ID: 358603
Sample Name:
WorkOrder266912.Pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 22:34:47
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

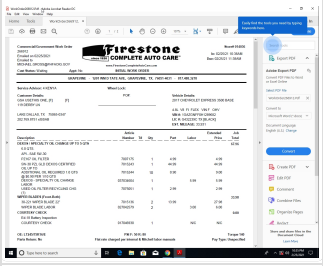
Analysis Report WorkOrder266912.Pdf

Overview

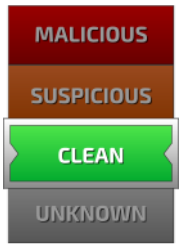
General Information

Sample Name:	WorkOrder266912.Pdf
Analysis ID:	358603
MD5:	2ebe035562b1a7..
SHA1:	8d206b01c0bbd6..
SHA256:	685c6b3fc5b79f2..
Infos:	

Most interesting Screenshot:



Detection

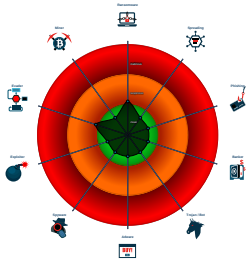


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

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

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 2616 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\WorkOrder266912.Pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 3468 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\WorkOrder266912.Pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5328 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6216 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=1724,128282512544814322 9,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2298543776899609676 --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=2298543776899609676 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6244 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1724,1282825125448143229,14443777595928039979,131072 --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=18073613818027731679 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6292 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=1724,128282512544814322 9,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4894735529953023862 --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=4894735529953023862 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6520 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=1724,128282512544814322 9,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3551037961868620507 --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=3551037961868620507 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6656 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=1724,128282512544814322 9,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13670455395302550708 --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=13670455395302550708 --renderer-client-id=6 --mojo-platform-channel-handle=2112 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

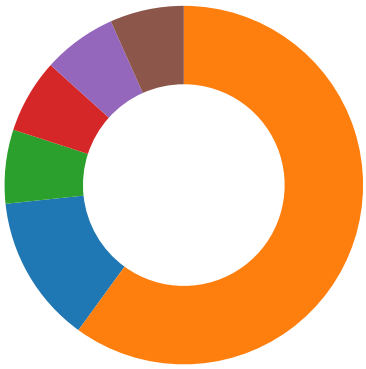
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

