ID: 369556
Sample Name:
T_C_CovidUnemploymentChallenges.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 19:28:55
Date: 16/03/2021
Version: 31.0.0 Emerald

Table of Contents

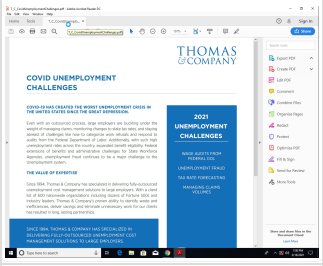
Analysis Report T_C_CovidUnemploymentChallenges.pdf

Overview

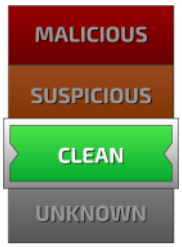
General Information

Sample Name:	T_C_CovidUnemployment Challenges.pdf
Analysis ID:	369556
MD5:	9581f6aba2b67b0.
SHA1:	ff2da8cf7374b01…
SHA256:	c15b0a6413b02f2.
Infos:	

Most interesting Screenshot:



Detection

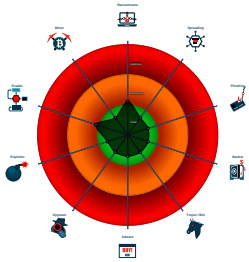


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

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

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 7072 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\T_C_CovidUnemploymentChallenges.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 7160 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\T_C_CovidUnemploymentChallenges.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5560 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6348 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,16331776786295461319,7200131169507494228,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=179149627330959911 --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=1791496727330959911 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6592 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1700,16331776786295461319,7200131169507494228,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=92258711054484144467 --mojo-platform-channel-handle=1760 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6448 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,16331776786295461319,7200131169507494228,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8257130289996470003 --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=8257130289996470003 --renderer-client-id=4 --mojo-platform-channel-handle=1776 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 1664 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,16331776786295461319,7200131169507494228,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7449791400690600131 --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=7449791400690600131 --renderer-client-id=5 --mojo-platform-channel-handle=2000 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

