469A818C271B4781091E0CEC09
SHA-256:	89F7FE9BEBDD723FE691B7081542E521A9D3ADE7537DF698548652FFF90FB14A
SHA-512:	BD2696D5EF169223BB79D9D77E50D31B84149E78A9116E25C3CE64A0D0D236440583D2F7590C84EF8828FC0D101C1531199AAA872B1A1F5719B909541D96684E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...!.../....."#.DJBq?...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....H!.O.....0\r..m.....,....._keyh ttps://rna-resource.acrobat.com/init.js ..i..../....."#.D..5A...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....o`.....0\r..m.....,....._keyhttps://rna-resource.acrobat.c om/init.js .]..../....."#.DN..A...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .a9..../....."#.D... B...A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....n.....

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):	5.631869658542798
Encrypted:	false
SSDEEP:	24:tB4v4/OSB4B4v4LSB6B4v43SB43B4v489SB:nMBSBwMoSBaMASBaMPSB
MD5:	18A7E3CC194E5E26CB1806A81C43F59F
SHA1:	80E18AEF1FB6C436F6C54C4230C93ECC9C97C6B5
SHA-256:	35C18E64B747FEB730C8804BB03AE44C52DCD59CCAC83CED57505E62E0D8DC7A
SHA-512:	3DBE12475277EA600D9639433090C455A16E2FB6C3AC1C68C694B0BA616617C2CCDED2EE4CBEC4280C7A9A4E4E90D10D307DA54924AE77BFD4949C3A04D96 4D
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 ...1.../....."#.Ds..?...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-vie w/selector.js ..f..../....."#.D..xA...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....b.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracke d-send/js/plugins/tracked-send/js/home-view/selector.js ..k..../....."#.D...A...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo...../3.....0\r..m.....v...n....._keyhttps://rna- resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...../....."#.D..&C...A..hvDO.N.t@.....n.*..... ....A..Eo.....A. .Eo.....!.F.....

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):	5.721584000569847
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsBMCqTY2iWulHyA1TK6tz+NtVYOFLvEWdFCi5Rsp3YDY2im:IbRkiDGLWussmbRkiD6BWuss
MD5:	FB7174323C54028D37A13C9E7B392368
SHA1:	68E4430FD2C1D12220009D7C08299064F565A52C
SHA-256:	3E329F1C7CCF44E60272151F65A164D0B74267B8EF3FD94B48372459B61C5228
SHA-512:	1B70EEA1E968A709A174D07E37095390EB9ACA4C59BD48EEA3D5628A96BB07401C03C6F9030688CED57E118DF6AA57D2CEB180EA46B70BA5A82015F4C1FDFC 09
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 .$<8.../....."#.DZK.?...A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....0.....0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..=..../....." #.D.*.B...A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.601056029959281
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuQSyVyh9PT41TK6t0+yiXYOFLvEWd7VIGXVus4EVyh9P/:pyixRuiSyV41TEByixRum4EV41TE
MD5:	A27DEACC525580FA2FEA64D2F644CD30
SHA1:	F524AB6A8AA544832871CAB2B40275F01E8B41A0
SHA-256:	38E785B63DCCBB5C8AC4EF89E53C60FBC01A69AADA1706373CD7BC75486385DC
SHA-512:	D4FEB6AF4E3863A05DE5A99D64FBC83EBB49219001412A95D6EB1E7FE4E518735AB3892EBD42F5A10E2CFC9E8DEF8BD497369DF0FB6B3309A4553EF01C7F2A 33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .rV..../....."#.D.A...Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo... .....8.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...../....."#.D7.1C...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):	5.634424742928793
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQ22n4SLZIl6P41TK6tiEvYOFLvEWdhwjQj/KlJky4SLZIl6P413:0RhkLshLZCjRhkZLZC
MD5:	603F38645AFF223431952C94FF498644
SHA1:	202D3B8F2B7EE778544AFBB3C8F1C1A447E24FBE
SHA-256:	82922C033C3E9ECCFD9F29B53D85265F9BC898A37C39EC553ADB6CD58438E3BF
SHA-512:	A99C4703D1DB42DCC7C63ABBC8D178D9DDC137BCB95688B936D3AD94C2A2671B9F4D1BDBC84FA75079FB3C85305A6C0745E2A936AA8F788F6916B0C2BAD17 B9
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..kA...A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....|).B.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .E..../....."#.D..C...A.].>....uUf..N...k.....c..l.A..E o.....A..Eo.....=.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.564116184765314
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQ/9Q76g1TK6tBIMJYOFLvEWdGQRQOdQy7OlxXQ76g1TK6tlH:2RHRQC09Q71VRHRQCf7Oj81uH
MD5:	7F1B69A36C0D4CE8451A6289158687E3
SHA1:	F95D3EEB22C4AA2B2E0784C50AE9AAA08B68BF47
SHA-256:	C59C511F5BD81809B0D92AA56EDFBB5E6680DE7F7A14C88A61C25315DBA8D856
SHA-512:	F038E3CC9A156564736BE13A341061B8A2B792D0AE98470A49426125305D2ED5F53E6B02EC1F40EC04B6320B0D05411A3FABE2C8906A0DDA08BA6D6C5D93600
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...../....."#.DO.A...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo. .....l.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..U.../....."#.D.31C...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..... .....A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	716
Entropy (8bit):	5.639285924367452
Encrypted:	false
SSDEEP:	12:Z5MS7+ENMuR/E85MSKk0INMuR/EG75MCNMuR/E05MiKbNMuR/Ek:ZSVuR/E8SSKFvuR/EG7SduR/E0SMuR/E
MD5:	17225418D740C23AD700ECDE3071FCD1
SHA1:	FEF07EFA1CDE094D2CCCE871290C3673BC18D12F
SHA-256:	EEA8BF0ECE574EF74D8665F5D95727391A1C610E64A242A003E6FF2DB3E8D0FC
SHA-512:	AA12273D70C9D46F06EB53B6E01725D7D9DC8BD3B6045699BE610370DDB88BABCC9F7428FCCC4C61676A090D857229F2DCDE8DF3FE85ABBB7F80D037934F9 D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...!.../....."#.DY.q?...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....&P.~.....0\r..m..... .3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...../....."#.D..5A...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb... ._keyhttps://rna-resource.acrobat.com/base_uris.js ...../....."#.D-..A...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....=.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..<..../....."#.DL..B...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....&d.%.....

