ID: 356983
Sample Name: IMCS Covid Program.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 20:30:53
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

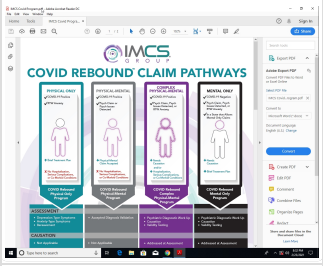
Analysis Report IMCS Covid Program.pdf

Overview

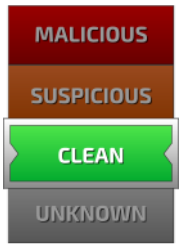
General Information

Sample Name:	IMCS Covid Program.pdf
Analysis ID:	356983
MD5:	7442f0868b88e0b.
SHA1:	fa961cb1acb493b..
SHA256:	2e6363947ba418..
Infos:	

Most interesting Screenshot:



Detection



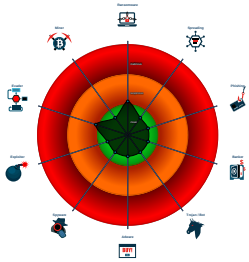
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Contains functionality to access load…

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 1560 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\IMCS Covid Program.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 1064 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\IMCS Covid Program.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5112 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6240 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=3499109752215329224 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6264 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4017212095282925109 --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=4017212095282925109 --renderer-client-id=2 --mojo-platform-channel-handle=1756 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6344 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10025927610161177688 --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=10025927610161177688 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6504 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4937386989897175714 --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=4937386989897175714 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6668 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8658298871532645 02 --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=8658298871532645 02 --renderer-client-id=6 --mojo-platform-channel-handle=2124 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

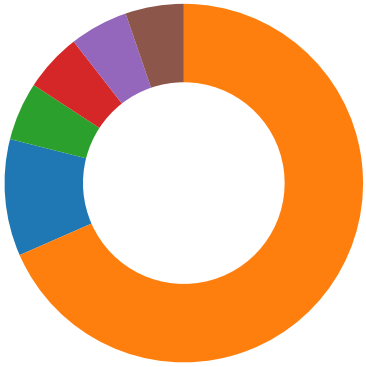
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