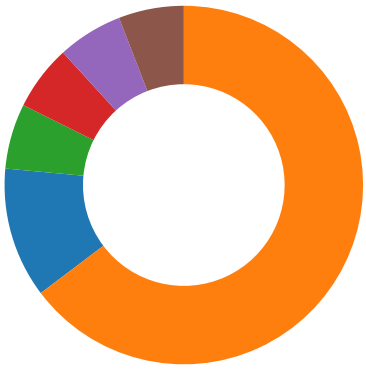
Yara Overview

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

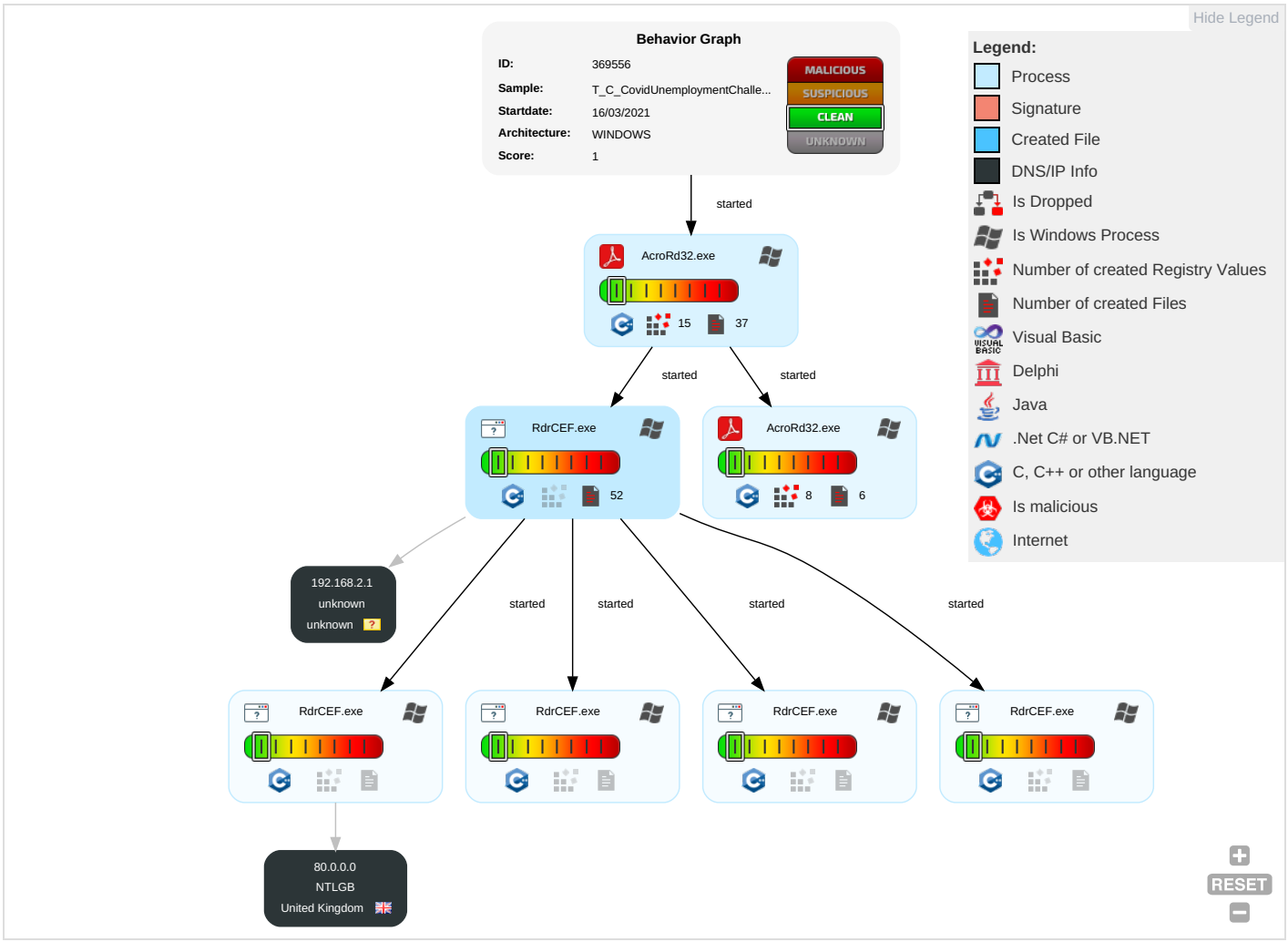
Click to jump to signature section

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

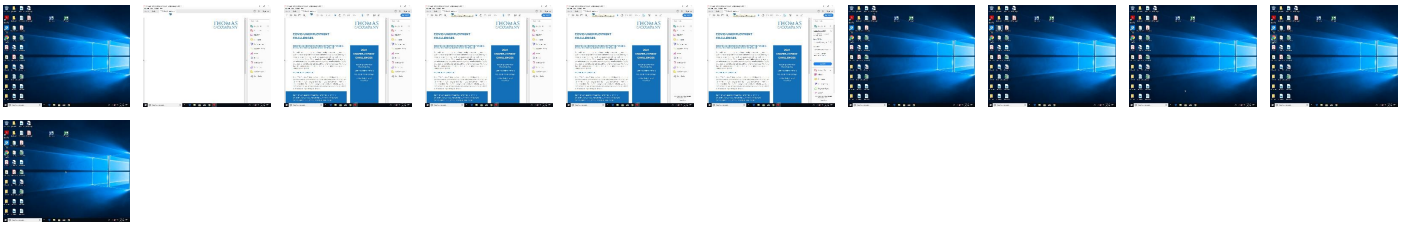
Behavior Graph

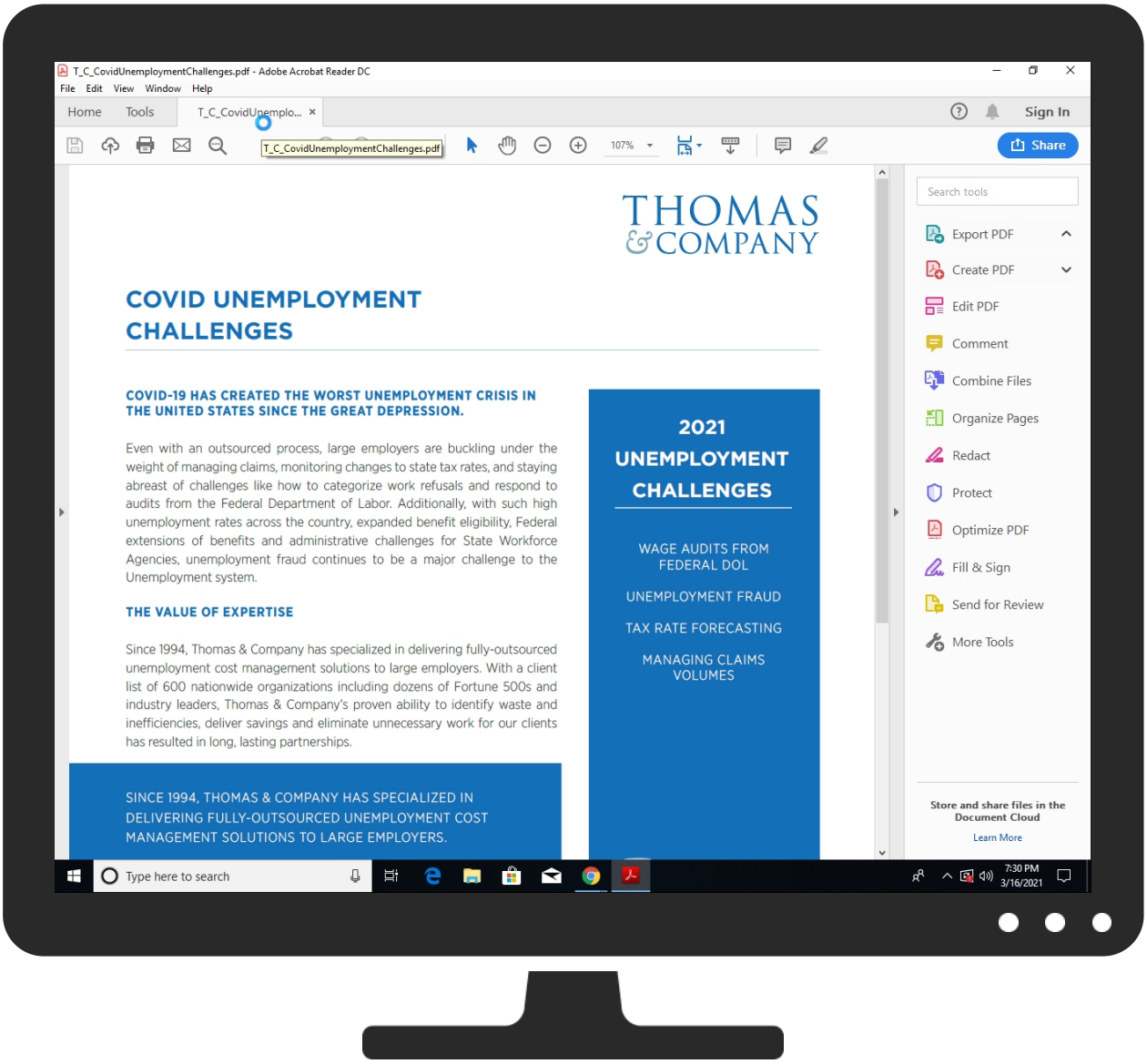


Screenshots

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://www.Thomas-and-Company.com	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4u	0%	Avira URL Cloud	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/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://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://cipa.jp/exif/1.0/)s	0%	Avira URL Cloud	safe	
http://www.adobe.cFZ.	0%	Avira URL Cloud	safe	
http://www.e.com/go/ipmrhpr	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/D3	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/uy	0%	Avira URL Cloud	safe	
http://www.adob.	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/Upload/y	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/Ny	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ZCW	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/_1v	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://https://ims-na1.adobelogin.comn	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

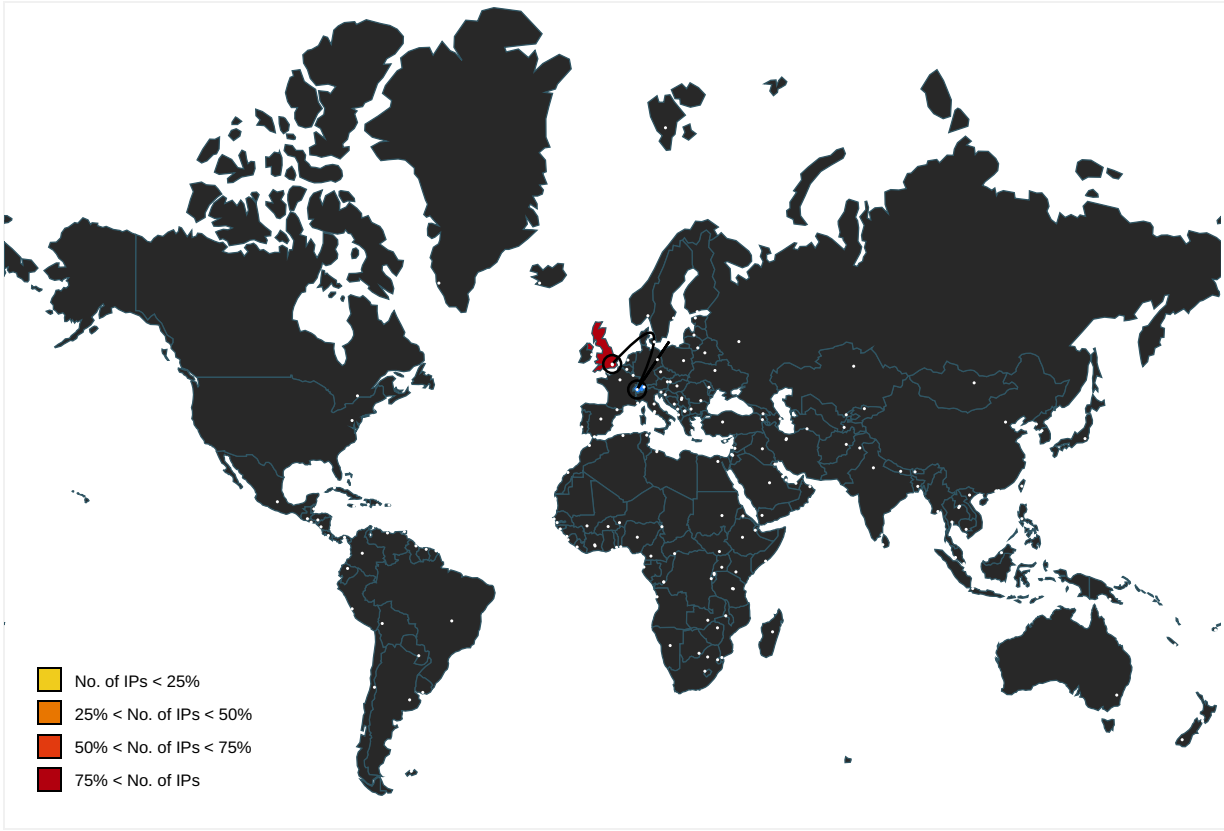
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false		high
http://www.Thomas-and-Company.com	AcroRd32.exe, 00000003.00000002.842505246.000000000B1E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4u	AcroRd32.exe, 00000003.00000002.842505246.000000000B1E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000003.00000002.829007781.0000000007900000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000003.00000002.829007781.0000000007900000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000003.00000002.829007781.0000000007900000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/)s	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adobe.cFZ.	AcroRd32.exe, 00000003.00000002.844011053.000000000CA6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/id/:	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false		high
http://www.e.com/go/ipmrhpr	AcroRd32.exe, 00000003.00000002.844011053.000000000CA6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/D3	AcroRd32.exe, 00000003.00000002.842437607.000000000B199000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000003.00000002.843123031.000000000B4FB000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000003.00000002.842505246.000000000B1E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000003.00000002.843915519.000000000CA22000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000003.00000002.843840459.000000000C9F3000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000003.00000002.829007781.0000000007900000.00000002.00000001.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, 00000003.00000002.829007781.0000000007900000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.echosign.comRL	AcroRd32.exe, 00000003.0000000 2.843123031.000000000B4FB000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/uy	AcroRd32.exe, 00000003.0000000 2.843840459.000000000C9F3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adob.	AcroRd32.exe, 00000003.0000000 2.843740268.000000000C9C4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000003.0000000 2.829007781.0000000007900000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/y	AcroRd32.exe, 00000003.0000000 2.842505246.000000000B1E1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000003.0000000 2.843840459.000000000C9F3000.0 0000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000003.0000000 2.842681405.000000000B2C3000.0 0000004.00000001.sdmp, AcroRd32.exe, 00000003.00000002.842437607.000000000B199000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/Ny	AcroRd32.exe, 00000003.0000000 2.843840459.000000000C9F3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000003.0000000 2.829007781.0000000007900000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ZCW	AcroRd32.exe, 00000003.0000000 2.842505246.000000000B1E1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000003.0000000 2.834228252.0000000009014000.0 0000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/_1v	AcroRd32.exe, 00000003.0000000 2.843915519.000000000CA22000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000003.0000000 2.829007781.0000000007900000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.comn	AcroRd32.exe, 00000003.0000000 2.834228252.0000000009014000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	369556
Start date:	16.03.2021
Start time:	19:28:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	T_C_CovidUnemploymentChallenges.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:	21
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@13/46@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): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.113.196.254, 13.107.3.254, 104.43.139.144, 52.147.198.201, 13.64.90.137, 40.88.32.150, 168.61.161.212, 2.20.142.204, 2.20.143.130, 2.20.142.225, 2.20.142.227, 2.20.142.211, 2.20.143.129, 2.20.143.6, 2.20.143.23, 88.221.148.153, 92.122.212.192, 92.122.212.216, 92.122.212.81, 92.122.212.194, 92.122.212.203, 92.122.212.201, 51.104.139.180, 8.241.122.126, 8.241.11.126, 8.248.131.254, 67.26.73.254, 8.248.141.254, 52.155.217.156, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, s-ring.msedge.net, acroipm2.adobe.com, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, s-ring.s-9999.s-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/369556/sample/T_C_CovidUnemploymentChallenges.pdf