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):	5.586869194576443
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu+Ol8evIm0bbsIDMGH41TK6tO:XfRMkK8OKsIZEY
MD5:	C7338A52C137C0D0326816478E22EF8B
SHA1:	0EC29B67E5937596B35B96BABED3E676DD068354
SHA-256:	2240721693E071DB40CF1E3607A00B6AE743D2CBA2FF989EED0F12BD57061596
SHA-512:	6FF9E9CE295DFC2D1C7F67899095874537F0A17C3D40E0D5E2294AFEEDE00076085EB30797B771B8D0452D0A829F600B9043532AA712DA87903E3761875E7A44
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .?...../....."#.Do..A...A..`....^....L>..Xa./.....C.y.A..Eo.....A.. Eo.....b.....

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):	5.574074671366839
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuA+DwI+by0zBUKSAA1TK6t6E4fPYOFLvEWdtuBOvm5jM+by0zBe:pRIh+besbRoTI+beRb
MD5:	DA9C4CA0B3A8C662114D00B5A27EFFDB
SHA1:	FF547F3109000D4BFD86BD44F874C4AEF01FCAAE
SHA-256:	A2591C63C55B6E1C419A0C7023DA860A9EA656BE82005B660A0980743973E196

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
SHA-512:	BF9E7CF081F98D9724E8769628D7EB0A24D28D0FFB0D1339E16A4BFD843CC3C2A0D50BC8FDFDDCA4F658131D766CDDEAB2FCD4853BD38650F28A7DF41DE1 610
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..d..../...."#.D..A...AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A.. Eo.....Qh.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .[>..../...."#.D.2C...AQ..E.=....=h`t..t..3%A.F$.. w..A..Eo.....A..Eo.....FR.....

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):	5.60039016672257
Encrypted:	false
SSDEEP:	12:KkXxKMSCvztUl4akXxKMSCv8b6ZtUlQakXxKMSCvNttUlw/akXxKMSCvDOQtUl6:KkXxiCrW4akXxiC0b6ZWQakXxiCFtWwh
MD5:	127CCC246B35CB51A4F68B7E3C8309FB
SHA1:	86ED1FA3F49DD5D9F7DDC41765459A33CC1F2867
SHA-256:	8E4CBE6262B48C5E8B43FFFB82AA071B282AB4530D8B553582531C96A7CAB78A
SHA-512:	0D301E536ED0DE5FDFF4121A35A8DDAAC50D11D1DF0BC361ACA898A7A44A8FD7231B4537197B349AE120810960051020265 9ED66A2078823E3A8E8FC6D92138
Malicious:	false
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ...!.../...."#.D:Xq?...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....P.....0\r..m.....1.....5... ._keyhttps://rna-resource.acrobat.com/plugins.js ."...../...."#.D..5A...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....G.....0\r..m.....1.....5..._keyhttps://rna- resource.acrobat.com/plugins.js .?.../...."#.D*..A...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....i.....0\r..m.....1.....5..._keyhttps://rna-resource.acro bat.com/plugins.js ..;.../...."#.D...B...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....

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):	5.611843540020655
Encrypted:	false
SSDEEP:	12:5h6OLNIRak2hh6OLYkGkDh6OLakn/bh6OLCk4:5h6LRvlh6+Dh6Gjh6e
MD5:	91795E9CEFC9CC37EFF51DEB9641413F
SHA1:	BD7BFEF44976492718DA59E323420C36E15C2FDE
SHA-256:	B358F91319F5493D6F0F4157E238EA5FF93B0CDBBDD6C1F7FAE5CBA7135E0768
SHA-512:	54B52A2E8ACDEA4CA1484768FAD61ADECB338C0ECA4B97DBC1C30F026E5045A14E9A2919F4872E3595CE76FDB72477E098EEA7FAEAAC061E98F000A28BB30 9DE
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .tu-.../...."#.D.#.?...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo....._.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .cs.../...."#.D..^A...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....-.....0\r..m.....;...I....._keyht tps://rna-resource.acrobat.com/static/js/desktop.js ...../...."#.D.L.A...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....$.'.....0\r..m.....;...I....._keyhttps://rna-resou rce.acrobat.com/static/js/desktop.js ...../...."#.D...C...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....R.....

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):	5.6721145162340605
Encrypted:	false
SSDEEP:	24:UB4v4oKwzXLnEkB4v49wKwzXLnpmB4v4g4KwzXLnuB4v49jKwzXLn:8MJbnZMPbnpWMT0bnOMEbn
MD5:	0CF38AD2D9FF2356D6176F2834626529
SHA1:	E1FF3DA98481B2B393A1740C51F2F1471DA73411
SHA-256:	149F6F42C00B08922DD1B6A60F0B53DEFC813D969490567C4CF908FDFF550B16
SHA-512:	F9A366048F87509089EC7477A86564D8195CBE3D350E8C79AB971574C6526C09E48897F4848DB471506CDA6EA35525D0F358E4314592AD0C1B90499A8ECAD640
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 .g.2.../...."#.D...?...A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....f.....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 ..X..../...."#.D...A...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-s end/js/plugins/tracked-send/js/home-view/plugin.js ...../...."#.D...A...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....Y.....0\r..m.....t...R.1<..._keyhttps://rna-resourc e.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .K...../...."#.Dt}7C...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....,.V.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.510874996556817
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQcpest5GFCaa+41TK6tk:NRMHdH4st5Gda+Ea
MD5:	A28C8FCFBF5CE67C6930308C08F14B3E
SHA1:	A43395299437E82453A0773235BB469FEADDE7BA
SHA-256:	70E512D42BA75A67AD0DFFBB52C8ABDC12BCD33C0CBC4869832C22393918E81D
SHA-512:	4A0083FBB517E32568188129B3DF7855752D15FF2435F170213EC8F8260472FA5A0DB503E62EDB30429B746792021DFD3745E1C4A04968DA3E8070A05556DE77
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .%...../....."#.DEJ.A...A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....H.....