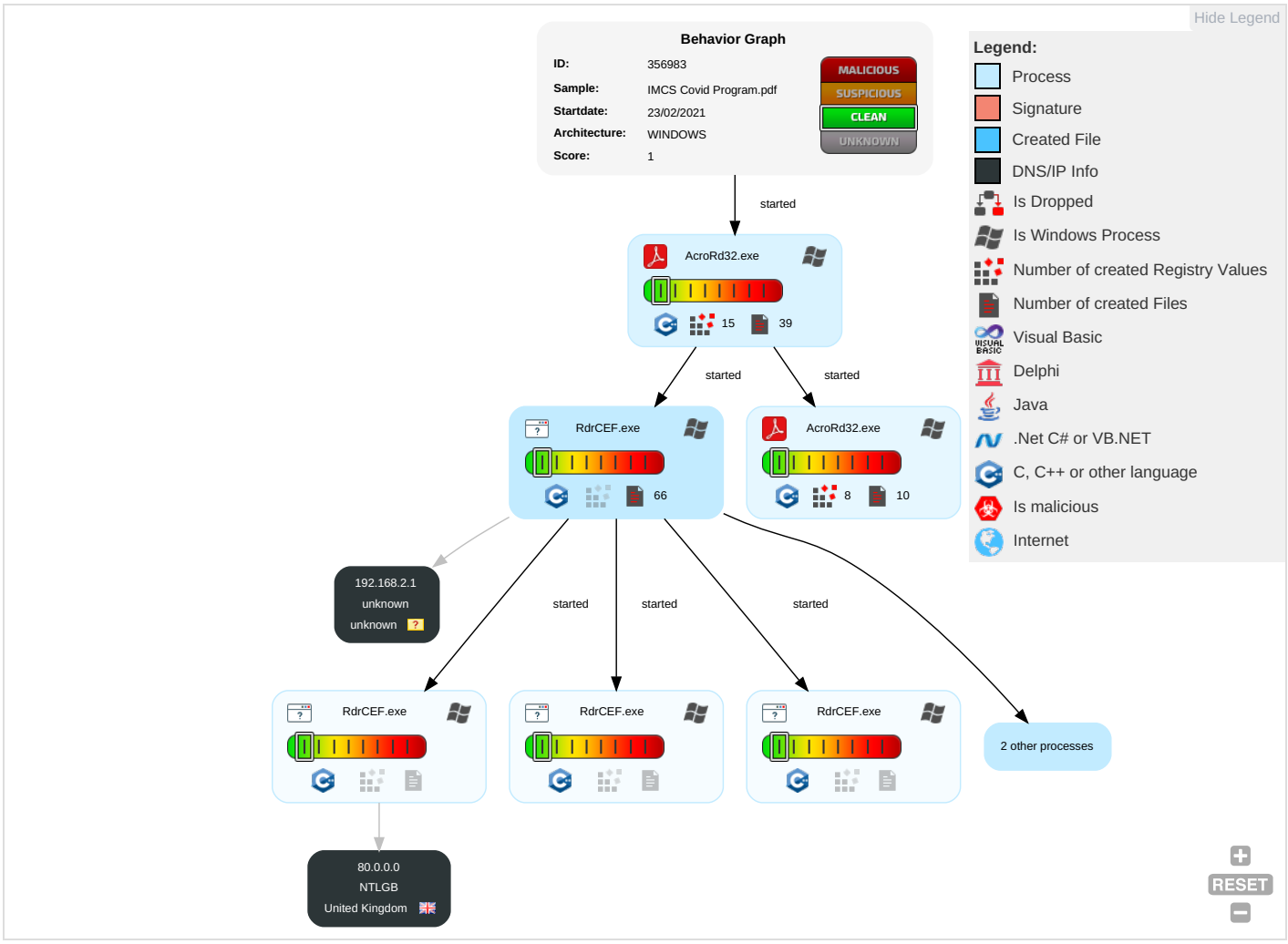
Click to jump to signature section

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

Mitre Att&ck Matrix

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IMCS Covid Program.pdf	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/&	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/Q	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/c	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/5	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://ims-na1.adobelogin.comS	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://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://ns.ad	0%	Avira URL Cloud	safe	
http://ns.adob	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/bx	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/z	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/s	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://cipa.jp/exif/1.0/Map_1	0%	Avira URL Cloud	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