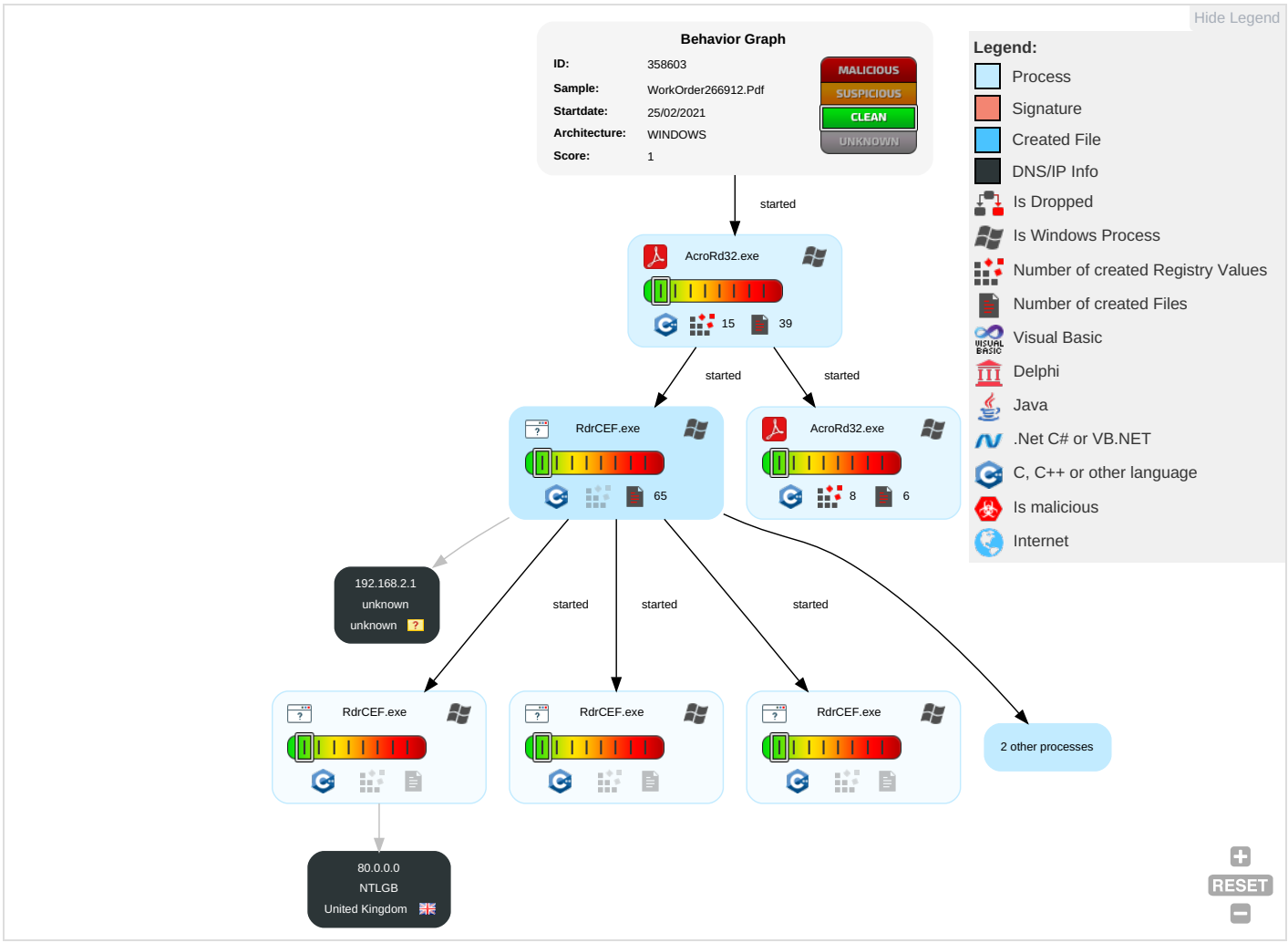
Click to jump to signature section

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

Mitre Att&ck Matrix

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

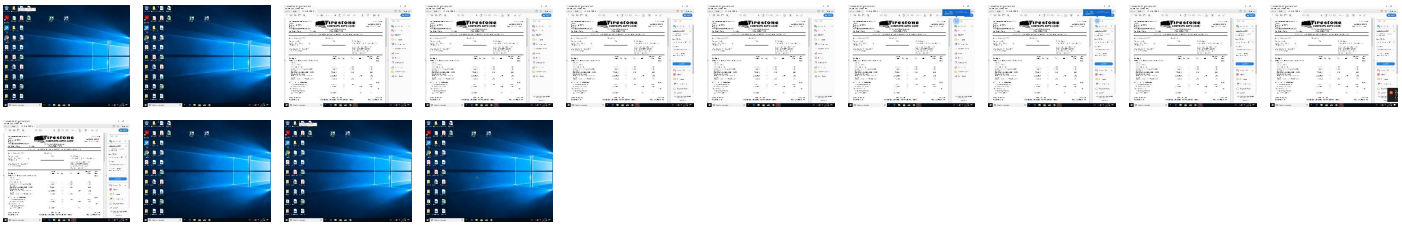
Behavior Graph

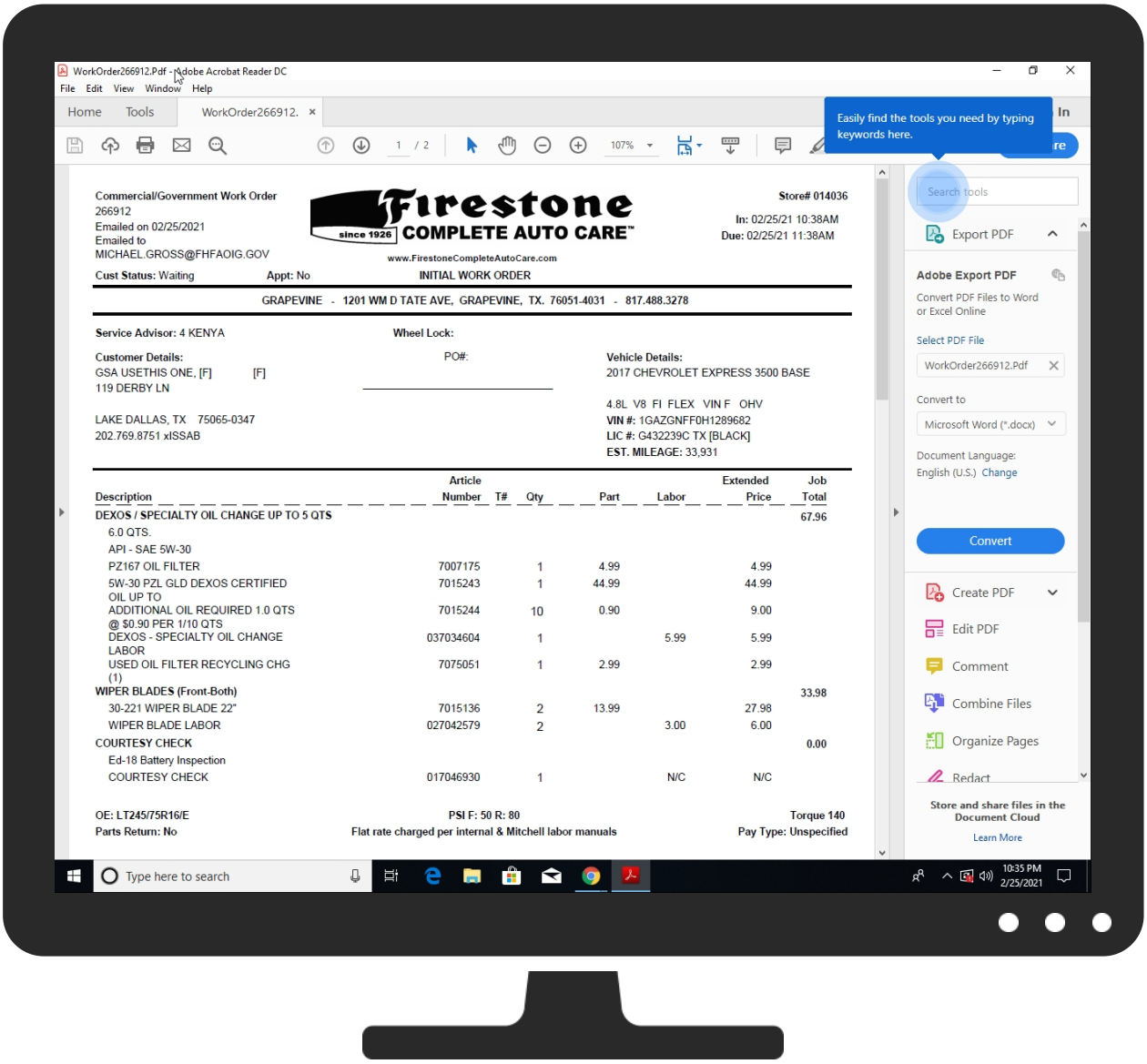


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://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://cipa.jp/exif/1.0/1.0/B	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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/_=o	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/d	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/7?z	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/?	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/;	0%	Avira URL Cloud	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/y	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/r	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://cipa.jp/exif/1.0/15)-	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/)=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

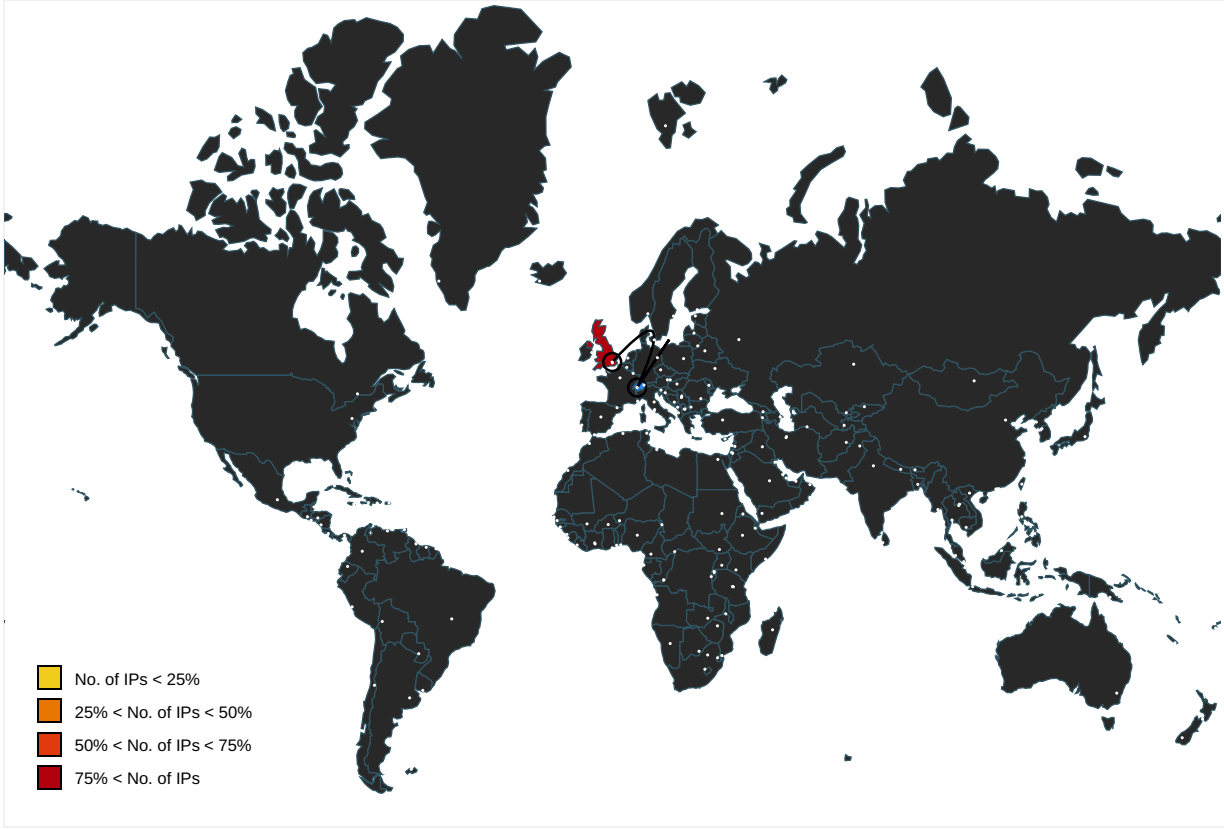
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#C=K	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/1.0/B	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/extension/G	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.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, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/_=o	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.firestonecompleteautocare.com/maintain/service-warranty-options/	AcroRd32.exe, 00000001.00000002.369959625.00000000099AD000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.380362308.000000000BA9F000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.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, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#M=y	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://https://www.firestonecompleteautocare.com/maintain/service-warranty-options/q9	AcroRd32.exe, 00000001.00000002.379625969.000000000B73C000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/d	AcroRd32.exe, 00000001.00000002.380171570.000000000B9E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/7?z	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es	AcroRd32.exe, 00000001.00000002.379744221.000000000B7DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.379928372.000000000B953000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.380171570.000000000B9E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/?	AcroRd32.exe, 00000001.00000002.379744221.000000000B7DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/schema#V=	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/;	AcroRd32.exe, 00000001.00000002.379744221.000000000B7DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.FirestoneCompleteAutoCare.com	AcroRd32.exe, 00000001.00000002.379858066.000000000B8EB000.00000004.00000001.sdmp	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/y	AcroRd32.exe, 00000001.00000002.379744221.000000000B7DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.379744221.000000000B7DE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/r	AcroRd32.exe, 00000001.00000002.380171570.000000000B9E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.369705799.00000000097F0000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/15)-	AcroRd32.exe, 00000001.00000002.380580150.000000000BB32000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.365171695.0000000008020000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/)=	AcroRd32.exe, 00000001.00000002.380120215.000000000B9B6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358603
Start date:	25.02.2021
Start time:	22:34:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WorkOrder266912.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:	34
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, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.42.151.234, 13.88.21.125, 104.43.139.144, 104.43.193.48, 52.255.188.83, 23.54.113.182, 23.32.238.129, 23.32.238.123, 40.88.32.150, 51.104.144.132, 23.218.208.56, 92.122.213.194, 92.122.213.247, 93.184.221.240, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, 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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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
22:35:37	API Interceptor	11x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSIjf0v9YP9XHTo1mHg1DdlnrlGItn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	vUp5vjYOoL.exe	Get hash	malicious	Browse	• 80.0.0.0
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	• 80.0.0.0
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 80.0.0.0
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 82.12.157.95
	wEcncyxrEe	Get hash	malicious	Browse	• 213.48.143.199
	Swift.pdf.jar	Get hash	malicious	Browse	• 80.0.0.0
	0001.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495.jar	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 80.0.0.0
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	2EB0.tmp.exe	Get hash	malicious	Browse	• 80.0.0.0
	muddydoc.exe	Get hash	malicious	Browse	• 80.0.0.0