Simulations

Behavior and APIs

Time	Type	Description
19:29:55	API Interceptor	13x 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	0000001_Carved.pdf	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	BWKPI3LiLi.jar	Get hash	malicious	Browse	
	fakeadmin.pdf	Get hash	malicious	Browse	
	x4F1uS8nAq.exe	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	0000001_Carved.pdf	Get hash	malicious	Browse	• 80.0.0.0
	BWKPI3LiLi.jar	Get hash	malicious	Browse	• 80.0.0.0
	BWKPI3LiLi.jar	Get hash	malicious	Browse	• 80.0.0.0
	2ojdmC51As.exe	Get hash	malicious	Browse	• 62.30.7.67
	fakeadmin.pdf	Get hash	malicious	Browse	• 80.0.0.0
	8dazsN65iH.exe	Get hash	malicious	Browse	• 80.193.200.66
	Y17R73rU50.exe	Get hash	malicious	Browse	• 92.239.246.126
	x4F1uS8nAq.exe	Get hash	malicious	Browse	• 80.0.0.0
	delZYToJxe.exe	Get hash	malicious	Browse	• 92.239.246.126
	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

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):	410
Entropy (8bit):	5.660029215448358
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QhlF/mi7Z+P41TK6tO/Een9YOFLvEWdM9QoU8qi7Z+P41TK6tG:vDRM9ktZiEw5DRM9pZiEl
MD5:	E860EFB027DF42F04D2D6A6D65D77BD6
SHA1:	9B5F7FA82C32C0F2D06D5AE6E1FA05F83B02B13E
SHA-256:	CFAF3F10A0C4A91DF106F734A647F894D57AD5F73D296DAC8C81447DB207FD23
SHA-512:	E2F4ED6C3471D11B1F5DBDD7F530E3B28926D966BC0344644B9CC5A440E1BA97927523B32C7F4CED95592673693534C95FED05B8BE766CC7943464F5258A229
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....A./....."#.D.L>..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 .x4 .A./....."#.D..PM>..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....n.....

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):	348
Entropy (8bit):	5.6151524654374265
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkl/p1F8Be7Ywcr1TK6ti2i9NqEYOFLvEktkUYXlF8Be7Ywcr1TK+:V9zo/pj9PQE9zVYj9PQ
MD5:	28C9677327D2472EFB46562C2FF67F28
SHA1:	4FD2E4B2C2A550A96095CF85F89586C85A1249B9
SHA-256:	9A5E3BF27F7BC4BF08D463655DAF924EEF36B61D65093ABFE425475CCC493C9E
SHA-512:	E094B89616B72A79C54EB24502AEE74BEC73547026C3A8555D7FA712BC0226C27B3CCD84C577910F0505FF3133E4ED7B9FFD8FDE915604B670E99F654B71CF9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .I|..A./....."#.D..QL>..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....9q.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....A./....."#.D.q.L>..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....;.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.591451659547328
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFJglUo6jryeRVFAFjVFAFG75lUo6j:tB4v4uSBVB4v4GVSB
MD5:	AF94214CFC81635CEDB23BF8980ECC2E
SHA1:	937B52B76BF58F3B7DA8AD2758F14D37CF082664
SHA-256:	25E4FF6F2606708D861B456F3E7F638BCC215D125F543443BD328104C5FBD600
SHA-512:	DB4AC95021180FF7F8CF0B9ACB5EBD6A626C53B3F7CDA21EA4842278282B624EF5795B2A3060F69D581B5330D1E1C349800DBDBDAE8BBE0CF1093700AFF6F2 2
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 ..U..A./....."#.D,..L>..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....x.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .....A./....."#.D..HM>..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....6 .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Entropy (8bit):	5.669373736584535
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsnq22iWulHyA1TK6t:IbRkiD+LWuss
MD5:	C34CCA173B9E4FDD997A72635E0E0A87
SHA1:	A2CFC315837A826E6402221C9FF00CDEE151D136
SHA-256:	A7D4CDB4BA6BF7BA70D681B905FF7779FE86CA8546117EAB98B5F8FCB3B146FE
SHA-512:	004E4EE89879218D76F197342D104E48891AD83B154CA6BF79456E7351E41FB18A8604CF20BEDD61106EBB6BC3BFA8A0E77CB202B0563A8EA066CD6D1737698
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 .5T..A./....."#.D...L>..A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....E.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.55628884089393
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVueKAGaFVyh9PT41TK6t8:pyixRubApV41TE
MD5:	F1297D6D6D83330BBC686CF98F00196A
SHA1:	59BB956103E8FD0654243F2C87941B2299442239
SHA-256:	AC81A08BCEB31E7BAC353963878C3B003CFEC9E6A5664086F905254402574B78
SHA-512:	3403095F9C99012BE50A820E2AA7D134EB6C6D4BE89523E850DA13424258A97B4514120374A6D674FC85C7CE7C50E768447908D3B774A268A32D235CD823DC05
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .o[..A./....."#.D.#HM>..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....2.....

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):	216
Entropy (8bit):	5.575920835499494
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVxKtl2jp4Sco2sZI8xeGvP5m1TKC:mvYOFLvEWdhwjQ6D6SLZll6P41TK6tr
MD5:	22FFC3759685074AAF3E685F7D424C77
SHA1:	5EC16652A68B924198EC80B28ACAE763DD8846F8
SHA-256:	8610DEF776AC4DF1C780944CB5A135C9B50B9E54177482C96A8B09FA604348A9
SHA-512:	C6D5E8A502C4283D5671C55A8BDB4074B65446CD978F2EF26353EFEEC47E8F6D3EC8860CB3CCEB15B8275CAE519619FC5BD9AC86F4F56DC2884E5563E613C 99
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ."r..A./....."#.D...M>..A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.475923428568588
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQLw46g1TK6t19fHl:2RHRQCUw41D9Pl
MD5:	0459F57383EE80B02430DD5C21346102
SHA1:	F1AA8C5AF9CE7AE180B455D43E1CBCA4F27F0DD0
SHA-256:	8AA869EFF2B1BD8141444F6708F29867D5564311DD036183454E35B6DFB47EFC
SHA-512:	B4AEF4DB8E1412EE264151A763EAAE86D6BE3ADBD92F4FDA87514727D55545A58C2BFB7FB23785D54BBF1D5BFC746AB11D2A53EFC9CA528167A318FFCB6A8 EE8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..j..A./....."#.D..KM>..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....z.....