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):	5.543441646047296
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuhoEP11TK6tLs2VYOFLvEWdvBIEGdeXugiLdP11TK6tu:BsR2EsepkusR2EseLeM
MD5:	8FF26F9DD8B808BBD6290149CF788F3B
SHA1:	263B0B4CE3A5FE970EBA1AF18B8B35755499216C
SHA-256:	958EF74EEC64BA8330E472C4D5A0773F03603208EB283B1C250AE5402099BDC3
SHA-512:	0E980E85DACA029DE5AED6655F76DEB21CD033E81A2F40B8A2356BB78C11FCB06BE37914936AD039C8086E774DB18921E92B3ADAF5DC83D41CC85D8D293972 6
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...../....."#.D,H.A...A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo. .....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .?/..../....."#.D...C...A.A.o]@r..Q.....<w.....].n\....A..Eo..... ..A..Eo.....!m.....

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):	5.6599593941299595
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ5LVGF+B7OhKlvA1TK6tyaVYOFLvEWdwAPCQfN40k+B7OhKl+:RbR16epBJkrbR16501BJkB/
MD5:	865E34F0CAEF519C6A5C24642233F10C
SHA1:	07645D7ED7A8AF957C1866932D1215A8D0C03461
SHA-256:	9D67625084FCFEFA70670A26079E9F729473EEACFECA1A982FFAC1D7786D65BD
SHA-512:	931A4E0154267CD85D16BE4145DA7FA727CAEEF3BE240E3456C8D361A8E6580CE5E55CF5149B78B3FF846A2CADC984ACF3B89571921086E9C694415EDFA849A 1
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D.jA...A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....M.....0\ r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D.g.C...A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....C.....

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):	5.645940551375739
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu0HPznQdFt1TK6tfNs2gEYOFLvEWdGQRQVu2SlaURnQdF9:B2geRHRQNL0JW2geRHRQklaUB0I
MD5:	AD5768F8919A3317B709F13C9ECE4CBE
SHA1:	55D74D7AA43DE517DB6D687056EF44E0E6FDE5BE
SHA-256:	CDD6084109336BF655C03DAEE717E21FF1F44C61EA4A4F121625E9C36639D262
SHA-512:	836D21972DEED1DC1404D38903E935F7E2D9DEE7990FFFAF8ABB7D52AEC21489F3B626633A69B589D24B2EF3F487F2D521F1DB164AD0C948F7DCF45496CAC2 E
Malicious:	false

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

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):	5.654019315217969
Encrypted:	false
SSDEEP:	12:WyeRldkOt1w5yeRlhBEt1wVtEyeRl48Et1wsyeRlqfEt1w:WJZfw5JZifwnEJwVfwsJifEfw
MD5:	33FB870C2A905AA9B4FA0753E27DA3C2
SHA1:	132D0F39B0260718DC13C91C0C8978A9AB25E0D1
SHA-256:	AF8C485E3ECD013D4F1C0AC997C148D756B3858088742DEA5E855A3E2080C743
SHA-512:	6BDA0EC558887F0E349433247D466FF0ACB017F524D91BE5A81B5255907972EDE163DBACF8A7CC070148BDB69CD8A5A99491777EAC25C88F966E5C1AED48CE4
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.....D.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..X..../....."#.D.cA...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.3.A...A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....a.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...../....."#.DaP.C...A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.573819169923571
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuTK2clCqwK+41TK6tanYOFLvEWdhwyuRI4XzlCqwK+41TK6tL:wRhk8ljwK+EGRhVeljwK+E
MD5:	741245C926587FB7F1D636B9AE5D5D64
SHA1:	445555A2039293F43EDCE3FE7D62753378EF2FBE
SHA-256:	46EB8E9E8AADBEE4226B425A502C5A440D5F632B81FFC12C571936B5C0AB39B4
SHA-512:	F0D43DE319757253E5E86F356740770A985B9ADDB84D33F643C65ED7EAE6F4CF07A06CC4500E8DA17BDD98663C1E5837ADE3A8891EA09DF52E64449B906D62DE
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...../....."#.D..jA...A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....u.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..5.../....."#.DB?.C...A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....3.....

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):	5.614449666496943
Encrypted:	false
SSDEEP:	12:/RrROk/sfLEF/NRrROk/JzfLESRrROk/yjfLEYRrROk/JSuqfLEnF:/PJ/s4NNPJ/V4SPJ/yj4YPJ/J9q4
MD5:	8CB6CE012E0B8D2EBA2C7104E9A56F95
SHA1:	FD4DE40EC37DA0DD07C82AE2A1A90B46B8767371
SHA-256:	D20E609A7EA08997A27688415D62399038837D2F49A5EDAF197EE97EE5ADDB3E
SHA-512:	51C3534DE6C64671EAABD3B79356C29B99FA428BD697EB858AB28E93BF9DC7CE38ED4D3D1407C39B09A38BBDC6348BD60715B5F5941184679D14ED2D9777CECF
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .h...../....."#.Dw.?...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo....._...0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..U..../....."#.D.scA...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...../....."#.D...A...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 ...../....."#.D...C...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....+u.....

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):	5.663404933319948
Encrypted:	false
SSDEEP:	12:xqTTE+CPLnxqTxXCPLn2H5qTSCCPLn3qT8O4CPLnw:AXHMnApMn2omCMn6x4Mn
MD5:	6C64AF1E5B8E9754D21E9EB68B383C98
SHA1:	94B7A71336E8F5E4AD0A2487C34B9AD9C08AB51B
SHA-256:	288EF64CB44613E594F757D00A0EA15FE367B8E2BDB763B018CEB230BA7E5D47
SHA-512:	494ED6619EB36F79AA4887EDFB06206C45721E4420A97236F95987605C5DD0BC4E29FC0D3DB4D4893DAD103AB3CC133A1FEB968CE35C7762F2CAF4DEA9C3E 30
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .?3-.../....."#.D..?...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....x.....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .?b..../....."#.D.u^A...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Z.....0\r..m.....:....f....._keyh ttps://rna-resource.acrobat.com/static/js/config.js .]../....."#.D2Y.A...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....d..B.....0\r..m.....:....f....._keyhttps://rna-resou rce.acrobat.com/static/js/config.js ...../....."#.D=..C...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....c.....