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	820
Entropy (8bit):	5.702853564385404
Encrypted:	false
SSDEEP:	12:vDRM9k14O5ZiEADRM99RZiEAhDRM9qwNZiEznDRM9r+KZiE:7XyOCE2BEA1znEzDbXE
MD5:	F15C8FA919D1D632FC5A3736D60DF310
SHA1:	7FE418A73616EAF728B629E20A4F06A6590A095E
SHA-256:	C5AF14E4C8B457FE7F029A9245DCCB47A7A14D747C701385E0E791C29D213755
SHA-512:	9D850293D3ACB052485F02BB0E8FC8976D07117375E8CB7C5B471ADD620FCE927190A18FA1609EB53D8CC8BB8811C87F3DBE4C16A533E9830305ACF97861AA1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../....."#.D...%..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....kC.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .0...../....."#.D.5V.%..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....DC.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .F+;.../....."#.D...%..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .;R[.../....."#.Dt.k.%..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....>.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	5.649344820207252
Encrypted:	false
SSDEEP:	12:V9zwM9PQt9zfYUR9PQK9zmz9PQBl9zAUE9PQp:XzwM9PQPzfYUR9PQmz+9PQBnzAUE9PQp
MD5:	A3082015715255EB6F01F416F91C3FEF
SHA1:	55EB06120E583BA7594305C742083E1ED8A6EE38
SHA-256:	06CE19918916D17F3482B53D021E777AED7F87157B515550798804BDC7A3BC93
SHA-512:	84F960833FFFA5A7069700740B3FA3D8D19D8195C81B44F069BAD3F220985EB6615776DEAEF5A2B4384B87C1A4E6448EB6442CFD79E58C14EBF6FFF7077198CF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..4..../....."#.D.Pa.%..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....I>.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../....."#.D.`..%..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....+.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...,.../....."#.D.@..%..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....b.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...K.../....."#.D.!.%..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....$E.....

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):	5.630813091281461
Encrypted:	false
SSDEEP:	24:tB4v48gTQSBJB4v4fdXSBjB4v47SB1B4v4J0SB:nMCkSBzMKXSBdMsSBfMw0SB
MD5:	D92B78A1CACBBD5CC6D6C0FFBC7F7CA9

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
SHA1:	A20D15D421B4255FFB48FCCF4A62E9D54DA64DEB
SHA-256:	375FB70B7A98FD0FC92314B0520F70C94090CEEAC2F807B511CF46DA5865F816
SHA-512:	1B7F185728A052CF7DFAF017B1042B51526FBBA6AD596A282ABDA7C761C3A7E2B293BE9CF865A7B61ABCA4F8778ED7495AB4CF64BED80AC621DDEE24DA74C6D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...../....."#.D....%..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....Y.v.....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.yM.%..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .+.:.../....."#.D.H.%..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n..... ._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .K.Y.../....."#.D3.c.%..A..hvDO.N.t@.....n.*..... . ...A..Eo.....A..Eo.....\00.....

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):	5.6618326211552334
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsZAlu0iWulHyA1TK6taeNtVYOFLvEWdFCi5Rs9v90iiWulZ:IbRkiDShFWussBbRkiDY90nWuss
MD5:	1E8DACCC10AD5755A1AB46D6E455042D
SHA1:	BB3251D1D2A11258BACAC4027F509C8B3FFE1D25
SHA-256:	0AE26D439F58FC27306879ACB6B8CAF1AB4FBB9C081635848ACBA4607D86E3B1
SHA-512:	56C83E7EAFBC758B8B29EE842130023C800C97E4A3E47BB32D41369BEFAB4385FCE2C0C4F8770EECBB3016B91700A61D0001D24D868B2A2BED43E4DB3A3532D9
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 .tJ..../....."#.Dp...%..A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....s<.....0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...?.../....." #.D...%..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	420
Entropy (8bit):	5.613586160081458
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu/JmIqFVyh9PT41TK6tkS+yiXYOFLvEWd7VIGXVuQVVyw:pyixRuJ8IqFV41TEgyixRu4V41TE
MD5:	8A4C5ECDA56FF81745BEC3079282A84A
SHA1:	7E27655E45D7FD5E5291A7B640A7B05A9D979828
SHA-256:	6057292C3FD07406A7FA2FCA12C984C5A0AC7BAB164ECDA7C3C2DDD39921D8BB
SHA-512:	72105D1986C038B642F4B84B7278DA1DE49002CCA190BAD01EB47B0A9B9359BC2F3D34D92D67E1B9AAE2951326C58FA370A3BB4613C993680E2632D3C0E2DD4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...../....."#.D.mO.%..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....}.N.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...Z.../....."#.D.wd.%..Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....a.W.....

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):	5.630015898594734
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQBPlaxbNLZIl6P41TK6t02vYOFLvEWdhwjQlzK+bNLZIl6P41TR:0RhkS0xhLZClRhkWzthLZCj
MD5:	6848878A62057791CBFB5BA179795FA1
SHA1:	569DF53EC71B8CE71CAA46C010B73DA931C427D4
SHA-256:	421F9FF4799739525642E3BF8E6C7E7088E0C67CFBAD4B80BF83806FF59A341B
SHA-512:	1B1C3C8DB596D424D2FC74B8497EC680604A3A6B61BE54C57532A2C82DFB684F10A96A6E34236F98EF0721642EF3624ACC36C93ACAE1B4B48A767B19715EB99
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...../....."#.D..7.%..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....a.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...W.../....."#.Dc.S.%..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....b.?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.556401289115315
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQfBoeF6g1TK6tdMJYOFLvEWdGQRQOdQEVQrsF6g1TK6te:2RHRQCQ1oRHRQClV91c
MD5:	977BE73E89FDFFDE93A7512AD3AD74ED
SHA1:	A5FB098183D14F447803F3AF6219BE27DC246D47
SHA-256:	A7C36445BBF0CD841E7724BC974E0F7497691469803A80D0FE21E35F04D8F079
SHA-512:	ED32CE8E8289C27F7A835D8A652A0E0ADFC55171732E00C91FC520DF7089FBBFF50E97421823654696348FE201B2EFFAEFF1E94F75350E58852A7FDA34B2DAC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .b...../....."#.D..P.%..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....UI.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .n.Z.../....."#.D..d.%..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	716
Entropy (8bit):	5.658219524511903
Encrypted:	false
SSDEEP:	12:Z5MyKMuR/EX5MClZyMuR/ER5MBLUMuR/E0r5MHEIMuR/E:ZS8uR/EXSClZruR/ERSVNuR/E0rSH0um
MD5:	BC89FE7B73B9B16116BFB65D33059411
SHA1:	8123E4D994BEE75FEE4E1D8CA9FDBD12A186B0DE
SHA-256:	2FD22FCB0FC53775C54175DC10D980F86199527B6FB037D69676B0B98B1706F2
SHA-512:	33D5AAAC9A5023759A6DC89C942D73FDE73C8B57125AD8E5F6B54E8A3B5201715BD2FAB865741E5448C89D247D27E891B1FBF7CE479382E14DF403FBF86B1B7D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..8..../....."#.Dj0b.%..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....h.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .c...../....."#.D....%..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....$.x.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...,../....."#.D.U..%..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....o.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...K.../....."#.D .".%..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....Xf(.....