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):	358
Entropy (8bit):	5.595674202071694
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLq8qgINMuR/41TK6tNOYOFLvECMLh5bNMuR/41TK6t0:Z5MObgeMuR/Ew5M95hMuR/E2
MD5:	11800A4A178FE49FE503265BF1B633FE
SHA1:	55600D451F5BEFFB27D0491A822B0B95E97D9083
SHA-256:	87068491C43E9F01336E97E9398E01D6BC56FA54FD834FCBFCC0018DA19870E8
SHA-512:	156CFFD72B92CD7EF1100FA2A8E0B7C1177581579E7A7343E95FA6725BFF96D86EA5C1AB3911C26891EADE7975C54C103F9EF47B1C0B040FFDC4F1B68A7C6D 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....A./....."#.D..RL>..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .....A./....."#.DxE.L>..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....!.u.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.490868165672692
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuClklBJ+by0zBUKSAA1TK6t3N:pRukYbe9N
MD5:	2F9F494BA5EAE320C9FDD4E8346FF6C2
SHA1:	93B2FED2F8393A8B0BF0D2DE68C2AB274F716143
SHA-256:	72BDF7F1E70AD28D03D83E5A356C59FD87ED9EF240AC98D7CEBE872ECFEE67CF
SHA-512:	2F651711C7D3268D71A54CC110421CCAB2350FAF73996F101A6C1737D6F1F235B182CF3FD4CC7F5D493233EAA1BC3174D915CFB4870D4F3FCC620FF1D5E6D8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .._ .A./....."#.D.~KM>..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....ANe.....

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):	354
Entropy (8bit):	5.566246400905361
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFvWtatUdyP41TK6tZl2d4HXXYOFLvEjMSWFvAUfctUdyP41r:KkXxKMSCvdtUl/lakXxKMSCvAVtUll
MD5:	E8857A74CBD0990CAA7854649261A3B9
SHA1:	680BBBCA0998F479F2A99DD345EED6A5DFDA1536
SHA-256:	59ADEBFF6D36F229C49CAE7B6EFED88314D46DE0D57C70AF99EDFBBADB04B396
SHA-512:	A7C5BB9F5F2B9F7CE7B3E8AA2F50655D65FF00BEA2F6D844977B0D983F3BBC0C3D433DB9A808EF14112639FAC962E64D45043A71EF7FFA70B4E540BCAE68E8 8A
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..~..A./....."#.DY.RL>..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....x.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js .....A./....."#.D...L>..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo....._..1.....

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):	374
Entropy (8bit):	5.604336303318097
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLFpyM+VY1TK6tLlEkl9YOFLvEWsfOLElcyM+VY1TK6tYL:5h6OLGkllbh6OLEl9kqL

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
MD5:	98F1E2CF414411D11D355E08F9F90E9C
SHA1:	401E05E2E0FB667A9D48DD7F246FAC788DE4523D
SHA-256:	4B2882FA01D947677BA1EB50194901B97FD9E11B2D627FA8329C0855C77C3224
SHA-512:	F2A2BC3C5E0250232B4019D9BD1EEF0B4A9378D53CF489E39AF6F31BD71E4B59EDC308255078C27CBC48E28C1BFF90597469472DA8937DD736AEC79908D4E5
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..w..A./....."#.D...L>..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....Cu.Z.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....A./....."#.Dfg.M>..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....S.....

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):	488
Entropy (8bit):	5.6130149745135265
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFjwSeKaTLnPRVFAFjVFAF5XwSeKaTLn7t:UB4v4jwzXLnPB4v4pwzXLnJ
MD5:	4F3D6167C4846AB648710F58EE865B02
SHA1:	0E1F22C177F402847A7F8E58939D06BC7F160909
SHA-256:	7CF5352432DD4011050903FA106DF31ECA3C6E36802323A1DE83F0AEDA464C77
SHA-512:	E820363675395150712A9D55DE76ADFE5DA2BEDF9FE4F6194FB174840F1D633DAFF769A7FFECB6A809673CEEF02E3B0EE803894688045A5FE05AB70ADF7C232
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 .....A./....."#.D0..L>..A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....1.....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 ..c..A./....."#.D..LM>..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....IN"a.....

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):	211
Entropy (8bit):	5.501316389465341
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuzneP11TK6t8M:BsR2EseweV
MD5:	3AF10BA4AC0C7958346F1E14E741C209
SHA1:	922AEB61552DC452551EB90EC174ECADC4B14DE1
SHA-256:	3490BE0DAFBC1775AD9812CE4C3A33AED2306280BC34E046E403C71D825206EA
SHA-512:	0FA2FE71CDF3FC634EC25D3E426D5C99A399CB7480C5E38575EAC04CC677253FDD14979E2627CA43EA41D588928A767D72EB7E052B959F7DEB2C7CC03486D0 6
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..g..A./....."#.D..JM>..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....q.....

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):	202
Entropy (8bit):	5.6034035533892945
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ75yTB7OhKlvA1TK6tdl:RbR16JBJkB
MD5:	14FD886909EC3A08709745256F0F4EC0
SHA1:	91036EBE79611243B9F571179ACAD433FF1702AF
SHA-256:	DF182F058F3556C2AFC79BE03EED2175312DDD523C6B9684936FDB612C4F15BD
SHA-512:	4CB891AFEBF6DDB79A01DEE8E0BB6DAFA7141211915D16017CC14A5A52A5B1903A6083958EEFC73EF214A52E523715AB3B7346009FF5C2185D9B3E99637B83B 3
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..m..A./....."#.Dy.-M>..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... {.8.....

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):	211

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Entropy (8bit):	5.566961960055973
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuMOwSQdFt1TK6td:B2geRHRQMn0
MD5:	1AE5C635208828087D0524BD71AF0313
SHA1:	DB5E02D0C74DB604BEDF5E863BD8EC6ECCF4BC74
SHA-256:	D8FCBA1BDC1FB76E01CBDAEA73076B4DCB9FA9C0B8558FC519FD63A8125E72D2
SHA-512:	BCCD8B60B293D37AF857B1766A0FAC336D56F6D48A3E4AE93FE9108DEA42A62DD69EAEE087692BC2734E41D43965D0C077F690BE51904813ABDC394D54FAD8 8
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..M..A./....."#.D..IM>..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):	412
Entropy (8bit):	5.607930756520509
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQH/ka17At1S/1TK6tazyEYOFLvEWdrIOQLJ4Et1S/1TK6t:WyeRll47At1wwyeRlKJZt1w
MD5:	C32981E8E27D16577C85C4D35E570FB4
SHA1:	DFA3FF6D93E68DA5CEB20214D5D29F042170FEF6
SHA-256:	38FBE44F319A2EF4990F29EE027EE41CE7A435C159DE04BBDC2281BEF35024B0
SHA-512:	643DC7F0765B9FF00EC9FCA895AFEFE23EE5C3115AD195E59B4A5F49644B24EA6E104F4FE0DB4A0813172BBB42B453667D3DB1406512004ABC1B67E8AF1612C C
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .....A./....."#.D...L>..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... ..0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .Y...A./....."#.Du.$M>..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.. ....&.x.....

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):	218
Entropy (8bit):	5.551888887397364
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvSt1lgVwWYNqww6U+5m1TK5ktwN:mnYOFLvEWdhwyupsqwK+41TK6tw
MD5:	FA21B35070BE7FED97273F4291482BDC
SHA1:	CAFC9D035424CF78ED82B60D7D2C2024C36F96B0
SHA-256:	64426EFF74C5B3D4D3FE85812B074DDAEBD67BAA41FA35B8F1066F2B343341FA
SHA-512:	FA07538679F135BE9BC701C14117AC5EE8E1DBCC201D36B03E64D659A05EB99A686B65D49CFFCD6EB1515DA142FFA43419C7A36A3D0CDACD5547BF3B8F684 50
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .7...A./....."#.D.~-M>..A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....32.F.....