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):	5.7034225955148905
Encrypted:	false
SSDEEP:	12:zRMCkGpZsDr+RMkDsDNtRMtIsD0RMO/AsD:zKjDr+BwD/cD0j/jD
MD5:	83FCFB3761C9C255004718F62D4CEA38
SHA1:	C2C47AA4D9E65F613EA7A01E0DECB720F670905C
SHA-256:	68CF3B4ACFCBFF74951FDA3F0CA40B2C521FEF3D075990B4674051D1105E091C
SHA-512:	61194D8AC3B3E5F9C7E58F10EFD7B9CFD0DA671EAEFFB9595633E6D5BD90093CAB7940A653B211259F17D8DAAE7E94E43B569C15956E48C896086074F53BB62 6
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...1.../....."#.D..?...A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.... ..7K.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../....."#.D+n.A...A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....q.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../....."#.D...A...A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....v.WN.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..V..../....."#.D2.0C...A..z._a...'.v.....4p3..1.'].. .A..Eo.....A..Eo.....5.H.....

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):	5.658564629065875
Encrypted:	false
SSDEEP:	12:6lJR+FoMllJRwTFoMWlJR6MCFoMblJR5sAFoMA:YQFoMhyTFoMcYMCFoM/zRFoM
MD5:	BB4FF925B3DD40AC23D7675F28F7B38B
SHA1:	14E1EF8D9ED9CAB20215B905FF09965F9A012146
SHA-256:	B0CBD90252CEE849D46FE7B89D8E95217DF1859C56752DAB78C053B9F8B89A7D
SHA-512:	AAF1642C5AA3B99E88F69524868A908952280D1963E2253D4688CCD4FC01CCDB92B7A127FDD968B19928E2AC5E777230D4647D9E2FCBE04B7C77FDBF41782DI
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...1.../....."#.D...?...Ac}.H7M=M..-.....lx..R.l...}Rl.$q.A..Eo.....A..E o.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../....."#.D...A...Ac}.H7M=M..-.....lx..R.l...}Rl.$q.A..Eo.... .....A..Eo.....g.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .zh..../....."#.D...A...Ac}.H7M=M..-.....lx..R.l. ..}Rl.$q.A..Eo.....A..Eo.....Z.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..W..../....."#.D@.0C...Ac}.H7 M=M..-.....lx..R.l...}Rl.$q.A..Eo.....A..Eo.....\q.....

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):	5.6142961811306495
Encrypted:	false
SSDEEP:	12:F8hRrROk/i3oe2l8hRrROk/RVe238hRrROk/EHe23n8hRrROk/pB8Ce2:UPJ/o720PJ/RQ2iPJ/X23SPJ/pBm2
MD5:	6AB36FC2E8DF9D020B2B0A1C18A83EDF
SHA1:	34EB04AD08CEAA1222993D523CF82CD7AB7468A1
SHA-256:	9555C86D7701EEAA3C84F395A4025F4C82C1615842E836C15E5AE44ACD508E86

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
SHA-512:	D2F4105D66BD25293F31B89ED8A2B92DB2E6125FDD40A61105D12FE3CE99324676673DC8A2F853059FACAA58BC3B59AFB7F8C32CEA8616DEB642F45BD6A07F7
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..j..../....."#.DY.?...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....6l.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..7..../....."#.DUhcA...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....Tjr.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .1..../....."#.D...A...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 ..o..../....."#.D ..C...A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....us.....