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):	5.5867936642415215
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuB0HCbSm0bbsIDMGH41TK6t:XfRM4i9KsIZE
MD5:	2EEA73043B4F013383474177C66E65F0
SHA1:	AC9EA094A5A8046B9D5B4CE02776E6A16E85DCB7
SHA-256:	4B57EABD93B30739D91E0BA08A4677E60844D83C3799A9761EC11E9BCF6FAEF2
SHA-512:	53B003E92A9775F7D15C1CC196DD6F9DA7C34BB3FB77F1530EEC444727A0790CF02DBEDE5B2E5789EFB0DB9979C7E9EF1FC60A1F82353680625ABCA713BE3D2B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ..C..../....."#.D>ug.%..A..`.....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Size (bytes):	428
Entropy (8bit):	5.575696029231625
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuASMby0zBUKSAA1TK6tp24fPYOFLvEWdtuYBQPMby0zBUKSAA13:pRHpbe/ZRdB5be
MD5:	06CFBFED4C10913A0FA1F8AEA4396C55
SHA1:	82BB21F04699D7616A61EDF8DB71338A3B92A674
SHA-256:	C88187D8AD32336B10DF6111C07381A969C5CA411291D53F9689E1A505C52ECC
SHA-512:	70C3D10D03517540B9C5EF37BFB1536CD666514AED289B49E1A1B75C18D03FF3E5B92DF8C7C2361CDBC9740069EAE0CD96F66EB21B7A18C642EB8EBCB88AD8C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..{..../....."#.Dz.R.%..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .Tr[.../....."#.D..d.%..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....8).....

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):	5.597791481868103
Encrypted:	false
SSDEEP:	12:KkXxKMSCvcfwvtUlEDkXxKMSCv23vMvtUlFCkXxKMSCvkvtUlHkXxKMSCvzWvtUl:KkXxiCcwvWEDkXxiCwvMvWIkXxiCMvWU
MD5:	AEB3E1CC2C327A86611E8768D33A72E3
SHA1:	CE0190D03BD4EC82ADB16ED1BD5AD47E5F4A8409
SHA-256:	BD703301116621DD8DE49CB59CB8DD253BDFD237F20C687C58BED780E5EF07E1
SHA-512:	2D922698FEF35C73004A0E8EDDCA8316BB95BEA457CA8D7C4B38691BDEC8F6C82219673DDF9646D90DCFDFC9107BAB719F2E4BD7318EA57AE00F9096DA2007C
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..6..../....."#.Dt.a.%..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....i.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ...../....."#.D.n..%..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....jK.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...,../....."#.D7O..%..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....&[.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...K.../....."#.D..!.%..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....K.....

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):	5.613683014140373
Encrypted:	false
SSDEEP:	12:5h6OLWmYkJHhh6OLYx9nk7h6OLBixdklh6OLxniXqk:5h6faJBh6K7h6jxylh6t/
MD5:	F551619D481A24CB4870F37B5BD57486
SHA1:	CC2EF2ED0C39416E8BE60103ACF43C537A70D368
SHA-256:	E05B757DEB7805F7ABB600B6C08D7984C10EB61FB522EDB6E7D5D7F4F72E4EB2
SHA-512:	0F2FA257C01CB7058EB2A3182AD71EF5F041E9C8C24FAAC118B810CA46A37E6D087136104F47FD2639E6BE5C438C3AF2C8BE0EE87BD83218FFB7D52688CA2A3
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .N...../....."#.Dj...%..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....qs.\.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...../....."#.D.^&.%..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....v.Q.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...7.../....."#.D"O.%..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....r.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..<U.../....."#.D.4H.%..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....{0F.....

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):	5.673351546700998
Encrypted:	false
SSDEEP:	24:UB4v4EXwzXLn+B4v4HwzXLn69OB4v4ywzXLniOB4v4CwzXLn:8M6bn+M5bn69uMybniuMObn
MD5:	1246DAB05BD503DDE7873D7BC78B039E
SHA1:	1F4DA912B483EFCB00F52C176834225F5BD3D643
SHA-256:	830FA9EEF3FAF302933939ABFF14A03DBCDAE1B93CA4857F3E06B4CBCC0A1A3B
SHA-512:	2BF3D199A87D36D1D0B1394318874BD57EA30F8B9160BE94DAED63BD5AFE084C0665D3E12BDFCD5AFFA2EE0FA1CDB9E80B52A612FA60A86B2CF5EC916C2CABAD

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
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 .>...../....."#.D....%..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...../....."#.D.}T.%..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....c.....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 .Aa;.../....."#.D...%..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....*..@.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .4.Z.../....."#.D5.i.%..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.548494684794388
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQPpNel5GFCaa+41TK6tL:NRMHdKe5Gda+E
MD5:	5A8EB326CBF83FAFAF4092B39E93F774
SHA1:	3260693D9FAED381F35694BE86804283806A6CA8
SHA-256:	3B4AEBD78BEBDE5EF706A75580441ACFC013F4D9D703FB2E088C97F52F4E9785
SHA-512:	FB7228A184B81B20BFBF48D1D47FCB5D030EFD2F65862F1A68C2BCFB0F4146F9B1DA78D9607544B73F8C4B463DDD78C4407D71DCC6210CC2CA09B33EF55C51 8
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..D..../....."#.Dl.g.%..A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....]Y.....

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):	5.533377421900329
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXudt11TK6tFs2VYOFLvEWdvBIEGdeXub11TK6tD:BsR2EsecTYsR2Ese2
MD5:	B49BA2F8954C84A049FA1FF408956794
SHA1:	2038F22A980144108F81E6A6349F210F5B30B122
SHA-256:	4193A19D1F1A07B4456B725123130ABF980D3E94FEA624D8123BC918A7613FF8
SHA-512:	E45FFD288BCDFC700FD21B00F00653B06AB78FC36C21C1A134362469ACEC80A300AF0F418862C6253148F361489739195728F54005C83AC2EA727CE457B6E14A
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...../....."#.D..N.%..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....a.8.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .-GZ.../....."#.D..d.%..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....X..v.....

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):	5.703282908607747
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQT+Aa4B7OhKlvA1TK6ttaVYOFLvEWdwAPCQ1344B7OhKlvA1L:RbR16aq4BJkmbR16k344BJk
MD5:	6C51A53027CA4C3E4787352493160B02
SHA1:	7328A21193E8F6C8A9819C9F83324FBF1189EE4E
SHA-256:	AA039ABB9F4D1458818160497C3E5FAC8E4F41BF2F80E6D48990FC1063951BDC
SHA-512:	A270100D8CDBA1D98E3B1F4D25DB673E7919981661C3998FED99D014E1872AF484588B2A895E03729CAF471F4507575AB4128BE118B430C0A7D64D728CD50CDI
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D.[7.%..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....!(..... .0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...W.../....."#.D,.S.%..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... .....

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):	5.60865952405145

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuZwKpFrGuQdFt1TK6tzEs2gEYOFLvEWdGQRQVuv0QdFt1Q:B2geRHRQU3rGu0dT2geRHRQq00O
MD5:	070A7185B6FE641AFA66C21BD860ECA0
SHA1:	FAB89CDB8E57F6075A789F5041124CFAA3769149
SHA-256:	3EDF072590EB65DAED7BEA5CC250394A8BB75AE31018AE899D14FB4ED0EFB289
SHA-512:	19CF045C257DF99C7CFD1C20A57C2E0DEDF0E8986DCE285454825BF3E0505D32FC8B3A0B3B24C8F73F75A6E6B0521CE47CC5419052512898FF7C354ABD4314
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...../....."#.D].M.%..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....FJC.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..EZ.../....."#.D..d.%..A@..{o]...9o|..qY....T....{.. u.b..A..Eo.....A..Eo.....J.....

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):	5.632981953661476
Encrypted:	false
SSDEEP:	12:WyeRl16t1w4yeRl7g6t1wK+yeRlLd6t1wwyeRlyb6t1w:WJ96fw4Jc6fwzJJ6fwwJqb6fw
MD5:	D5636FEEFEF7586C837A8D633610EB4F
SHA1:	D5A3BE5B4E2E0175CE2302B20C033D2375A8FB53
SHA-256:	EBAD83797939C8A8F2A916824FEBB359E3D9A04BE2A2944B59FD0131B48EA06A
SHA-512:	864F288CAC4447D46977059BA0E7D20498562CEC63FAF3B54EA3CAFF5E796B1C42925E179683C2B0CAA1BE980A5C5AF1AA4D78224CEAEF417F59D2E5BADEC 2A
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .u...../....."#.DkE..%..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..%F.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .fx.../....."#.DjL0.%..A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....;..g.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .. 9.../....."#.D"..%..A.t\a.....x5.'OuE.C..@.....x..A..Eo. .....A..Eo.....T.0.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...U.../....."#.D..L.%..A.t\a.....x5.'OuE.C..@.. ....x..A..Eo.....A..Eo.....c.u7.....