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):	230
Entropy (8bit):	5.571479876581484
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuMwabfO441TK6t:/RrROk/1fLE
MD5:	0548815EF3BA05241CDEC700078BEE28
SHA1:	669E2D98033DCEA16319DDA566F2F7434F389671
SHA-256:	0E9D76F75373B6CD479CF0F9974BB177E7B0D8525FF940EBF64A57C4A688BFF2
SHA-512:	6E8E92999935AC526EFFABF1BC92D50A1E8BA2F5EBC9C39EFBFF229554AF05DB9307D845A1E1FAD935B653586EC8672592D2FCF4A58518744E53ABA36FA7266 7
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .G...A./....."#.D..#M>..A..~..rw.+[....!.)?..f.U..(=.=. A..Eo.....A..Eo.....+k.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.637198083985638
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIdtQbS1QPLr1TK6t5+mDEYOFLvEWXIQhCS1QPLr1TK6tD:xqTPbSCPLnLZqTtkSCPLn
MD5:	6341379AD1C0A6C9E489021C36899D12
SHA1:	9BBE75FEAC10BEF71ED48599C473113C84005A5F
SHA-256:	557BBF4D38FE55A7BA737B5644E762023256A3E8874596B1B3E506DDEDDEFD6D
SHA-512:	1DB0055A27E271905F3FF0D9986A3DE2699C9BFB9D92C9DAC96568B3E9D9CB4B4B67F3AA4E3FA2FB458304B5DE3E88A576D8116351AC5B5F6C9DCE8234B6370
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .^_...A./....."#.D...L>..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Y.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....A./....."#.D9_.M>..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):	414
Entropy (8bit):	5.638496761989548
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuevgRLsEJ41TK6tDE52YOFLvEWdMAuJnjLsEJ41TK6t:zRMvLsDBBRMvjLsD
MD5:	1F3A909FAC47EFBB1D3A1BD1F42E3B31
SHA1:	DD4785D7E86063036A90D1D224CC2F8B648A3AA8
SHA-256:	AA8F9C2D65437233CCDF12A40BDDF7111F32BCDE13FF333EAB543090F8688F2B
SHA-512:	260BAAF0856E9A44760A6F780AB89390C33EB4E3CCC138170ED76465ED08DF850DFE46D402C61D3EFC3B8A5563A85E94ABB3B06BB98A86EE1AF4C86F2373B06
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .. ..A./....."#.DY..L>..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ...).....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..p..A./....."#.DrMJM>..A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....#&.....

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):	420
Entropy (8bit):	5.591892609694666
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAu6bFFong1TK6tYYilPYOFLvEWd8CAdAukZ/+Fong1TK6tt:6lJRRFoMylJRbZGFoM7
MD5:	C6B32235429C095B7E9CA6C36FA61030
SHA1:	0159841C26B7521C0AB88E94A74E2F1BDC66ED3F
SHA-256:	366898559C0FAA53EAC610420D2EACA41A12E27F2A0E4FAC060BE53AE86E2534
SHA-512:	5475A90E591878ED4A8CB7C21BE6E6C9399C90E60888BFE18B063CDAF68A3C5CCEB09B2AAAC7833FD0CCA87F16565B82D57981CBC003B29EE2C2CF93D575F54
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..>..A./....."#.D.).L>..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....D.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..r..A./....."#.D.dJM>..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....D.1.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.62096127131253
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/Iu0+l9A2e16wG1TK6tMY8nYOFLvEWdrROk/luvhg2e16wGy:F8hRrROk/L1e2V8hRrROk/bVe2m
MD5:	DD5B752101FF508890F2D858D874D1DD
SHA1:	7766A2A0F35EB23504C84FA6DB81AAE75BADC837
SHA-256:	48BC067A6E4DE5513D52C23F749014D1650082ADED36F19FBFC34D375E7F1B6B
SHA-512:	9523184D5C3E0517ADB82D38648E98082396E05C233459D44704AC8875B6B5469477F5A7904840016A40C3C6B64BFD2EBDFB33D9E211352E3DF9AF1237FFFF2E

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....A./....."#.DB..L>..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 .}...A./....."#.D..#M>..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....

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):	426
Entropy (8bit):	5.675014243683238
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQjLh0XrNJli1TK6tb8LrnYOFLvEWdrIoJUQl02axEqrNJIW:ehRcyyrNJICF4hRc509FrNJIC
MD5:	4C496723F9A7B0D225373BCE6913F71A
SHA1:	852CEE021B5B2403BAB8DF15F48426E53573F342
SHA-256:	6DA21587C8E3EF68AF8445BD427DFD8DF6E72114D16A1A1CA5C695BDB0B3614D
SHA-512:	FB6D384EAC5EDF64BC2DF0A1B028628C3CCCBA0FD692329D57F5FA07E6E96C51010DF002A7834171C06FBE7CF9BCFD6B048F6EDBAE19C5C60291D1AD0A826D2
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .."..A./....."#.D.~.L>..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....P.W.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .....A./....."#.D.?$M>..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....Xq.....

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):	416
Entropy (8bit):	5.605343822188204
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhued6o8Lzgm2d/1TK6tG+OEYOFLvEWdrIhuDP303Lzgm2d/1TK+:0RUd6oiRe08R5/YRe
MD5:	89EAA01C7D341D32EB8722CF2DC48164
SHA1:	660855910B5AE989CA7C601A0FE6D3E537BD9AE8
SHA-256:	28638B533D3F0AD0B3E7E481B453456EFB6717C8DB07EB200CCBDDA0DA5430A8
SHA-512:	A7DE009B67D40B4CA85EFAE6037590B27333A92ECF09193C243C38AC31C15696CFC4E59DF1EF6ACAE2C56DB10754C54DC14E92114064C8FEBF2F5AA1DEDE443
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....A./....."#.DQO.L>..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 ..m..A./....."#.Dz.#M>..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):	376
Entropy (8bit):	5.624619819824043
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kpw/Was2kx56uvp1TK6t1IHeAElVYOFLvEW1KCk5aiWas2kx56Y:6JJK4u9NJJKCk9Wn9
MD5:	815B99D1F714388C4A458EE2F509C9A5
SHA1:	B902A46B1AC0806CAD78AC81B1CEAA9A34553957
SHA-256:	C257D1E3024F701F91FCC81976A7DB08FE57FCCDEEEC784E3E956D9F7D7E1AF3
SHA-512:	D9F39EE2A356C975456C3393C1AD5C0F528180A1346369554B17B624A8DBD4B7A5D66A7FA43675018D61068CC168F47DAC226C87B8E61071CD5B65127AB3DB3
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....A./....."#.D.dL>..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....JHO.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .K}..A./....."#.D...L>..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....W.....

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):	214
Entropy (8bit):	5.604275622737502
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
SSDEEP:	6:mWYOFLvEWdBJvvud9ghUDLYtmOZn1TK6t:xRBJcDDcFZL
MD5:	6304EDB0876A3DBA273B69A5014AE5B7
SHA1:	81680FF90719F29B159F780811581DA6E6AEED02
SHA-256:	643CA86A5FBA1E68373507B31EF2E3EC0DC5927AEE1A6C77B3A7D3BF495D6CD4
SHA-512:	FC31C55A1EC88F05956369E2C6DBBAF9B5DA114E8C9AD418F57759B9D6053103DB9308108E685A23004FCCFB873BE0F807E0B369E0B62043A1A3B22B5449921
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..j..A./....."#.D..JM>..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....A.....

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):	422
Entropy (8bit):	5.6250928469110795
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7JwIoI7yaVPu1TK6tYtMsRPYOFLvEWIa7zp7Hgx7yaVPu1TF:BPH/wIoicAPHlg1c
MD5:	11E9ED73C6E708589F25C44028FFA87F
SHA1:	5F52B76139BD199827C5169E6D19950444F1BDD0
SHA-256:	542062AF96AA797C935D19C3A7A1BD7E5D0C7CC3EFF1D3FA46E755F4D231735B
SHA-512:	8957F2C27D4E2A452FEE2894BF8820329BF416B1BF4A63D31C16796CB7F1A7FFEB73C54B901273009BC22B9B7F12D3402209F2B2BA8BB25E3B797E736F0E8B5C
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....A./....."#.D.MSL>..A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....gM.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....A./....."#.D..L>..A...L...Im.@.....E.nW...IP..A..Eo..... .....A..Eo.....g.(.....

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):	208
Entropy (8bit):	5.565233267751388
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuV0/tlmGxGJs4XVAZ+8cV3vRm1Tu:mKPYOFLvEWdENU9QXLCiM3Y1TK6te
MD5:	FB1237B2BFC31F153EC4BF4BDAD80DAF
SHA1:	934F91ED60E5A828DC14D18F3F624A63A4D22E97
SHA-256:	061E30C5B6EC4EC1458103B073F0D3AE5397531FF27D70CAD7BD0A130A60D071
SHA-512:	08FE0213351B96B8340333B510E2E205B8146C6A3783917AC1D26FA22B46FB66D4717570EDA9FFBB5316D7F30B69C6D1C27EF3FCC17338C6D280E085325007CD
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .fp..A./....."#.D}x3M>..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... ....A..Eo.....g=.,.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.598188810887315
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQa0t2jBRCh/41TK6t9P9/:XRc93Di/ETP9/
MD5:	D8E25D0DBBCE6F2415A220C417A1283F
SHA1:	8E0D2D2090B468C5FE7D68E01616CB1E19C724A4
SHA-256:	02D36266067034955C774D8371DB6F7155815B2658A00B57DB9FFBA236041635
SHA-512:	E93A0DC5190E0CF908C6E913F05E8CF5285C44F7E44B109B8920ABC7E00ACFA504ECA53FE79A0BD77C87DC38C176041FECF522EB1D87D4DD298C6814485436 8
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..g..A./....."#.D..XM>..APJm...0x.x..RD...BB!@5..<..]....A..Eo..... ....A..Eo..... j.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Size (bytes):	231
Entropy (8bit):	5.576803586784169
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuUS+ULlF4r1TK6tR:bs6xRkiSELlF4nX
MD5:	EAEE3C7DB705E62714FB565702277BAE
SHA1:	F41A1DB36CB5B02A3D847F1FB094325B6BC32ADA
SHA-256:	F1C3EC7D04F54AC16219BE96C57D9C6B1DC6B9412AFC2FB1BBDFF5ACE40AA2A8
SHA-512:	D60E96912C1D23B0FD052DCF15A3D289286937EE5D90192663BBF41521B8208170BE1A20502CCCB698F04AF7FA18EB079423F391FA33DA2B8E392F6D9BFFE919
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .v...A./....."#.D...L>..A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....Z.....