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):	5.698980624454083
Encrypted:	false
SSDEEP:	24:ehDs7JICThNk9GJIC9hB59JICCIh2+JIC:esTX0q9Bjj
MD5:	1EE5A07141380BFDD9F7415AE50B9C09
SHA1:	3BEAC65586963D1FA88AC26C9131957616F01C58
SHA-256:	ADC131C83E6D599A27A188F173E0F48354CD86EC184796B9DBCF4A34F29DBE67
SHA-512:	4137074A17D0B945DD43A533D85C9A80F5D8A91F9243077DBBF399E06B365FCCD3ED9F0567D35B7B00E76231D9E95633098B9DCEE65E7F7DB22CDA65E03B4F9
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...../....."#.Dbe.?...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 ..f..../....."#.D).cA...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.Z.A...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.z.C...A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....>={.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	832
Entropy (8bit):	5.627658767969819
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuYL9uLpLzgm2d/1TK6tvNMOEYOFLvEWdrIhuDWHeTLzgm2d/14:0R2LKhRe98R5WH4Re4RF/ReQRQf3Re3
MD5:	2DCFFF2F9B4D7975DF19CEC657FCB25B
SHA1:	349E4646FD434076BE7797C121FBCBDC1BEBAE13
SHA-256:	02C0ADDE2B910538B4B6DFD5E3FC739995789FD29C0D5F4436C04FE329486D13
SHA-512:	8275870AABE238EA465FFAA28ADB253913C00CB76438D8D0A076A0868253E99FFC45BFFF2AF8F0498F910135DC996DA9007D7B50A8B17E23CE2E2F3E39F8A041
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..h..../....."#.D.w.?...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 ...../....."#.D..bA...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....Wd.|.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...../....."#.DP..A...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..../....."#.DL..C...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	752
Entropy (8bit):	5.639858715827188
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KJkf2kx56uvp1TK6t88AElVYOFLvEW1KFWkx56uvp1TK6tgt2Aa:6JJKJkVbJJKnSKJJKHvzGiJJKzdV7
MD5:	569510B271C402757FAEC5E9C148D28D
SHA1:	ADE8A8FD087D2899F79EFAE5BFB89AE729C37674
SHA-256:	C06366D8634C7E7C61FE3310A3CF3DD3063648A5D2520F4316F737E4BB2A0518
SHA-512:	CEC3CEC4FD688112D443DB9B30CE635ED5E5D783CA8953BBE6E3AD174EC7B54CCD2FCBEB21D84BBB10B92A3F66251D375E783352B210696F08907152405F093
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .Pp$.../....."#.D.?.?...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....Y.a0.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..r..../....."#.D.WFA...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D...A...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .:P..../....."#.D...B...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.631137392188462
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuPGehUDLYtmOZn1TK6tSWYOFLvEWdBJvvuc/l9hUDLYtmOZn1j:xRBJMGrDcFZLPRBJbIIDcFZL9
MD5:	F65BAE3C53398393CA8EB4DC8240303A
SHA1:	52D81D0D562969D3E6AF0927E2E6C228274A562E
SHA-256:	01B3216BB839DC161182B99285A9C2AF24C0005956117897862 63B749EA81BE0
SHA-512:	44316652A16587F160A8494F416B6421BAD0A8D84A76F2962FA6A62BE251E590EC4F5DD1C7540AF216A0934F159E6CCD6C64ED46A7449D1344CCC61E66E55F85
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...../....."#.D...A...A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....t.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .]U..../....."#.D..0C...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):	5.667677489329685
Encrypted:	false
SSDEEP:	12:BPH4OEcb7PH6IcrzyPHXGJcm7PHr16cp:BPHccb7PH6IcrzyPHXscm7PHx6cp
MD5:	93C34B6041CEF6AB906B3E30AE664494
SHA1:	30CB1BD16B6E82095FD05D6B42E6C5EF93D3FD8B
SHA-256:	82F5B2FD49F98DA46B0A05EE0E7F95C06A1043F6BDF5D0784A9D977D7298F038
SHA-512:	B891048B4D540F33FE405F5D82F3B7C52728E0B8858EAB89F6C134B701F17C6A707D45C810089FE04CE9C0403F764A98C169F4553E563C0EEC547363CF662FD7
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...!.../....."#.D..q?...A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....[.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.D..5A...A...L...Im.@.....E.nW...IP..A..Eo..... ....A..Eo.....S.1.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .U...../....."#.D..A...A...L...Im.@.....E.nW...IP..A. .Eo.....A..Eo.....X*.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..F.../....."#.D...B...A...L...Im.@... .....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.586341162295379
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QBkdiM3Y1TK6tl+KPYOFLvEWdENU9Qa3iM3Y1TK6tA:bJRT9cer02JRT9N3r0
MD5:	D1E01DD311D8D6FD8C5A074C8B1A11FF
SHA1:	9894EC38530138866276B2CFEBA2B11EECF3C6EE
SHA-256:	7B218C5D6E8A69516EEB944A267F562EFDE0DB696EDAB96D04EEA4AB9A2C1BBA
SHA-512:	835EA713676C0F5EC61770F3F157674AF00F0F2E1687875BCAA3616DB7310CD5DADFBB69F9E93032D8587EB0E2F7A244D4C3C8062A989C211CD48192DAC186F
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...../....."#.DK.pA...A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo... .....3\.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .z...../....."#.D.. C...A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... .....A..Eo.....V..9.....

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):	5.625205443543067
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQr6HjBRCh/41TK6tE2Qt6EYOFLvEWdccAHQ3yXmkHjBRChL:XRc99Di/EuHRc9ZmkHDi/Ei
MD5:	BADBAC69794A51ACD99CD3A90A4A3941
SHA1:	00B9C554501C6ACC4302D0B5B555A8A77B85B7B2
SHA-256:	9E39A522354689A140B924BDE0F6124B72270DF5E340439756DAFE09AEB474F3
SHA-512:	F49B53243C591444528D69349A2196A3763F9CC8FC3E1FCC3EA4CAF8BC6EB7A5C305704024D7C4E3080A477B94CCC7B3C0FAA096F8F1A5A32236DE0A7290D08

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...../....."#.DG..A...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....Ep.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..P..../....."#.D$D:C...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....0.....

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):	5.615639395418434
Encrypted:	false
SSDEEP:	12:bs6xRkiO2LlF4nyZs6xRkiiGwdLlF4ng:brxpLoyZrxppwdo
MD5:	234A673DB627868FE0A7C2CF9861A595
SHA1:	F9497F9394E14D74C2E90D33E16A1E20083426F9
SHA-256:	47020558F532D39B8F5D20A61A2271B7B2DDD0621A1E7988A1C97F65F7AE56DA
SHA-512:	D953513EC6C491E24A04E519C0E0C0C5A3F5225F9D54189C2A60E689797D4735FB009EA523A5056E7D1D67315B851C22D5D28BEEC889836F903FBDC386011E5
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...0.../....."#.D..?...A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....@.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...../....."#.D.D.A...A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....

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):	5.54663307443274
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuOxSY941TK6tF+hYOFLvEWd/aFulSwm5jfY941TK6tcx:WR29EOR+T5U9Eux
MD5:	BDC644862B625DB696F22185922B3768
SHA1:	29D4402A5A17EA5C743D64984F0AD14DE15A8857
SHA-256:	A6A7EB17F8A20CAD96CC1FE62065F7900C0392BD1FD7B1BDC6E8BA07390E84B4
SHA-512:	AD1CE609E1F7AA91C90E41470E86E7ABB50114A0D5323B8D4A21245895FB94831D6AA065750B4C4FF337C445415B484F06E231775A5B4F3F8CD40E2863C2CC74
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .hk..../....."#.D..A...A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....}ak.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..P..../....."#.D<22C...A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....,IY.....