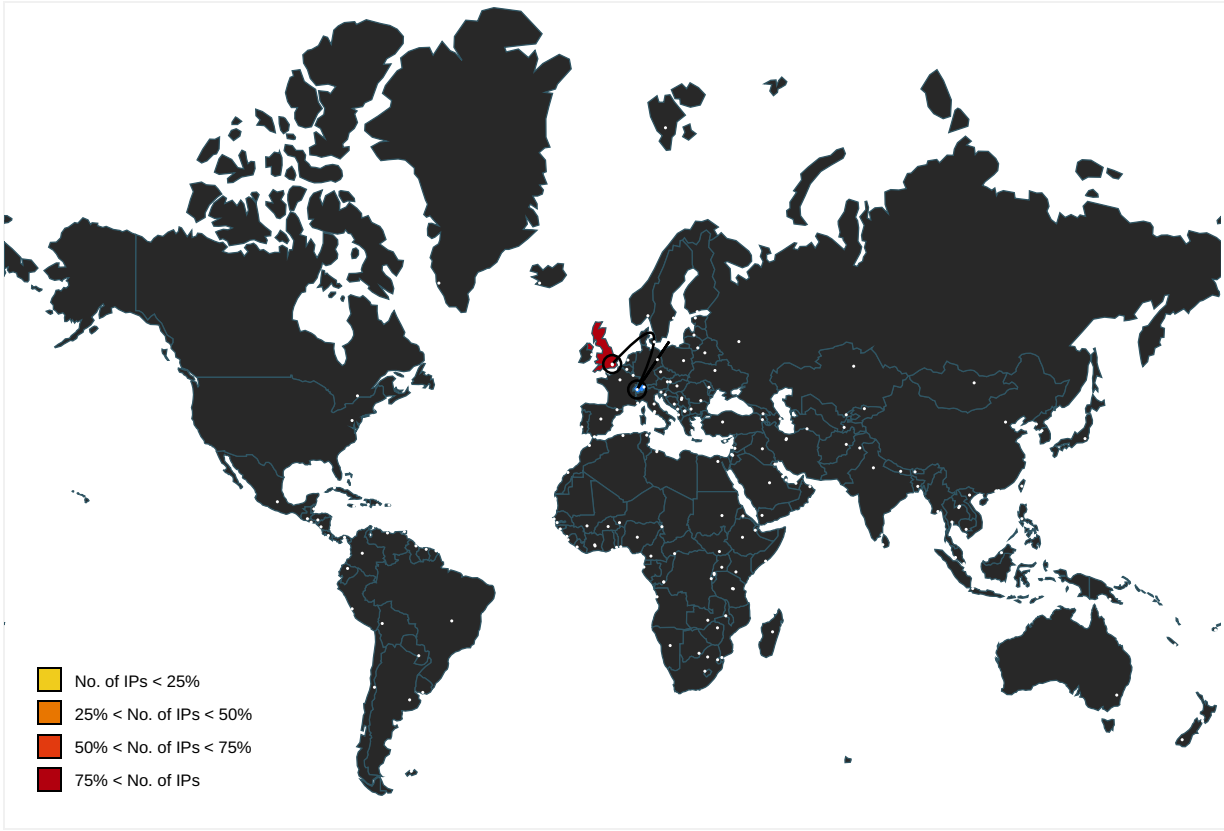
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/&	AcroRd32.exe, 00000001.00000003.212091877.000000000B16E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C	AcroRd32.exe, 00000001.00000002.428837997.000000000AB1D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/Q	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.433071944.000000000CEB7000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/c	AcroRd32.exe, 00000001.00000003.212091877.000000000B16E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.417386687.0000000007810000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/5	AcroRd32.exe, 00000001.00000002.433071944.000000000CEB7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.417386687.0000000007810000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.433223222.000000000CFAA000.00000004.00000001.sdmp	false		high
http://https://ims-na1.adobelogin.comS	AcroRd32.exe, 00000001.00000002.422232135.0000000008FF0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#1	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.433071944.000000000CEB7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.417386687.0000000007810000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ad	AcroRd32.exe, 00000001.00000003.211323396.000000000CFBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adob	AcroRd32.exe, 00000001.00000003.211323396.000000000CFBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#7	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/bx	AcroRd32.exe, 00000001.00000002.428837997.000000000AB1D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.useplus.org/ldf/xmp/1.0/z	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.433129769.000000000CEF3000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/s	AcroRd32.exe, 00000001.0000000 2.433129769.000000000CEF3000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpExt/2008-02-29/q	AcroRd32.exe, 00000001.0000000 2.433129769.000000000CEF3000.0 0000004.00000001.sdmp	false		unknown
http://https://api.echosign.com	AcroRd32.exe, 00000001.0000000 2.433071944.000000000CEB7000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.0000000 2.428837997.000000000AB1D000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.0000000 2.433071944.000000000CEB7000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.0000000 2.433129769.000000000CEF3000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.0000000 2.417386687.0000000007810000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#A	AcroRd32.exe, 00000001.0000000 2.433129769.000000000CEF3000.0 0000004.00000001.sdmp	false		high
http:// www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.0000000 2.417386687.0000000007810000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/Map_1	AcroRd32.exe, 00000001.0000000 2.433071944.000000000CEB7000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.0000000 2.417386687.0000000007810000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.0000000 2.433129769.000000000CEF3000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.0000000 3.212091877.000000000B16E000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.0000000 2.417386687.0000000007810000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.0000000 2.422232135.0000000008FF0000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.0000000 2.417386687.0000000007810000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/)	AcroRd32.exe, 00000001.0000000 2.433071944.000000000CEB7000.0 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:	356983
Start date:	23.02.2021
Start time:	20:30:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMCS Covid Program.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:	40
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

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@15/48@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 131.253.33.200, 13.107.22.200, 40.88.32.150, 52.147.198.201, 23.211.4.250, 23.32.238.136, 23.32.238.123, 23.32.238.129, 23.32.238.113, 23.32.238.122, 51.11.168.160, 52.255.188.83, 184.30.24.56, 20.54.26.129, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.190.160.4, 20.190.160.71, 20.190.160.134, 20.190.160.132, 20.190.160.129, 20.190.160.8, 20.190.160.75, 20.190.160.6, 93.184.220.29, 51.124.78.146, 51.104.136.2, 20.190.160.2, 20.190.160.73, 20.190.160.136, 20.190.160.69 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, e4578.dscb.akamaiedge.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, ams2.next.a.prd.aadg.trafficmanager.net, ocsp.digicert.com, login.live.com, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, settingsfd-prod-weu1-endpoint.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:31:45	API Interceptor	14x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSljf0v9YP9XHTo1mHg1DdlnrlGItn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	