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):	215
Entropy (8bit):	5.483786972819279
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvLe/lD1uoXkTcu1isLK5m1TK5ktf:mhYOFLvEWd/aFuMnXh941TK6tf
MD5:	7D0C82E8BC27DC99E2D486733863AAEE
SHA1:	1FFDDE47BC35DD554E8EC792349CEF7B216F6C07
SHA-256:	46805E579D95F699EA8928E5A30B8C948EBCB0CF437DA74E2F0F9FA958778083
SHA-512:	AA0BB0185FAAB7DB522A69533A76D6FB1AA90055DACE586F3AF25269D34FBB0B37E78C7407A94701844BF6DE7DD6F2C16DBAC3A3D01E4270188BE785B17ECD 2F
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .cy .A./....."#.D.KM>..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A. .Eo.....E.....

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):	208
Entropy (8bit):	5.540162537465922
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQHmBoBMqVd3G4K41TK6tD:2DRuRQpB9Vd2k
MD5:	7728C7A0C210C53C00E653F7E68C58BA
SHA1:	485AADD9CF01C62DBCBA586F06F2EEB0F554EB90
SHA-256:	E194A7E27D1F68241129FF8A8DCCE65DE0E9A3C6FCFF5E906ADE764EECC5D0B8
SHA-512:	CAF01E9F37A02C58722917C2941CCE8AC8F79C7C7CE67606111E49F45DC9DDF860E2B8AE6A9AC418B9F6E38A90342CB55035998D4D8A6C3453E54AF16C89D0 D
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..F .A./....."#.D.UKM>..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. .....Y6%.....

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):	416
Entropy (8bit):	5.618434150290398
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q9CtOuA424r1TK6tQt2kqYOFLvEWd8CAd9Q//OuA424r1TK+:+RQuornmtORQgrn
MD5:	DECA066D347ECF94627DCD7AFA079CC0
SHA1:	1AD50BA2750DB5FDC027A5B71572FB831D72FE36
SHA-256:	7A41AA6EDE658A9C368D0657AB508A4B8796D0AD5D5376AE7550AE844FFF8898
SHA-512:	9D76D1577A650E2A3E01C7F1D5F434EF3C7AB17BFFD26A33E5CA8A16A6B87E8B918FE2F0D20916DF297D8652585F5F44CFFC2AF49B8204847DF06C5DEA24E8E 4
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....A./....."#.D>.L>..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.... ...s.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .!8 .A./....."#.DQ.XM>..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....

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):	210
Entropy (8bit):	5.495095296292436
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvUu/tlyGdSrg2iHio/Mm1TK5O:moXXYOFLvEWdENUAu6yC8n1TK6tJ
MD5:	EE11207FA75BF5F0C0A4DEDF39184ADD
SHA1:	5AF303425895BDEE8FC57275128F560049B191AD
SHA-256:	97C7E8C37F2FAD274DCAC34CD91EE7CD364C9D347663B5671DBC05B288082AC3
SHA-512:	1E7BB3412F3A313CB4D8EEDF440E65C0D04DAE480ECF3B0183B8E3858614D02DE59B8CA7D82AFF0F0C067C6988B6B92BAFBE6E452D21AEF314C3C9D035F258F5
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .1...A./....."#.D1a-M>..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....R.k.....

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):	442
Entropy (8bit):	5.646038864057867
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQynhLKsLmB41TK6twQZYOFLvEWdrROk/VQxx5K/s4dsLmBl:nRrROk/VR9omnRrROk/Vex5as4vm6
MD5:	EDABDCD5BBD00B3FADA0C6633C0C07EC
SHA1:	1B9B10844B54E09C239B896A07F2998663D425D2
SHA-256:	B41190FAA6E7FF6BBF4DA1EC1CBEE53C8E3FC55F5D910993F4A42370981B64A8
SHA-512:	F98DF0C3893F5ADF6B60B4657DE914BF8D6F0A5468E3D9CED30BAEA0814340603E291121FFF632A57E5D28D612A5B3DD2B2A9001DF75BCDD3E04669730EC4350
Malicious:	false
Preview:	0\r..m.....]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .....A./....."#.D...L>..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....QO.....0\r..m.....]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .F...A./....."#.D.]$M>..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.568634885414253
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuQ72uxAdm9741TK6tX9t:qxRc272uxAdu7E
MD5:	0546ED930187373CB1061A1BFA62F134
SHA1:	21538A4A9D41A49BDC6B7FBDA3648FF6586D63E5
SHA-256:	7D3431C1B611AB1A1AB78FDD8AB278C874F5D426A20B9C0F1B6FBD3067EFE3D5
SHA-512:	9FC191DE3E128B811C0F07221F62B625CB801B2269DA11633B3F4F9F3824BED17919125E97579E2D105A96873358ADF123136728713273530 99FC5F7C767396C
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .O...A./....."#.D..HM>..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):	204
Entropy (8bit):	5.5204133994302165
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvg/El/lbgG7kTSPfB6shoq+Nem1TN:mMOYOFLvEWdwAPVu2/27ZkJn1TK6tR
MD5:	3DF89EAD6F15E5276C2C50A53D13027F
SHA1:	3C71EFE30278EC548AC074055CE383980F1EF3C8
SHA-256:	83C848D8C9B7DE32EEBF32880F652AC22C75494A2D701F1DA011F51ACA429FDB
SHA-512:	B8B8ABA6485E2D859BC8E70726BB42449FB224D0593F67CE13B99BB7063E3ED3C028F476327D9A1B4BF8B620DD80CF1C1777694C4E9EB0F60BB500A9EE319D8E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .s...A./....."#.D.:-M>..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... .|i.....

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):	212
Entropy (8bit):	5.633428001301942
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ2f6zhcsBXIh1TK6tH8:mxRBJQtCDB0q
MD5:	34A61740DD3171DC672C61B4CDC2D4E8
SHA1:	EF07DB71664BA83B7DFDA04719564A11C8872D2B
SHA-256:	2FA62C4D289F1D3EF606FD2A0BE759D4692DB67A9ECE9D4351CE8C8ECC967CBD
SHA-512:	5F4F97D14CABE924610C2486632230784304020733483C7B83CEDBA78A4690EB62664A5CBE2463532CD142CCC9FBD7672C05FBC8512AD524B587F27175942681
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..n..A./....."#.D..KM>..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..E o.....#.....

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):	456
Entropy (8bit):	5.62417876948565
Encrypted:	false
SSDEEP:	12:3RrROk/su/UIc2H/HRrROk/sj/hBKMcm:3PJ/PO2/PJ/AhBKJm
MD5:	AB590F68A8031087B4DFE2038B3EE411
SHA1:	8C0E5DEFD6902068CBCF1A8AD3022ACBC8C9BF3E
SHA-256:	680766247B413ADACE2D28DC0D35A63844D57E40650D0BD949CABD124AA87F6D
SHA-512:	0EC9DCA3E80522FB60477B4FA81AA121CA0C35F98E246664E5DC405C54E2B09C30540973BAE01DFE99D41455CCEAB19F2ADA35B78C761D3B87EF2D1D66F9B4 9A
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .!...A./....."#.D.L>..A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....b.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..!..A./....."#.D..$M>..A.....9Q] .8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....v.8$.....