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):	5.568396087012724
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQYFcmBoBMqVd3G4K41TK6tRw/MR9YOFLvEWd7VIGXOdQfx:2DRuRLqB9Vd2kEgDRuRTDwmqB9Vd2k
MD5:	A37C42368C30FB5B97A733A1994E30DE
SHA1:	5BCAD7E7720B3F0B4C1FAA880090FB40BA096D63
SHA-256:	B8A1D5A996E002CDDC24CDFBB73F9916606B3EC7BBB584A2F810862AFE6A5555
SHA-512:	7CF4D4F5911C56C05DEE9AA6574493829750183C0B0EF09354912E1AA03F553203503614F1697A0E50F22FF238F74DE3B21439D74C4674EE898B3EA8319AB4D4
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .$...../....."#.DZ..A...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....].....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .:...../....."#.D..2C...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....M.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	832
Entropy (8bit):	5.627671996185328
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q2j5RuA424r1TK6tnkqYOFLvEWd8CAd9QvSuA424r1TK6tl0:+RQhjCrndRQgrnpURQnrnXRQpTrnpt

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
MD5:	3206F180D72493477E7B6AE3644E76D8
SHA1:	DA68736BD2A553B00B1F9440277ED9C20140CB41
SHA-256:	34CBB932B9D09E2CDBD08BA1FD51D05CF0C0F8CE18641C109229FEB0537A0771
SHA-512:	FCA0060677591DC5149A83D1064FB169F245991ED46AF13AE61E687F73573518C71DE91A11F984C62E723C184036CA8C375F24C3D1BA37E7AD8F87A5275A3D7B
Malicious:	false
Preview:	0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...2.../....."#.D32.?...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-.A...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....Z7U.....0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..o..../....."#.D...A...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..3C...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....>u.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.5861483717287905
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuR8VPesyC8n1TK6tE8oXXYOFLvEWdENUAuQiyC8n1TK6teFl:xhRTQVPl7QaDhRTWi7Q
MD5:	00497797C6EC41A8C5B3722E5CF23F41
SHA1:	45C1E0B5F082D1E64477F27E4F8C078FE73A3DED
SHA-256:	058DEA30B76C391B642632E43EA6E77A3A6EA32CBC893F003D0144454C770ED1
SHA-512:	D329CBF791E558574FDD286EADD26B08F050046FD9CC5462408C0193C81B8008805C0B8117C76BB73C92538092DC44A6BFE5E6095B2D069C343D0AFCFCA2EA
Malicious:	false
Preview:	0\r..m......R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...../....."#.Dm.jA...A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....I.....0\r..m......R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..3..../....."#.D.).C...A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....Go.....

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):	5.68570327021316
Encrypted:	false
SSDEEP:	12:nRrROk/VLVmclXRrROk/V6nMmURrROk/VrMmqRrROk/VC3emM+:nPJ/NgUXPJ/8hUPJ/bqPJ/Uv
MD5:	1CB4950074B1D1BE6E5E50331C5BE9DA
SHA1:	BB4E68F790B1844AF0C1D0385FBDFB90A246B9D5
SHA-256:	6397388528D3FAA860CBE94E79DDB8A64D7E22A5D112C3F6E0568A943DBFD6B5
SHA-512:	DEAFB6D9E5DA5DBD2FE0DF15B36E1F904B57A84A313B623C67FCB9F2014017C119F74DFBFAC8B2A5771069060672558 43ACBA48CA55C57CF8579F8FAE2723F E
Malicious:	false
Preview:	0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...../....."#.D..?...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....!.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..~..../....."#.D.)dA...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....q.v.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..*..../....."#.D.y.A...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....7.....0\r..m......]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..../....."#.D...C...A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....[.....

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):	5.604819606203108
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuW0xAdm9741TK6tVZ/lXYOFLvEWdccAWui/id2xAdm9741F:qxRcpAdu7EbxRco/g+Adu7E9G
MD5:	FC8EDC32BA09B656B66EF073C5C592DC
SHA1:	1AFFEB970BCD21367E411AD8115EE0FE225CAA6D
SHA-256:	DB5B3F5F9199630A1DE366FE99236595051BF5804F364198215986E01B5BDA39
SHA-512:	18B62CA2526398D53C95F6673F7BBFECB16791F1FAC5AD8353DBA8DD7E87DAA8049E68D49932A48611AF646F25C6DA2E946BE26E8C182BFECED41E17986C50 E
Malicious:	false
Preview:	0\r..m......R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...../....."#.Dg{|A...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....t.s.....0\r..m......R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .]...../....."#.D|.*C...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....~v.....

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):	5.582284950471284
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuhE2Kk7kJn1TK6tNMOYOFLvEWdwAPVuMekZ5KkJn1TK6t:2R1j5nL7R1P/5VL
MD5:	075CCE5D425FFF95EE8412DB7EEF9ACD
SHA1:	05906F5A7AFFF4156AD7494805FE4D2238D2F2C1
SHA-256:	60BB329DF238F82D57FE4C78AF6C13446DBC5F8B079A916F2559C315D53F7310
SHA-512:	5B0C06E9CE74024A73A53C8D7669DA37465752FC166DCA202BD40FEE62C8889E8FE7C9AE9258F69686226C2E4BC5E5E7D234F590C10ED177C27ABB80AF106A5 2
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...../....."#.D.tjA...A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ..8^0.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..2..../....."#.D...C...A.....k....F..D..O.n;[.1m.....=..A..Eo..... ...A..Eo.....>m.....

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):	5.695290822467785
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ1Cr2zhcsBXIh1TK6tK23PXYOFLvEWdBJvYQ/D2zhcsBXIhm:mxRBJQCg2DB0ZxRBJQS2DB0gn
MD5:	DE99850781D4FAC81F9AC71A344B744D
SHA1:	5B9EE04BE73B090261FD0B371F93DEA46B35769F
SHA-256:	9CB5890141C195FCD02B983A6ED1B6A950CEA359062CCBDC75C8974F566B1BCA
SHA-512:	73871AC5090EB392F4284A253BABDA1B49A3D0F2BAFF71BD2D4D68DEAA7A82FEB8EFC639A682FFCF23DCCB204380ECA9488CE66E5F82BD555F22A96A34A48 6A
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .c...../....."#.D.,.A...A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....9.q J.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..Z..../....."#.D..1C...A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo .....z.....