Domains

No context

ASN

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

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.645877194808745
Encrypted:	false
SSDEEP:	12:vDRM9B1iLZiEaDRM9SfzLZiEQDRM92LZiE:7BUE4DzUEmpUE
MD5:	C2B0AF2B71EDC059E6FC08D6B6AFD2B6
SHA1:	D3E25A1D1900C343EC02CDDD0C2C1495BC5704BC
SHA-256:	51A8C558A16574DB502EF7D43C6C52D9A70C31B5F55F72AEA4D169BF303DACE6
SHA-512:	71903B3A4F9F67128B73BBE199FDAF05D7340A3572A02960173CE5EEA7CA4340557FDAFCBB770CE87D319255BB8411D155E18DDFEDA0281A2ADB25D058D0266 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...e../....."#.D`.,u..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....I (.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...../....."#.D....u..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... ...H.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .S..../....."#.Dr7I.u..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... A..Eo.....irVV.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	5.634511855829325
Encrypted:	false
SSDEEP:	12:V9zyK84x9PQkcl9zUjGCli9PQF9zIr9PQVV9zQ9PQ:XzZ8o9PQFnzU6Cli9PQHzIr9PQNzQ9PQ
MD5:	C63E777A5D060DBF200A2EE65DFA48D3
SHA1:	5CD317A0131689A49F25C7973D3064C8B2EC6E3D
SHA-256:	A31694CC65BB210B0471039AE59F5C2AC639915A1ACFC298A8612D4ABA659A99
SHA-512:	376EEAA536044F5C44C759159A07E6C030CE5F8EFDBC2C61F44AE17B9C7E7A33FF9D4614E005A66DE4BAED56C1C4D5B87EF3D1807EEA5ACDCBBE1BDFB10B 0367
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../....."#.D.]..u..A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna- resource.acrobat.com/init.js .I.P../....."#.D.{.u..A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ... p../....."#.Dy.S.u..A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....Oj.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../....."#.D.9..u..A.1.x.'.vl ..*|Z..o...+.4....0..A..Eo.....A..Eo.....$.d.....

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):	738
Entropy (8bit):	5.594296575901893