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:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.0695758994299425
Encrypted:	false
SSDEEP:	24:a8bPIDMyXGXMsJ4MamW9VHUElLnNYLkMKXlT8gcRlyJH2l:a8DabgMg45J9VHUElLnNYLkMKKVmc
MD5:	F5CB5E5BF6CCAE49B467807D153EAB68
SHA1:	38AFD5774DE9A2B16904FEB631D5F17EE7EA21A9
SHA-256:	10577A88CFC6DCD47D0DA7C9132C418E3240E602E936AD8884EE221B9FCEB219
SHA-512:	947E01C2C34C8663E0256FF5D232181F3E41F9FBC49E6489F29D2F9B279C87F3B081BB87877103B1348A2533219003DE8B8025A9139C00F0CD14E93E48A56257
Malicious:	false
Preview:	....qt.1oy retne....)........T.....3.....A./.....v...q.....A./.....C..M.....k.....#...(...k.....]...l.p..A./.....p..A./.....6<|.....A./.....<...W..J....A./..... .oB*....A./.....a.....A./.....;.y~A.....A./.....P....V....A./.....F..=z;....A./.....o.....A./.....*.....A./.....2q.....A./.....Gy.'.h.....A./.....k7A.....A./.....:. .N.A.....A./.....;/.....A./.....A./.....P[. q....A./.....,+..._.#....A./.....J..j.....A./.....[.i..%.@7..A./.....A?.2:..@7..A./.....q.@7..A./.....u\]..q@7.. A./.....!...0.o@7..A./.....*....@7..A./.....o..k..@7..A./.....^.~..z.@7..A./.....+.{..'@7..A./.....@..x.@7..A./.....*)....J:@7..A./.....&.S....@7..A./..... MV3..@7..A./.....+.U.!..V@7..A./.....D.4.@7..A./.....~.,.4>.@7..A./.....

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):	5.1494079541694715
Encrypted:	false
SSDEEP:	6:mB6Du3q2Pwkn2nKuAl9OmbnIFUtpE6nExZmwPE6UkwOwkn2nKuAl9OmbjLJ:/q3vYfHAahFUtpvEx/PvU5JfHAaSJ

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
MD5:	1F26DBE0B4A3281EAA8800E2D1EDA7B5
SHA1:	3A2085C048E0B26CA377E5B05F27F4B017660E18
SHA-256:	CFD9729D94E20FE1C2B511C0BD9FD88FC25AD47C7F8134BA92D12FCF7BEC26C9
SHA-512:	808A7F371019F2FD7A415B8B9C98E96E66C0D2AB06E061248394C3A53A2F2096C625586BEF82B6E4D89D08BEE2AAE86C013C768B847CF89B2F4BBBB00561F06
Malicious:	false
Preview:	2021/03/16-19:30:10.280 1a20 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/03/16-19:30:10.285 1a20 Recovering log #3.2021/03/16-19:30:10.287 1a20 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):	786432
Entropy (8bit):	0.008050090959268128
Encrypted:	false
SSDEEP:	12:I+mmTsx+mmTsxlNTpyxHHyTpyxHHyTpyxHHyTpy:TmbsmbPXytHwytHwytHwy
MD5:	03B3B4BB0F979E273B32ECC52C9B0E01
SHA1:	D307CEFF6AC7E7D3E424C1A855C56168596AEF69
SHA-256:	299FDCED8539A4D45595DBB33856A5A4045215BFECDD3EB7206996390C48C643
SHA-512:	4927E9663FD9AB3DB4449C765F0A55D33DFB51029B3F129E8FD1625C0C5F5593F52E59F180A5A0D1FE49D13C16D84EF3875FAB580375CADB6C5A4CF7439EDA1
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2103161829552-275.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	2.702521529040984
Encrypted:	false
SSDEEP:	384:hx0c/Q7olY+W0snfktuG18XDj1/O30KRKQjm9fS/xZ:Ac7lYlcH8XDjW0KRa9fS3
MD5:	A80A74FF3AA63AAEEF9FC19527BF3EC4
SHA1:	406C70ECBDD19E738136C8EB85C13DF08810FD49
SHA-256:	2369188D53D9B87540E5511D252196F3D685D24683D679F00ACF91E7D87F2AA9
SHA-512:	30987B9BFB2E3C2BC02CAB34A06D8E69DD86736EEE7DE191353294496A1FF29B817B3074C8B1910428F149CABF19FC63F70D21F1C9B201BD726EA036F3C52A0
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:	dropped
Size (bytes):	32768
Entropy (8bit):	3.448568453101604
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CKj49IVXEBodRBkWCgNOh1CKT49IVXEBodRBkWCgNOhm:HedRBuedRBpedRBUedRB3
MD5:	659254A3DA8AC9D2502A07D26DE08628
SHA1:	5404025277FB8F68668829267AE1B65586BC7674
SHA-256:	5FCF49D848CC9FF292AF2B358DC0226FDEED02E621CB29B9E8562BD851AC7140
SHA-512:	913450229A45C93892A0EDC43BED2D7D9795A12342FF4BD7950305FA900DC8821E490EABF50A16AE8669FE7DE8DC355401E3DE524298127526CBFC084ACDB02
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

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
File Type:	data
Category:	modified
Size (bytes):	34928
Entropy (8bit):	3.313553727600439
Encrypted:	false
SSDEEP:	96:X7CgOOhZCPJ949lVXEBodRBkqCgOOh1CKLt49lVXEBodRBkNCgNOh1CKZd49lVXQ:8iedRBVSedRBBCedRBByedRBs
MD5:	028C1B9783109D374A1023EED38673F9
SHA1:	0D1E121900632CBA88AAE48D1B24E28485B28C74
SHA-256:	B93124D7A1CD07817C571F270D93B7BDB520E84FDD59B54705A0539841CD115F
SHA-512:	964688E898143E5CDCC036AF0E62AB5BC03373171199649CBC32472BA91DE2C40D3587BC20824441214C5B4D1EF45E3BA7788072741B6FC578997923CAEC18B(
Malicious:	false
Preview:	.....o.x@..... ....W....X.W.L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZN6lU3pzewr4C5cxjYu1O8MEzImyYyu:J0GpiyVFihNGU3pze84TM8ME8dK
MD5:	2BFF64250CB0FE468269E2E38549893B
SHA1:	29CB98C8D8D0C8C4A76E4B6E6F271E25CC94EAC0
SHA-256:	717838C2DD4DE07142039E317BE6CB81C9B920BEF3B412B9A3C25A1DB240358A
SHA-512:	21CBAA75C9B2D37BCB1FC8B0FD5E1590F55F98BF5D0337F55B2323425F2003839ADEA69CDF771A7FDC4C2AF1A137C8C9188E03B721820FF94AAA05F489F0A11 4
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.794693762398311
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	T_C_CovidUnemploymentChallenges.pdf
File size:	64315
MD5:	9581f6aba2b67b091a6cfe9e8cd48c22
SHA1:	ff2da8cf7374b0126691d9973a8f0e78d9bca460
SHA256:	c15b0a6413b02f2d5ee4f6f14a872bb09c9e132d1309de1 5d46289bad4e683c8
SHA512:	7ace6a80321c95195778eb639c8722c68fcc85405a89f8d b567268817480e5103faa18ce6ccd9a7e962cd154e8f8d1 15e1ae7798e315813c01eeb173f8a331ba
SSDEEP:	1536:4V9e803J3xU8RcU1+/UQRbZ/h+lu15qKfS/CxR3c 8AeMBL:FF/I/3B1h+lu15qL/Cx5DQ
File Content Preview:	%PDF-1.7.%.....1 0 obj.<<./Type /Catalog./Version /1.7./ Pages 2 0 R./Outlines 3 0 R./Metadata 4 0 R.>>.endobj. 5 0 obj.<<./Author ()./CreationDate (D:20210312092411-05'00')./ModDate (D:20210312092 411-05'00')./Producer ()./Subject ()./Title ()./Creator ()./

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.794694
Total Bytes:	64315
Stream Entropy:	7.911045
Stream Bytes:	56007
Entropy outside Streams:	5.339292
Bytes outside Streams:	8308
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	65
endobj	65
stream	30
endstream	30
xref	0
trailer	0
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2021 19:29:38.310095072 CET	65298	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:38.361644030 CET	53	65298	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:38.657809973 CET	59123	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:38.709400892 CET	53	59123	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:39.996215105 CET	54531	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:40.047878027 CET	53	54531	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:41.040455103 CET	49714	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:41.089122057 CET	53	49714	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:41.846326113 CET	58028	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:41.895423889 CET	53	58028	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:43.359363079 CET	53097	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:43.410758018 CET	53	53097	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:44.332814932 CET	49257	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:44.381620884 CET	53	49257	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:45.129936934 CET	62389	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:45.182626963 CET	53	62389	8.8.8.8	192.168.2.4