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):	5.632547785657583
Encrypted:	false
SSDEEP:	12:3RrROk/sDX2cBRrROk/sgoLcJRrROk/sHcClVRrROk/sI7ccS:3PJ/EBPJ/7DJPJ/TmVPJ/X75S
MD5:	5A5CC36AAFFFFD2C08AEC3066E6F2BAF
SHA1:	F591ED5A8435D885FB81083067C011FE0BBA704C
SHA-256:	DC5F2E587B5D3391659385C2C18672BB333C62E8A43421B7467E97D2BB6B4F9E
SHA-512:	EE516114842A9AD585B7D4A6B189CF7E6F8BDF9F3DAE17812AACC65F900DAE6F01C03CE34DDB6B21CB2843E9E95EEACB9BFB8FB47E75C6656752E1BF67DE6 183
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .v...../....."#.D.+.?...A....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....r.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...../....."#.DnmdA...A..... 9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plu gin.js .>-..../....."#.D..A...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo....."..3.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop- connector-files-select/js/plugin.js ...../....."#.D...C...A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....T.....

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):	5.237110158615816
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPojKbuZKfO1tMBIMZECVdj3EYthE9aRMI+:h1zZ4+dsp6ljKbuZRKGC/j3Ntp+
MD5:	02A44073C6103BBA310180284C2E9EBD
SHA1:	F9EEDD0A6BEB6CCAB3F9BFB37EFC9AA75C389D1E

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
SHA-256:	AC8C7DBD12593B689624B29665AD38A64D18111F362B9861370897994E611780
SHA-512:	46292C757B598CF2D3E3657ACA967D9F700DEF60F201A3C52C7123A8358379E9615BB134FD53C3D3004E52B85412EB1E158237B1CC484F695D776FF4F07DE655
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...j.=joy 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):	5.261600372152383
Encrypted:	false
SSDEEP:	6:m5cCq2PWXp+N2nKuAl9OmbnIFUtpOc5ZmwPOcsnFkwOWXp+N2nKuAl9OmbjLJ:PCvaHAahFUtp/5/P/y5fHAaSJ
MD5:	9A3DB9E83C3482EBAAF0B12A53440A00
SHA1:	8C879579D7981B44253249F65B3276B0D31DCE81
SHA-256:	1719B9ADA08864225CD32A8A6275FBE2100A92901E8741091CFFC2D1C0924AB7
SHA-512:	6811B6B7FAB433B622DD3C8A08BD8D368348F891F1403645B5C5B89A01346F17433FC55CC9083202037A8CCEF682983ACCD34B961670D478DE46B1532ECB3E6
Malicious:	false
Preview:	2021/04/19-23:13:18.772 1b50 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/04/19-23:13:18.774 1b50 Recovering log #3.2021/04/19-23:13:18.775 1b50 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-210420061313Z-191.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	2.148767721262248
Encrypted:	false
SSDEEP:	384:2M8T4Og6sJEMqz7R8XCG8snn73h9Rh9pjJzod3fsmcn2w:2nT4OgVEMkVsg69/9pl0d3fdw
MD5:	28E62CDEA0C4641DBC6742E4FEC44B4A
SHA1:	675521404A4D4BA86CB7EA84C8638BA6A72B2F6E
SHA-256:	9B240A71A4BFF4D61080C2C472ED0799CCCB9020D12FE94B0995EF0972E9FFD2
SHA-512:	97A7BFEE66C94BB6A32B806FA62107C3886222792C0BE6C86E4C8FB7655C6FFEFC051A24D52BF0CA8E4F71589C47CF0981A529C06385ED3530A70457A2BE13C
Malicious:	false
Preview:	BM.....6...(...u...h.... ....

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

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Size (bytes):	32768
Entropy (8bit):	3.3876533839719
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQnOhFVCsL49IVXEBodRBkRSnOhAVCs749IVXEBodRBklSnOhKC:iGedRBpedRBYedRBQedRBu
MD5:	F4679DEF0BD47C27490C92F732EAF49E
SHA1:	A6B3394592B39E588316F10ACA00AD171966AF5F
SHA-256:	5A72E4A382251F35124D3FF1EE0D6C5C967DEA211BA9468ADDA6DD96A1E051CE
SHA-512:	C122857F43E6BA34958CEFE90EEE7F3CB93F10B28FF31BB767D8EB38E1EB4572A2B971211C0EC14A583D2FAF96C88008FC4737DF2E7AB7EE4E4E70A1F6B0F9A1
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):	3.1996684529760047
Encrypted:	false
SSDEEP:	96:l7OhFVCPv949IVXEBodRBkZnOhFVCsjLR49IVXEBodRBk9ySnOhAVCs3d49IVXE6:lriedRB9LGedRBSCedRBNyedRB7
MD5:	AF42F42C35AB7B5716FB0F1F37405BA6
SHA1:	6D5267939271F64B3FEBB5A7C2AE3365D57007C4
SHA-256:	4DDF99BAAC60DF73219E98C71DBE6921035C50D49A1AE2682D1354C2339310A4
SHA-512:	5C670234915319DE7EE0697E22B0B29551BD5A30FFE1F6CE2D185FB62FE69DE7A31DB225139AB78EDC78065F7CC760A440F6432FE9046C948F8CF451D8A4A98
Malicious:	false
Preview:	.....1qtc.....X.. .h...y.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6476	
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 1.4
Entropy (8bit):	7.40317228838786
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	doc13798320210419100501.pdf
File size:	139604

General

MD5:	3290102a424ad87067467fc04458312b
SHA1:	906ed1cf70e333e1820c6daf461dc244e309e7a0
SHA256:	f3cef618295d205d3f9339da45491c2711c92add67e3839bf819c02579b4d087
SHA512:	1a4260c665bdca606311124598327ec9fd0fb1eca21e714c534b0ccaa231157b91a76fa251bef582e100671601d372f1c892c692ec4a12a0c90a34306663582e
SSDEEP:	1536:3oAnohKM1WUKNz0zY5OW3wXeoIuogiowoCjTI/jJV02oaWg11xQUqOq/YFBkbWUL:xokztGJzjBohokTIGCtqhZoX8lwL
File Content Preview:	%PDF-1.4.%.....5 0 obj.<</Type /XObject./Subtype /Image./Name /Im0./Width 3300./Height 2550./DecodeParms << /K -1 /Columns 3300 >>./BitsPerComponent 1./ColorSpace /DeviceGray./Filter /CCITTFaxDecode./Length 4 0 R.>>.stream.....2>G2..GV".!q.1.:@.$.-&.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.403172
Total Bytes:	139604
Stream Entropy:	7.398764
Stream Bytes:	138536
Entropy outside Streams:	0.000000
Bytes outside Streams:	1068
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	8
endobj	8
stream	2
endstream	2
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