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):	5.602828222393186
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuh/fCZ4rqwK+41TK6tLHlEnYOFLvEWdhwyuD3fSvwNrqwK+41TM:wRhKNGwK+EKRh0vSCGwK+EC
MD5:	2F2102A5979B6BF9074663165802C102
SHA1:	C6DB4BCAB9255CB286C05E128C7025AB40EA4FF9
SHA-256:	11A22ACD6FFE59D10C882FDC8797BBB15EA6DAE7089B29494BBD1EA831B6602D
SHA-512:	8D2D2FE773930B1E6DA3C78F41A2D3F4259C9730D8F4DC49D9EDED5BCE71694C2A0F8B85373F4033880A2C8339C93082D2D30FB663E5B6ECBFD3A299925E01 E
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..A.../....."#.D.77.%..A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..EW.../....."#.DByS.%..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	920
Entropy (8bit):	5.658615078449104
Encrypted:	false
SSDEEP:	12:/RrROk/VfArKlfLEvRrROk/gK/dfLEiNRrROk/WzHfLE4RrROk/2fofLE:/PJ/VfQ4vPJ/74iNPJ/sH44PJ/2fo4
MD5:	4DBA93E15541398DB8C21DE9ACA6D117
SHA1:	6664D9A3220912DD2A91A9305976955CF13C7394
SHA-256:	09A51CC67CAB945D1CCD443D4B2E3AF774E33585CD002B6237C2112A9002DE02
SHA-512:	98E59BE4C618A064087A61E1147C55CAA50DE42EAA64578960955FD8E66190E5F6C5C9522E42DBB638DDA268F565C7434C8D4C16FC6B46F9EED75FB7CFEB23 B
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...../....."#.D./..%..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..'..../....."#.D./.%..A..~..rw.+[.... !.)?..f.U..(=.=.A..Eo.....A..Eo.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .s .8.../....."#.D...%..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....Cy&.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector- files-select/js/selector.js ...U.../....."#.Dk.L.%..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....B.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	744
Entropy (8bit):	5.649487092005681
Encrypted:	false
SSDEEP:	12:xqThKGG2KCPLnt5qTDD/KCPLnRqTNqKCPLnZqTUQ0CPLn:A1KGG2KMntI3DSMnghdMnoAMn
MD5:	91C954433C488CB0F701A548F5DFEA16
SHA1:	A57A2C34AA9996C547E6E4BBE019C71CFFFEA0DD
SHA-256:	2065359553CDB37F9BB06201FDDFAC4D8668918D5E0AB72B2F02DF4BEAD357D5
SHA-512:	CF4D700AF21B4BC539959CF534A2DC4C12B0A86CB43CC54ABA98B0F545FD2484207EDFF402F95D2D9980AEE37C9AB18341EBC48B8ADE66F597524C86010F12C
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...../....."#.D....%..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....~"_.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...../....."#.D..&.%..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....t!.....0\r..m.....:....f....._key https://rna-resource.acrobat.com/static/js/config.js ...7.../....."#.D.G.%..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....L.....0\r..m.....:....f....._keyhttps://rna-res ource.acrobat.com/static/js/config.js .`0U.../....."#.D.(H.%..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	828
Entropy (8bit):	5.692783165241261
Encrypted:	false
SSDEEP:	12:zRMWsD87RMCKOAsDpRMmP/sDNsRMmsD5:zQD87NrDpWDuoD5
MD5:	8829FD84E29D45E132519F3C6BC89C62
SHA1:	095DF4CBB15878D517CE99DB79BFD9CA71771634
SHA-256:	5D6FC59A0678D5624A4B47B69ACE7260206195969F1585D9CF6878965E78C05D
SHA-512:	F6942E02B664F30F7BC10FD7B718493F5E59713C74A747A4778D62327CB2D9EAB80623BDA0D85D23E21E57AEC57E7D2D0EAA2934F25189FE34487437EBE6C2D
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ._)..../....."#.D....%..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ....|$.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../....."#.D..N.%..A..z._a...'.v.....4p3..1.']...A..Eo.....A.. Eo.....g.w.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .X.:.../....."#.D...%..A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....E.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .'KZ.../....."#.DWBd.%..A..z._a...'.v.....4p3..1.'].. .A..Eo.....A..Eo.....ba.....

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):	5.660613113256624
Encrypted:	false
SSDEEP:	12:6lJRvFoMUlJRo6f+FoMRlJR/hFoMixlJRPFoMhv:YRFoMyqRFoMFzFoMiltFoMh
MD5:	443AAC3E13A5F6CCB115D5A0AEFE0D91
SHA1:	955ABE1BA6306DBA706DC5535F9932C2A5703047
SHA-256:	8BC914AEC035C8192789214D2D15691DBFFBBC97287DA6509555647BC52EFB3C
SHA-512:	7C0BA2D24FD4E3D2CBE96E0E45A53236ABC7F5EFEF431309D8CAF0F25F436D38C927DA4AF75013568CE10C28B0B8C8E040CFC09F336B1BF8B9B61C1F3A75FEFC
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .7+..../....."#.D....%..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..E o.....~.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../....."#.D..O.%..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.... .....A..Eo.....=pj.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...:.../....."#.D+0.%..Ac}.H7M=M..-.....Ix..R.l. ..}Rl.$q.A..Eo.....A..Eo.....0.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .{QZ.../....."#.DiUd.%..Ac}.H7 M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....N.].....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
File Type:	data
Category:	dropped
Size (bytes):	892
Entropy (8bit):	5.646280123703268
Encrypted:	false
SSDEEP:	12:F8hRrROk/kVe2Vz8hRrROk/xJYLe2w8hRrROk/Fde2v8hRrROk/jJe2:UPJ/52wPJ/xSq25PJ/y2aPJ/A2
MD5:	6D69754E2158A7C89B38DE9C6DD69E91
SHA1:	0E8BB987394FFDD77EBD5AF36ACE73677F4050B2
SHA-256:	3636592C99765B00CAD0B5AE70E9B62E1B619F66B1D3BB4B6564AA8D5588C275
SHA-512:	77A66B1E585A4B5A8C2BE391FC02339AACEE8BEA97FFC1206358FDA08EE3B9F11EB7203A23F60767D5FC79327B01A37471B1A299795E8028A5A8479BE5DDCAD D
Malicious:	false
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .|..../....."#.Dl$..%..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 .."..../....."#.DB./.%..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....N.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .D.8.../..... "#.D"..%..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files /js/selector.js ...U.../....."#.D.EL.%..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....w.....

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):	5.716650746960152
Encrypted:	false
SSDEEP:	12:ehRc+frNJICmhRcmo8rNJICBIhRcLrNJICVhRcwfXrNJIC:ehxRJICmhcAJICKhOJICVh/JIC
MD5:	AFF33AA719B072E0B563965F66D03FEB
SHA1:	F4A72857834A87E7CE77B60F36B228E148F9F671
SHA-256:	842A09D3096967B70E6D88B1434D18546D1A36313695D887B2422BFE490C6491
SHA-512:	2EA6893869A0E48F9607D34A421D0EF22603FF06BC9504F6B876B0EB09D3482BA40EF1002982A651EE1A83EED063669DD81127A545BC7B13CC54B313C605B565
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .w...../....."#.D.h..%..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 .R{..../....."#.DC.0.%..A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....k.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .."9.../....."#.D...%..A.;"./N_.,.:C..2....9L.H... 3:...A..Eo.....A..Eo.....f.c.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...U.../....."#.D..M.%..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):	5.638395355297835
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu6oUZLzgm2d/1TK6tMh/2OEYOFLvEWdrIhuEBllSOZLzgm2d/r:0Rk7ReuhcR2TlnRe6R8wORebR9DReX
MD5:	A8C2834581D82CBAFCBEA8463486E052
SHA1:	414AD4CD86CBB5C8FE19F2C8ED2D5B9A45BE8350
SHA-256:	2C027D82332536A0795D06DB284E50689DCDFB02EB2EC964A81966EEB07E5462
SHA-512:	4AD711F4BC9FFF469C90C9F45212CEBE9C03401E3AAEF6507081C69041A728B7B4255B0A44042BEA2511E81868262DFEBF84858F33597770F84E225201D6272E
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..Z..../....."#.D....%..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. .....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...../....."#.Dy.-.%..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A ..Eo...../.c6.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .{.8.../....."#.D.x.%..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....N.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..U.../....."#.D..L.%..AZ.Z}Q..4.o....0+..[|..n:*. .U.W.A..Eo.....A..Eo.....G.....