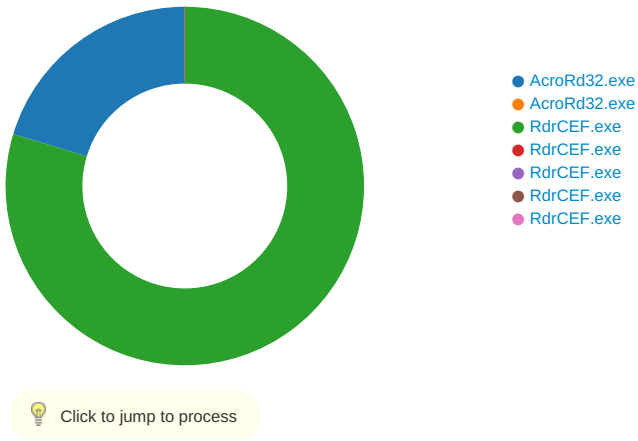
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2021 19:29:46.807971001 CET	49910	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:46.860755920 CET	53	49910	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:47.812777042 CET	55854	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:47.861828089 CET	53	55854	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:48.997679949 CET	64549	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:49.046602964 CET	53	64549	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:50.062757969 CET	63153	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:50.111660004 CET	53	63153	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:51.206418991 CET	52991	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:51.255177975 CET	53	52991	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:52.162094116 CET	53700	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:52.211395025 CET	53	53700	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:53.152676105 CET	51726	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:53.204591036 CET	53	51726	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:55.144221067 CET	56794	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:55.196017981 CET	53	56794	8.8.8.8	192.168.2.4
Mar 16, 2021 19:29:59.450264931 CET	56534	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:29:59.510781050 CET	53	56534	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:03.677939892 CET	56621	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:03.678833008 CET	56627	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:03.736769915 CET	53	56621	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:03.745304108 CET	53	56627	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:04.687402010 CET	56627	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:04.687743902 CET	56621	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:04.750106096 CET	53	56621	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:04.750660896 CET	53	56627	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:05.169404984 CET	63116	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:05.231118917 CET	53	63116	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:05.734152079 CET	56621	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:05.734266043 CET	56627	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:05.793066978 CET	53	56621	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:05.798295021 CET	53	56627	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:07.102490902 CET	64078	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:07.151248932 CET	53	64078	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:07.781152964 CET	56627	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:07.781208038 CET	56621	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:07.838495016 CET	53	56621	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:07.840991020 CET	53	56627	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:09.055058002 CET	64801	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:09.112042904 CET	53	64801	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:11.829946995 CET	56621	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:11.830058098 CET	56627	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:11.888609886 CET	53	56621	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:11.891204119 CET	53	56627	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:14.305504084 CET	61721	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:14.356381893 CET	53	61721	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:14.896454096 CET	51255	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:14.946276903 CET	53	51255	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:33.931207895 CET	61522	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:33.987694025 CET	53	61522	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:35.894659996 CET	52337	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:35.955509901 CET	53	52337	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:37.151098967 CET	55046	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:37.211328030 CET	53	55046	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:37.679092884 CET	49612	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:37.770977020 CET	53	49612	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:38.211878061 CET	49285	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:38.286093950 CET	53	49285	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:38.814047098 CET	50601	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:38.876137972 CET	53	50601	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:39.468961954 CET	60875	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:39.526561975 CET	53	60875	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:40.056487083 CET	56448	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:40.114450932 CET	53	56448	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2021 19:30:40.336036921 CET	59172	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:40.402514935 CET	53	59172	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:40.946918011 CET	62420	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:41.008764029 CET	53	62420	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:41.874397993 CET	60579	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:41.931701899 CET	53	60579	8.8.8.8	192.168.2.4
Mar 16, 2021 19:30:42.566399097 CET	50183	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:30:42.626810074 CET	53	50183	8.8.8.8	192.168.2.4
Mar 16, 2021 19:31:25.504364967 CET	61531	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:31:25.553639889 CET	53	61531	8.8.8.8	192.168.2.4
Mar 16, 2021 19:31:27.327406883 CET	49228	53	192.168.2.4	8.8.8.8
Mar 16, 2021 19:31:27.397882938 CET	53	49228	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 7072 Parent PID: 5920

General

Start time:	19:29:44
Start date:	16/03/2021
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\T_C_CovidUnemploymentChallenges.pdf'
Imagebase:	0xe20000
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	E565C3	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	E7AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	E6EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210316182955Z-275.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	E6EA85	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	EE83C8	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	EE83C8	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	EE83C8	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	EE83C8	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	EE83C8	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	EE83C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1hkj7s8_yn95y3_5iw.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	E6EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	E6EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1yef5qb_yn95y4_5iw.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	E6EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1c5y8mt_yn95y5_5iw.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	E6EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1fngk3m_yn95y6_5iw.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	E6EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1jenmqg_yn95y7_5iw.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	E6EA85	NtCreateFile

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	E6CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	E6D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	E6D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 \cTab0\cPathInfo	success or wait	1	E6D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	E2EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	E2EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	E2EA55	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	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/T_C_CovidUnemploymentChallenges.pdf	success or wait	1	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	T_C_CovidUnemploymentChallenges.pdf	success or wait	1	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	E7DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 54 5F 43 5F 43 6F 76 69 64 55 6E 65 6D 70 6C 6F 79 6D 65 6E 74 43 68 61 6C 6C 65 6E 67 65 73 2E 70 64 66 00	success or wait	1	E7DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 33 31 36 31 39 32 39 35 35 2B 30 31 27 30 30 27 00	success or wait	1	E7DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	64315	success or wait	1	E7DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	E7DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	E7DF47	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	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	E7DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	E7DF69	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	E7DF69	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 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	E7DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 7160 Parent PID: 7072

General

Start time:	19:29:45
Start date:	16/03/2021
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\T_C_CovidUnemploymentChallenges.pdf'
Imagebase:	0xe20000
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

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: 5560 Parent PID: 7072

General

Start time:	19:29:54
Start date:	16/03/2021
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:	0xdf0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	EE59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	1	EF83E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	38	EF8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	109	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	EE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	4	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	12	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	EE59E2	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	8	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1087	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	29	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	6	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	3	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	4	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	EE59E2	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	1	EE59E2	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	2	EE59E2	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	1	EE59E2	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	2	EE59E2	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	2	EE59E2	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	2	EE59E2	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	12	EE59E2	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	2	EE59E2	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	12	EE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	EE59E2	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	28	EE59E2	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	2	EE59E2	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	30	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	EE59E2	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	9	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	EE59E2	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	10	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	144	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	EE59E2	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	133	EE59E2	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	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	24	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	EE59E2	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	97	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	EE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	EE59E2	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	3	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	EE59E2	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	85	EE59E2	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	1	EE59E2	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	4	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	EE59E2	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	7	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	EE59E2	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	end of file	1	EE59E2	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	163	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	EE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	EE59E2	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	2	EE59E2	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	1	EE59E2	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	75	EE59E2	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	1	EE59E2	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	6	EE59E2	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	1	EE59E2	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	16	EE59E2	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	1	EE59E2	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	5	EE59E2	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	1	EE59E2	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	1	EE59E2	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	1	EE59E2	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	2	EE59E2	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	1	EE59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	EF83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6348 Parent PID: 5560

General

Start time:	19:30:00
Start date:	16/03/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,163317767862954 61319,720013116950749422 8,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1791496727330959911 --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=1791496727330959911 --renderer-client-id=2 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xdf0000
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: 6592 Parent PID: 5560

General

Start time:	19:30:04
Start date:	16/03/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1700,16331776786295461319,720013116950749422 8,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9225871105448414467 --mojo-platform-channel-handle=1760 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xdf0000
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: 6448 Parent PID: 5560

General

Start time:	19:30:06
Start date:	16/03/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,163317767862954 61319,7200131169507494228,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8257130289996470003 --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=8257130289996470003 --renderer-client-id=4 --mojo-platform-channel-handle=1776 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xdf0000
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: 1664 Parent PID: 5560

General

Start time:	19:30:08
Start date:	16/03/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1700,163317767862954 61319,7200131169507494228,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7449791400690600131 --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=7449791400690600131 --renderer-client-id=5 --mojo-platform-channel-handle=2000 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xdf0000
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