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFDwlUo6jNyeRVFAFjVFAFoxNiYlUo6j7yeRVFAFjVFAFPBL+R0l8:tB4v4ESBDB4v4IiYSBFB4v4PBLLSB
MD5:	FCD2ACDB3680599292CD96476FF8FEBA
SHA1:	A3A881A03FE845312503118F7F52A1C7D6DD460A
SHA-256:	4D648A92C16654578D8A42381146388B87FE0F1157BF8490EB6C413D9BACCD90
SHA-512:	FB87E755F6858614BFF5F244C2384F6608F9E293ED505454ABDC8C67FE628AB96C5949115FE49559EAEA25244778FC7CBE816A9B62FEF02AEA85A61788634CCE
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 ...c../....."#.D..(.u..A..hvDO.N.t@.... .n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/ selector.js ...../....."#.D...u..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....V.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..'.../....."#.D..A.u..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....TSy.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.650561115995741
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsi9gJiWulHyA1TK6tz:IbRkiDaoWussp
MD5:	45943A1BD8D965477C09907B702FB06E
SHA1:	9AD91FE5115176E6E65B88B4A1802E45E58FC1B8
SHA-256:	8E3DFC1A98252A4891DD23E1304256A8F344AAE27F6AFF4F2CFA4C3FB9745429
SHA-512:	0027FA79BA2A15A561E87F680D396D1748ABCDED6DAD39A70FA4EAE85B6C437CBC71D9D8BBD891435942BD1359ABE4AD6B7D4855C238AD916B19D584213332 CF
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 ...../....."#.D..u..A..8 P..a...R..Y....7.@..2Dm{..A. .Eo.....A..Eo.....O.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.58574125970802
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVutTRVyh9PT41TK6tRAe+yiXYOFLvEWd7VIGXVuKIZDRVW:pyixRudV41TE/AhyixRu/DV41TEDqt
MD5:	87B361866632EC905FE4FE56C4BEC93E
SHA1:	C5B4503B0B88C7B73AA83E72EF42832FDB626CF0
SHA-256:	272DF481E5E2DF46F182B50567D79DB1B108E7AA14CC4D4196A77BB77684F6C2
SHA-512:	8706A91DD851E4AEE0426B99D8A85A8D2DA060F8F94A1511E799372DDC336BB033672BBE92AB58F9875D86C25B2D19E02CC5A146E3D9AA298CC2815598F8A31
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...d../....."#.D.*+.u..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.. ....C.d[.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...../....."#.D.#C.u..Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....d.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.59018790699387
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQJ/+V64LZIl6P41TK6tNNMvYOFLvEWdhwjQHkvLZIl6P41TK6tB:0RhkO/4LZCNqRhkOkvLZC
MD5:	964EC5A28BA1951AED53CCDF6344CC1D
SHA1:	87366A248A0B822B416DF2250136EF2E0538F76E
SHA-256:	C5BAB40C4EDD5F89735870F2D8BE264ED7DC0CE4A72A0C6D6B5AE37875A6659F
SHA-512:	B3C2E3C32CC641DAED864A61FAA0AC079871D5AF28FE796E74220F6AACAC4A94648C249C60AA989B231FED68BF2365025771834C117EE7B67663CDC36EB12D A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .._../....."#.D....u..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....3y'.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .8..../....."#.Dp"1.u..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....0.1.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.513399618717739
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQMCuHlPV6g1TK6tSJYOFLvEWdGQRQOdQ9oCqV6g1TK6t7:2RHRQCRCalPV1ERHRQCooCqV1d
MD5:	38AE88B20A4A968D598629E2054A8534
SHA1:	2BD9198F488A95D320EDB9C51BCE887051772A07
SHA-256:	5EFA5A5AA4847EDA5818C766E74ECCE630E8CFC53479E23CFEDE5BDD62BD1E2F
SHA-512:	9F4CD6331ECA538F93F8311F1B4E4E659309D20E07435C94791C95BC72DBA19CDE9E96D63038635370951AC740636F9E45A099024134566C81A7A2EF2E3739CA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...d../....."#.D.A+.u..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....V..y.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .#..../....."#.D.<C.u..A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....K-.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	716
Entropy (8bit):	5.605050306970696
Encrypted:	false
SSDEEP:	12:Z5MUMuR/EL5MYrMuR/EhG5M+GfIMuR/El5MTIMuR/E:ZSNuR/ELSYIuR/EhGS+GfJuR/ElSTJum
MD5:	4C982389C52203AD6207D9879C191B77
SHA1:	C2B8C70EB83A8CAA365EC36F85502C9CA1CDD5C3
SHA-256:	D4791631913BCF5C667BF930D44384025B5AF1B13AD45C3892ECA880E165C3CC
SHA-512:	D17807C59E00868029C0E7EA3743BFD6C390CC422BBEB6440089F55BBA4CDAC08F3C756905DEDC36D8137C76F53A1E4427ED7CC49D02E9F7A428589EA87B6CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .19../....."#.D.K..u..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....[.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...P../....."#.D...u..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....z14.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .E.p../....."#.D;.T.u..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....6P.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...../....."#.D.M..u..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.588513135829259
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu8W+m0bbsIDMGH41TK6tk9//:XfRMGSKsIZEC/
MD5:	1779EE17B68B5D5C100C765135359894
SHA1:	00EA1B2F96D01D3CC76BC9B1B166327CE02B141E
SHA-256:	DE743A4565DAD7056FB488FBA8618F5AFCA2832A97D7802807F83799AF9766CD
SHA-512:	C8F6272B10ED2AE34B5B8D7F9D4174EE3827AF7C066F7F3B23605CB3F58BF176B2DA15FEE72EF04A50502AFE9CB2B7F0B5B039BE0D7FBCCD51C428E9D58DA171
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ...I../....."#.D..A.u..A..`.....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....*.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Size (bytes):	428
Entropy (8bit):	5.531166895720577
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtusI3by0zBUKSAA1TK6t3e4fPYOFLvEWdtuq7B99uby0zBUKSAA5:pRDmbe9xRtVube
MD5:	85BDB77881C2B499DA366329B1F3ACC5
SHA1:	0FC7C65A93766E218F853C86C80FDF30B7DC66D9
SHA-256:	0498DCC341FA8709377F1B6634465EE7BA2FD607E46152B500B3720ADF337167
SHA-512:	1170C78CBB75157D867F84C544CED6D9B0A87EC34AEC3F19844B339ECE37D187838DF00CB433DEC08F6E1D810BDE8BF4DAB23D286827573319B5DAB171B0A6D1
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .n.f../....."#.D..(.u..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....V,,.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...../....."#.D>zC.u..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....AF.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	708
Entropy (8bit):	5.565444297585538
Encrypted:	false
SSDEEP:	12:KkXxKMSCvlyctUlCikXxKMSCvaStUlqakXxKMSCvCihotUlQkXxKMSCvImzotUl:KkXxiCtycWCikXxiCSSWNkXxiC6iKWQy
MD5:	EC91322451C7ABD2C62105CA61E7BCC2
SHA1:	D7E32F1C56B99D3DBAC21BDD3F5BF16BBD8EA791
SHA-256:	A673E215BAF95E56A1D2C50CA6B01BBE35622188724B72D41FE9209ECEABF4C0
SHA-512:	B944A755EAA83FE85A159750B72FB2939814 76CA36518201926B28D64BA11FC656DD185D111CB203A8415E2204D46A1998AC28CC254AA1A21C0C2158D07BD8C
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..*.../....."#.D....u..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....<@=.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .C.P../....."#.D...u..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....L.]v.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...p../....."#.D..S.u..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....n.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...../....."#.D.F..u..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....9R.....