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):	5.665340340195915
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KW9kOkx56uvp1TK6taHeAElVYOFLvEW1Kv2ekx56uvp1TK6tKAv:6JJKW9w0CJJKOF8JJKJ7JJK1+lg9
MD5:	618284E1BDDDAB9173DE20C85F2A68D2
SHA1:	EF5AF0372C337AABC4D07832C32DC8ABDD59BF35

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SHA-256:	D66B6BF44E51DA38AB14E31804999EE7725C20AE7979A64B3BF69AB3DB2C39D5
SHA-512:	FA19A76F810C5109E0F30F4E56D30F78E0C4441C4B06C148B5F04E86E43E68BE5D7B2FA941782C094C559E7958FA290D3B8E39C84BB9A1CB023102349DD3FC2
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D..u.%..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....yd.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .. ..../....."#.D.t..%..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....:n.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D....%..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .E.M.../....."#.D..2.%..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo...../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.659255623765122
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuVc7hUDLYtmOZn1TK6t7WYOFLvEWdBJvvuaAcYvhUDLYtmOZnH:xRBJ2lDcFZLORBJgKDcFZL/
MD5:	AEFCB2C37EC358CF5F72EDEC11DA7B57
SHA1:	0088D9598FFE4833551A564AEBFA0DB30C5A2895
SHA-256:	376084631D67E8ADE47CAC4AC3AA49E4B5E71A03310974DBB2C5318672049AB1
SHA-512:	96C84DC03DC65E37637D6B5E30D02A33D6EC9189376673D6018A756B158749A2177AB55C2CB4857B787908F737BB72BC7757D799D9B65676572F571C6B0297F5
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...../....."#.D.NN.%..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .CHZ.../....."#.D.%d.%..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....W._.....

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):	5.649025551040199
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp73VPu1TK6tysRPYOFLvEWIa7zp7ouXEVPu1TK6tTsRPYOFLu:BPHFc3PH2kEcmPHfoLc35PHi0cd
MD5:	EA33A9E25392371EE9AB24D991E65801
SHA1:	D29C63178588E507F8A01FA00ADAFE115CA26A45
SHA-256:	CA62348220CBF242593EFA4112386297375E24D1A52CB9885302700FBDF4737E
SHA-512:	A10AEF39A9D20D9B8D0C6ED322F9B48EE91B88371000E8DDD0425F2D9FA6228F9727DD604AC5FB794CF393FB62CD956B914DB05F7989BCD7CA57E457B6BCB32
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..G..../....."#.D.]b.%..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....wr.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.DG...%..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....ID .....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...,../....."#.DZ...%..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....7@.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...K.../....."#.DP7".%..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):	5.6331452726507765
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QM+WLUlowiM3Y1TK6tneKPYOFLvEWdENU9QYznlowiM3Y1TKJ:bJRT96WglPr0JJRT9VZPr0l
MD5:	97A37733C7F522F0008824E77DE2C3D5
SHA1:	E064E2585DAD06CD3E0499AA522A28D7767DE016
SHA-256:	4842E15683A1446E663571E74CEC3EBAE02664AD9FBAB85C3DC8386880D7782C
SHA-512:	F7E71854914B0F334AC78980AC5C16D41F95694F988277139AC22BA8D2E7BE016B42E69F677405994513D199D1246E24E9892A05A88A9B68A5B496FBE0413EDB
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...../....."#.D.h<.%..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....I.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..W.../....."#.D..V.%..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....^..7.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.6552551839129
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQSUzjBRCh/41TK6t+Qt6EYOFLvEWdccAHQWBfX2jBRCh/4K:XRc9xcDi/EpRc91v2Di/ES9
MD5:	0D016B100A57D4B79BACDC1455BD70D9
SHA1:	2513E517CAC37C646C17862C2D492527C9175E9C
SHA-256:	7DCF27CA8CE1779BB8A64870AD51F7BF9FF4572433BDAB72E47CEDBE2E87E5FA
SHA-512:	0660EE849FC6B9DD09DB69EF9FFEA848925569B954F18B8CAE4FC3BCABAEBC1D1EFFF879D6A36094A9F81DE035B8E37218B02F5869DE9EAA5FB252FCB08A98EF
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...../....."#.DJaX.%..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....Of.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .O.Z.../....."#.D..m.%..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.627787413680547
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuFQCD69DVULlF4r1TK6tEEqs6XYOFLvEWdFCi5mhu901R:bs6xRkiQCOt2LlF4nGs6xRkiJ2LlF4n
MD5:	447DA4B1D01A5FA915120B6EE8A119CA
SHA1:	0E04AF8963A66B6F14E7CA90775A86C16D0DB422
SHA-256:	D5127233D8B97BAB327C77372071509722BB635C5FADAD16FA9691B266CB5A02
SHA-512:	03220AC6F372F348D1B520687937A5726F745BB1A830FAE199C6EEF7C16C1DBDD405EC02FEB885C17E65D50D09307D0BE9F02558EC52BCE67CF1E98347D91A3
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..Z..../....."#.D..%..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....u..U.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..J9.../....."#.D..%..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....ky-.....

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):	5.572878252933503
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuEXKaB/N941TK6tgH/2hYOFLvEWd/aFuDk/8N941TK6th:WRIKY/N9E2/mRtk/8N9E
MD5:	41C66CB5B6AF3FBB039D515CE3966A8A
SHA1:	E852A2D36F7E658F9AF8B7D24CBDAE948DE3EB92
SHA-256:	3528908F03EABA6F8EDA743A3F5AF6AA08F07DA2B1265218C9A28FE0DF52AAA3
SHA-512:	BC9F35467F7BE28BDA6F36DE3925FBDCC8302E544D8DB816A31A7B0542951F1C54D6760658C0BA517E8EAA1301A59486EE3230E210D166CF951EBEF77B6274D
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...../....."#.D.(R.%..A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A..Eo.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...[.../....."#.DO.d.%..A...a.f.m.i.o.p..3U5....^...I.A..Eo.....A..Eo.....f0.....

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):	5.566227475510162
Encrypted:	false
SSDEEP:	12:2DRuRgQyB9Vd2k8ODRuRlT55B9Vd2krH:8GSbdT7sfbdTr
MD5:	492FE35F726020102CC7181E98867A27
SHA1:	FEB0326A5BAC98A05CD45F8D83CF03D41BFCD9DF
SHA-256:	81251CC8E08CBE32187D31EB70973AAC627A92101B84808F0CB21255D11DCDA0
SHA-512:	E598688C71841FD614476A97CA558684114281E7905BA6638260991827D192D837C197E4BD29F68314FA3624383E1F775B3536079C077871CC241510E5D3B153
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..V..../....."#.DqXP.%..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 ..c[.../....."#.Du.d.%..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....O.S.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	832
Entropy (8bit):	5.663537567109709
Encrypted:	false
SSDEEP:	12:+RQaXsrnTRQornf2RQuPEJrnYuRQthrnG:+HAnTJnf2ydn7Sn
MD5:	A519B2F09351FAB52D5FBF23EF260481
SHA1:	122A324A5448EBA2802001D09F7481A15869F0DA
SHA-256:	9810E51328DD4F0D5248C492F789BEB7DB7A1265937DD893E7C9383C0528C183
SHA-512:	D573D6220781399B719FC3572EC84DBA21A23F148E28E0D9CBF2A8899087D7D7372123F8CC2854CDF2D04B8105D949DCC27F1505C0171925F951BAD579F2AC0
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...../....."#.D#...%..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....C.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..L.../....."#.D..Y.%..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....Ra5.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..,;../....."#.D...%..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....mz.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..T[.../....."#.D.qn.%..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....M.w.....

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):	5.600109661134812
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAu/l18yC8n1TK6toEoXXYOFLvEWdENUAuu1iaD2XS/yC8n1TD:xhRTi7QghRT2Rqs7Q
MD5:	F2247B5A25A313B2A62E83EEFF502875
SHA1:	A16F121CEE9FA7FE3118816868A8C7E62B6546CF
SHA-256:	AA8D996E7077A9DB76D165F96A8FDBBF57A7E43F7F49E3C8C6DBB33846D43A86
SHA-512:	7EE9E07DCB51677B33FF9BC294F5E0B7DE9CC49DAAB3E15D8B2D1AAFCBE2E9A8BEFA34C46184FC88B27688E39EE13C32AAFEE1B451685497E71A3E63F89160A1
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..?.../....."#.D.$7.%..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....Y.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .aDW.../....."#.DReS.%..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....(.....