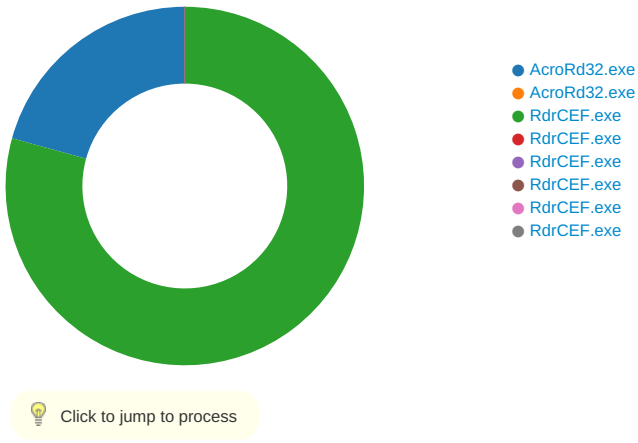
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:12:59.730878115 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:12:59.779827118 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:00.608719110 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:00.657419920 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:01.362535000 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:01.419745922 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:02.393541098 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:02.456609011 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:02.527645111 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:02.576495886 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:03.513765097 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:03.564656973 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:04.980043888 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:05.030499935 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:06.566307068 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:06.614856958 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:07.496222019 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:07.549954891 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:08.669658899 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:08.719635963 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:09.523595095 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:09.575476885 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:10.685981035 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:10.734586954 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:13.073066950 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:13.923541069 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:15.699414968 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:15.753278017 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:17.415400982 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:17.464351892 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:21.556360960 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:21.617345095 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:21.679827929 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:21.738579035 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:23.377432108 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:23.381226063 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:23.436728954 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:23.443228006 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:24.381038904 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:24.381076097 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:24.441407919 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:24.441550016 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:24.807385921 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:24.864831924 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:26.405145884 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:26.405185938 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:26.462320089 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:26.462378979 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:27.587065935 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:27.637686014 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:29.662621975 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:29.711286068 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:30.407099009 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:30.407134056 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:30.456679106 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:30.469522953 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:34.710629940 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:34.784656048 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:35.765254974 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:35.829770088 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:37.850775003 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:37.909023046 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 19, 2021 23:13:53.684042931 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:53.734563112 CEST	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:13:55.254196882 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:13:55.325457096 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 19, 2021 23:14:04.899420023 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:14:04.948210955 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 19, 2021 23:14:15.070398092 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:14:15.128757954 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 19, 2021 23:14:28.796236038 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:14:28.862894058 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 19, 2021 23:14:45.369602919 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:14:45.432821989 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 19, 2021 23:14:46.715816021 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:14:46.787158012 CEST	53	63619	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 6404 Parent PID: 5736

General

Start time:	23:13:06
Start date:	19/04/2021
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\doc13798320210419100501.pdf'
Imagebase:	0x10c0000
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	10F65C3	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	111AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210420061313Z-191.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	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6476	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	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock6404.1.1464209272.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	1142657	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	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	11883C8	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	11883C8	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	11883C8	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	11883C8	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	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1g3xyeu_1fzh943_4zw.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	110EA85	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	3	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Reso7dg_1fzh944_4zw.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	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R8o51c6_1fzh945_4zw.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	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ra8mnpb_1fzh946_4zw.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	110EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rvauj7f_1fzh947_4zw.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	110EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6476	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	114D405	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	110CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	10CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	10CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	10CEA55	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	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/doc13798320210419100501.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	doc13798320210419100501.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	111DF69	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 64 6F 63 31 33 37 39 38 33 32 30 32 31 30 34 31 39 31 30 30 35 30 31 2E 70 64 66 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 34 31 39 32 33 31 33 31 33 2D 30 37 27 30 30 27 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	139604	success or wait	1	111DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	111DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	111DF47	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	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	111DF69	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	111DF69	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	111DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6476 Parent PID: 6404

General

Start time:	23:13:07
Start date:	19/04/2021
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\doc13798320210419100501.pdf'
Imagebase:	0x10c0000
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: 6708 Parent PID: 6404

General

Start time:	23:13:12
Start date:	19/04/2021
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:	0x12d0000
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
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	27	13D83E5	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	13C59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	104	13D8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	214	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2173	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	3	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	23	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	56	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	60	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	54	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	19	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	4	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	19	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	239	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	283	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	267	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	32	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	7	13C59E2	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	13C59E2	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	170	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	13C59E2	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	15	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	325	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	13C59E2	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	3	13C59E2	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	13C59E2	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	142	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	13C59E2	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	13C59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	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	13C59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	13D83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 7044 Parent PID: 6708

General

Start time:	23:13:15
Start date:	19/04/2021
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=1720,1001149262048530690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12742373955121677917 --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=12742373955121677917 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x12d0000
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: 7072 Parent PID: 6708

General

Start time:	23:13:17
Start date:	19/04/2021
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=1720,1001149262048530690,16326826708203091992,131072 --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-preferenc es=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAA AAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAA AAAAAAFAAAAEAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAA AAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Ad obe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token= 8293892013758276365 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x12d0000
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: 5444 Parent PID: 6708

General

Start time:	23:13:19
Start date:	19/04/2021
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' --typ e=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Acr oCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,100114926204853 0690,16326826708203091992,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14988028654324180745 --lang=en-US --disable-pack-l oading --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=14988028654324180745 --renderer-client-id=4 --mojo-plat form-channel-handle=1836 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x12d0000
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: 4644 Parent PID: 6708

General

Start time:	23:13:23

Start date:	19/04/2021
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=1720,100114926204853 0690,1632682670820309199 2,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1643063119428019652 --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=1643063119428019652 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x12d0000
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: 6164 Parent PID: 6708

General

Start time:	23:13:29
Start date:	19/04/2021
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=1720,100114926204853 0690,1632682670820309199 2,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16149447064209592232 --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=16149447064209592232 --renderer-client-id=6 --mojo-platform-channel-handle=2176 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x12d0000
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