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):	5.68408864675385
Encrypted:	false
SSDEEP:	12:nRrROk/VDVm4fRrROk/VOpX+mtRrROk/Vym5RrROk/VmCqm:nPJ/64PJ/stPJ/h5PJ/0i
MD5:	A4D60963FDAAADC93A3081B6965E39F0
SHA1:	A78B974EA864433F7762AEA80E0CFCD2F8702C36
SHA-256:	0F57896024446FBDDC44E0DA8DE7F7B54A67C075EE98FBB32B7B0402103F64FD
SHA-512:	17B04C846F1AE9782DCF55CA8D234C370216D325E9EA99FF1DC3AD272EDC3AABE9E13B2B31AE1254D977417C9FB38CA7C7387EB0E49979EBB47F2A9A5950F192
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.....$.j;:C...A..Eo.....A..Eo.....a.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..~..../....."#.D..0.%..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....Y.*.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..$9.../....."#.D...%..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....)....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...U.../....."#.D.0M.%..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....S.Y.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Entropy (8bit):	5.614180682073117
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWusj/GAdm9741TK6tb2Z/lXYOFLvEWdccAWu3/kSaGAdm97p:qxRc+6Adu7EB6xRc9kS3Adu7Esf
MD5:	3CCB1391263E025F6355C525BCFA80CE
SHA1:	2FBA1731CB775AE81FABC405D9D3C917E7AF690D
SHA-256:	141E865F81BCFF3656B9DEE1D0FACBDBD279285DFDAC8D166A6A1E303DA75240
SHA-512:	A02B6960C3DB884CDB14AD246455E580FB71F194D40C5799DE9CC1E8C0ADACCBD538F7743ED5B23E9A4812C41508921B18313F11D5A2CD0C271BBCC61775D9
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..0..../....."#.D*.M.%..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...Y.../....."#.Dq.d.%..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.627214150828743
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuloCljV4Jn1TK6tPMOYOFLvEWdwAPVuofC/R+GHJn1TK6ta:2R1bCWLBR1cRpLI
MD5:	ABFB9A0FA446009D6A2FCC628E7D6AA4
SHA1:	1C6A394A846452CED23987165694136F068B9061
SHA-256:	BE14A793F1CD79547381FF563A65F5023BC08CDED5F8CA20C7C7DAF53B829F2C
SHA-512:	93265E566E30F29581975944FF79ECDCFF1F1317987DFFA95F024325EBA4213394F306CC56DBAB1576874747EAC801677704E29271F8550603E48E107BC04ABD
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .}=..../....."#.D..7.%..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....,p$.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..CW.../....."#.D.GS.%..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....(.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.673492783469724
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ7zhcsBXIh1TK6tq+3PXYOFLvEWdBJvYQnuoxKzhcsBXIh1r:mxRBJQQDB0k+xRBJQuxKDB0
MD5:	F27849590B7817E4221896AAF6E7C5C7
SHA1:	83A59D5C801CC07D1F3467E1B19339F4B57D9BDF
SHA-256:	42DC6A01977A94BEC396CF7E1F0CEB1117F3C0BACBAAE1AA0097E277C536466D
SHA-512:	F75235EACB22BFFE423FAC8A7599EE54AE176CFFDB4A484633D88BE83A229ED7199FD607D99413D0E93A7A388CAC0A8CFBF439AE51B9A1746E3C4730096E4A61
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...../....."#.D..P.%..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....r.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...Z.../....."#.D..d.%..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....D.?e.....

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):	5.655680805115209
Encrypted:	false
SSDEEP:	12:3RrROk/seHcDRrROk/sVlDcTRrROk/sIcldRrROk/s9oe79lc:3PJ/Z8DPJ/PTPJ/+fPJ/ze70
MD5:	6D960924C1CCD6F56580359848EF2F30
SHA1:	4B703636198DCA3ECF6D8C14387A316A97BE10D3
SHA-256:	5B84697B55D2F60273ACAFBB6FDA774683745FD245E3254B868758F6098F96FC
SHA-512:	97A238D72DD2EA7A20DF906D4C7A3B992962EB9E49237C29467BCD71EF895637CE46F20B1E75A42FE53D5F59BE36DD150539E3AE28D0598CAE2E0F66DDDEB05
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...../....."#.D....%..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....t.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...../....."#.DAb1.%..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .4&9.../....."#.D.0.%..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...U.../....."#.D..M.%..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....J.....

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):	5.267124425518569
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPmmnUplDTOTXTmrMlwid4XVZiCAwKi:h1zZ4+dsp6HmnUpQzSrSwidOwJi
MD5:	B8AE5BF695B578B96D7809684F456485
SHA1:	D8F7EBE0C9465CBA3140BD5B5B82FE74BADEDE71
SHA-256:	D894E668D3BA0FEFD0FECEA236D63BAA184FF401CEB24E1E27050211694A771A
SHA-512:	7DAE28E45919A72C004152CEE72292A631E7B59A1DFB142235C646C2DC515C8A24F3D496365505AC30430578F2F8402F08C0FD26D3669CB6D3C96C0027207460
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0....=..oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.193538256050488
Encrypted:	false
SSDEEP:	6:mNPfRXQQ+q2PWXp+N2nKuAl9OmbnIFUtpePfRXfdWZmwPePfRXeQVkwOWXp+N2nC:/Q+vaHAahFUtpAg/PxQV5fHAaSJ
MD5:	46E16951825B71DF4965DEA74E869250
SHA1:	4AB4EF9C9DFE23D806719BB3FED83775B6CE7C68
SHA-256:	36C4DD77662A8961F817B311F509D26EA1FB71525674276D074BD36D9A9AB520
SHA-512:	9C20301D8418B638E24A2D4FDEFBF178C841918E2263FD9910B445A4FB7720E03E616ECA5CBEFFF0665616653EAAF9A8AB64F8AE168AC061A1884C19729A28E
Malicious:	false
Preview:	2021/02/25-22:35:42.557 190c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/25-22:35:42.558 190c Recovering log #3.2021/02/25-22:35:42.559 190c 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):	0.010450311063861047
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDdsmWiDdsmWiDOsmWhCDTsmWhCDoDsmWhCDoDsmWhCDoDsmf:tFVFVAnfnovnovnovnovnovnovnovno
MD5:	C5320DB321A0EC2EA0AEE50ACE073382
SHA1:	2E3A5F1F8C5FE89B022C94BD3574BECA1445D34D
SHA-256:	10CB1245EF4F539D1B2E962879068A09BDCFD07FCEDB103F78A17338C73A6B22
SHA-512:	1FC54F5F46BFBF53AD1955165B9D246B1F351CA134578A028B118A3F887B8F72F710776A7FDF45731CE6DA20ED37FE07AE67FFD3B3236B845FC1140178C8D153
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210226063537Z-206.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	1.3239371267630786

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210226063537Z-206.bmp	
Encrypted:	false
SSDEEP:	96:GONs4ClCgPw7PJcMMMEMMMMEMMMEMMMR9jMQc8HkvtLMTfwS5I:pZTCgP4J3vX7
MD5:	EA216EBAE3DEFE301C225B735674B3DB
SHA1:	D457DDD7015E61F5CD55979AFD69450804437A1F
SHA-256:	CD84DF710ECA654F15AAD380D64B1DA80A08F689049D040288D4DC5216BF6134
SHA-512:	09360F8A6CAD1A624502DC21E4590809606A9C2703AB4BA650131467EF4D9C1C4729BB7E8417FF48C5CC934498B1D500CA34ECC7D75B7D9932874775DBAF4B9
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
Size (bytes):	32768
Entropy (8bit):	3.388046368530882
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQnOhFVCsL49IVXEBodRBkRfnOhAVCs749IVXEBodRBklfnOhVw:iGedRBpedRBredRBYedRBM
MD5:	69D46D5E361A0BC318CE6F1681231B4B
SHA1:	D6AFCD3247296E01F8B0CA69BD383F64A6B7C8F0
SHA-256:	5F1D7A143F6004EAAEFE02C72217FD3B207BCA06C79516A30FCB033A688D3D18
SHA-512:	9E409913AD575949A244D8EE0AAB637B5079AD2B268650DDE717F77267439FC696C5892E450234B724AB7B27B8341F5D9EED61BAF67F2615888D98D73A75DDD1
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):	3.2017981604678383
Encrypted:	false
SSDEEP:	96:D7OhFVCPD949IVXEBodRBkH8nOhFVCsgLR49IVXEBodRBkaNfnOhAVCsNd49IVXq:DviedRBEULGedRBZCedRB/yedRBc
MD5:	487F6C18D5A08392C271DE3D0433097D
SHA1:	E9E18904317BF4697D03D8B3D35AE7B90050C37D
SHA-256:	2E226B7B23B3F364D3ED4CFD1B9FF72DA334D4F116AE1D067EFF3A931C4730A6
SHA-512:	AADF891AC86F8ED7DC3159E2BCFB2422ABC325D98EC1A5084CBA75285BC0D57C042F1248BA8D4C5AD048BF13C909BF89960DE6828DFB32AA9CF5446DA9AA0F00
Malicious:	false
Preview:	.....X.<..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.3468	
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

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.3468	
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.973980781745228
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	WorkOrder266912.Pdf
File size:	337441
MD5:	2ebe035562b1a79e82f6446265068456
SHA1:	8d206b01c0bbd6a5c1f8e48bbb3d3f90f5f15498
SHA256:	685c6b3fc5b79f2375e0397190d5fd1da4e82193aad8a9f05eb8efdb1246bd41
SHA512:	6a9c0cae6684093ac930d372be0454f081bbdf57a00b1ed1ef2aee70720733fdf19de7a465c52eb09bcee7c2350c15d4aef372e648021227d8a3170e116ef20
SSDEEP:	6144:QHutiKabgBS1LBQbJ4nYFFPIW+4iKvV/YR+OJsL1fwomic5M1:SutiyBeLBQOnYFFPI0JYMpx2M1
File Content Preview:	%PDF-1.7 .%.... .1 0 obj .<< ./Type /Catalog ./Pages 2 0 R ./PageMode /UseNone ./ViewerPreferences << ./FitWindow true ./PageLayout /SinglePage ./NonFullScreenPageMode /UseNone .>> .>> .endobj .5 0 obj .<< ./Length 1868 ./Filter [/FlateDecode] .>> .stre

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.973981
Total Bytes:	337441
Stream Entropy:	7.975664
Stream Bytes:	334152
Entropy outside Streams:	4.916649
Bytes outside Streams:	3289
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	43
endobj	43
stream	16
endstream	13
xref	1
trailer	1
startxref	1
/Page	2
/Encrypt	0
/ObjStm	0

Name	Count
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

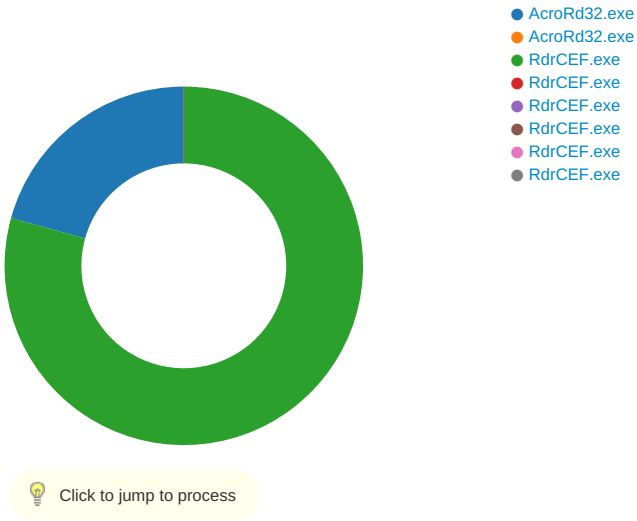
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:35:23.373473883 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:23.425183058 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:23.588741064 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:23.637284040 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:24.740400076 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:24.792789936 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:25.935245037 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:25.984261036 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:27.066452980 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:27.125526905 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:28.444392920 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:28.493303061 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:29.460150957 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:29.512005091 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:30.607872963 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:30.661221027 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:31.752717972 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:31.813262939 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:32.947957039 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:33.001430988 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:34.119849920 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:34.168889999 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:35.362503052 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:35.411684990 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:37.801177025 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:37.852890968 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:40.268208981 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:40.318483114 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:42.041941881 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:42.090845108 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:46.058219910 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:46.062726021 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:46.111917973 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:46.115781069 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:47.055397987 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:47.055474043 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:47.107248068 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:47.117309093 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:48.078428030 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:48.079278946 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:48.132689953 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:48.140396118 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:48.241543055 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:48.299060106 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:50.126945972 CET	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:35:50.127000093 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:50.178950071 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:50.180715084 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:53.679711103 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:53.728727102 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:54.136766911 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:54.136825085 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:54.189179897 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:54.192670107 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:54.937616110 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:54.989275932 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:55.789124966 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:55.838701010 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 22:35:57.389606953 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:35:57.441343069 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:05.552655935 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:05.613615036 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:10.471024036 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:10.530344963 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:18.581079960 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:18.629664898 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:29.219132900 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:29.296852112 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:29.802599907 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:29.882596970 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:29.928527117 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:30.003401041 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:30.422291994 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:30.513237000 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:31.018302917 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:31.075737000 CET	53	60633	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:31.570230961 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:31.627536058 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:32.162858963 CET	63619	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:32.212977886 CET	53	63619	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:32.822608948 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:32.889543056 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:33.780487061 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:33.871028900 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:34.747560024 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:34.807852983 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:35.255776882 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:35.318850040 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:36:37.465183020 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:36:37.525876045 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:37:07.714078903 CET	56338	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:37:07.762851954 CET	53	56338	8.8.8.8	192.168.2.3
Feb 25, 2021 22:37:09.505965948 CET	59420	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:37:09.581895113 CET	53	59420	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 2616 Parent PID: 5660

General

Start time:	22:35:29
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\WorkOrder266912.Pdf'
Imagebase:	0x13b0000
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	13E65C3	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	140AE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.3468	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	13FEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock2616.1.2885663546.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	1432657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	13FEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210226063537Z-206.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	13FEA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14783C8	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	14783C8	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	14783C8	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	14783C8	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	14783C8	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	14783C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rqa2te1_rk8k4h_2oc.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	13FEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	13FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1a7m3fi_rk8k4i_2oc.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	13FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R10l7qab_rk8k4j_2oc.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	13FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rgatecg_rk8k4k_2oc.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	13FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1ae6bsu_rk8k4l_2oc.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	13FEA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.3468	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	143D405	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	13FCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	13FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	13FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 \cTab0\cPathInfo	success or wait	1	13FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	13BEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	13BEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	13BEA55	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	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/WorkOrder266912.Pdf	success or wait	1	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	WorkOrder266912.Pdf	success or wait	1	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	140DF69	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 57 6F 72 6B 4F 72 64 65 72 32 36 36 39 31 32 2E 50 64 66 00	success or wait	1	140DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 35 32 32 33 35 33 37 2D 30 38 27 30 30 27 00	success or wait	1	140DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	337441	success or wait	1	140DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	2	success or wait	1	140DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	140DF47	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	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	140DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	140DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	140DF69	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	140DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 3468 Parent PID: 2616

General

Start time:	22:35:30
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\WorkOrder266912.Pdf'
Imagebase:	0x13b0000
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: 5328 Parent PID: 2616

General

Start time:	22:35:36
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0x150000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	2459E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	33	2583E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	112	258447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	217	2459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2164	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	4	2459E2	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	2459E2	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	2459E2	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	2459E2	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	22	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	56	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	58	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	20	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	19	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	237	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	288	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	2459E2	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	2459E2	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	195	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	32	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	8	2459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	2459E2	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	2459E2	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	168	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	7	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	2459E2	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	14	2459E2	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	2459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	2459E2	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	2459E2	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	316	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	149	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	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	2459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	2459E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	2583E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6216 Parent PID: 5328

General

Start time:	22:35:39
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1724,128282512544814 3229,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2298543776899609676 --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=2298543776899609676 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x150000
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: 6244 Parent PID: 5328

General

Start time:	22:35:41
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1724,1282825125448143229,14443777595928039979,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=18073613818027731679 --mojo-platform-channel-handle=1752 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x150000
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: 6292 Parent PID: 5328

General

Start time:	22:35:43
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1724,128282512544813229,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4894735529953023862 --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=4894735529953023862 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x150000
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: 6520 Parent PID: 5328

General

Start time:	22:35:47
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1724,128282512544813229,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3551037961868620507 --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=3551037961868620507 --renderer-client-id=5 --mojo-platform-channel-handle=1864 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x150000
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: 6656 Parent PID: 5328

General

Start time:	22:35:49
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1724,128282512544814 3229,14443777595928039979,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13670455395302550708 --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=13670455395302550708 --renderer-client-id=6 --mojo-platform-channel-handle=2112 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x150000
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