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):	561
Entropy (8bit):	5.608549412586817
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLGETWyyM+VY1TK6tV2kl9YOFLvEWsfOL++EyyM+VY1TK6tFklP:5h6OLzWfkPJh6OLJEfkQh6OLQWfk
MD5:	27FBC7AAFBED128665DBFCA36D7F7C42
SHA1:	D817B4537821709E67DE17B8731052BBC37207AA
SHA-256:	A41EF105DA4FC6492B3C79A18C11B7A566247634F2BA34D4BE65FD17AB4C9036
SHA-512:	F9AA541077611F41921810606C37683D8685B3D658569140BA3C8FCEF727A58977A0788EDC6F37EF72B046AB0F6B9BB0E4FA69DB07E16E8741B345EB16831C5B
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...[../....."#.D5y..u..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....A?!.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ."}|../....."#.D....u..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....e.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .]H.../....."#.D$.$.u..A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	732
Entropy (8bit):	5.641839352986289
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFMswSeKaTLn0RVFAFjVFAFIwSeKaTLnARVFAFjVFAFNwSeKaTLnw:UB4v4MswzXLn0B4v4IwzXLnAB4v4NwzE
MD5:	2E211836EF371E1C5E9215B4A497327A
SHA1:	849A2B381B599BAD57232303D2CBAFDBAC762934
SHA-256:	B01D4EAA90273B6B15CC362ACCD60ACFFA9886125415EA9850FFF1203B1B8C44
SHA-512:	85F4D9EAC49DDF8B70F0563E201785752A98FACA8A9E634E8CF91332A98F442C8DE70C7BA637E13008C548EBE8C58B5FD86D4D842D80572E6867788D2232B3F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...d../....."#.D.y1.u..A.....H...{...2.. /.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..8.../....."#.D*...u..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo..... .....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...../....."#.D.vG.u..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.493686232392832
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQQZ5GFCaa+41TK6ti:NRMHdhZ5Gda+EM
MD5:	223EDA06877360D89576B063E8665BE3
SHA1:	6E5D53C487C00A08A5EAA290C3C25A804E0793FA
SHA-256:	75B684DD8FF10F59A73A2CAFBD2FBE6FB737EE9A72A4554C324DB4BC767C6E98
SHA-512:	F6BB7B0AB5025F37128D8782079100E5441207E4094AD7D9FE7C738B8D81A6455377F5C04F38E2D135904498CE66EA6EF300E35235EAA98963709CB0D544D483
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ...I../....."#.D..A.u..A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo .....Q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.517428890519337
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuUOY11TK6tJl2s2VYOFLvEWdvBIEGdeXunCOx511TK6T:BsR2EseMG7sR2EseECOxX
MD5:	EFBFC8A771CA3B03FFB3DD8E70EA547B
SHA1:	1B6F46AA1798EAF692694D1DE28DBD9BB8B8AC99
SHA-256:	26716D82CD881CFAABB1F9D499E360FB4F5893F022E1C44B9F59D10A8286B02E
SHA-512:	4A2AF0AF1853F01F29A845583963A3E53A17AAB041EC9FC19D4E5765CE1714940DE0E11852B9603BBCB59805AA58CA7A76C513D6ED4B58419E9105A057C1E05
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .b.c../....."#.D.,).u..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo. .....W.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..p.../....."#.D.wB.u..A.A.o]@r..Q.....<w.....].n\....A..Eo..... .....A..Eo.....X.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.658256600228183
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQlce+B7OhKlvA1TK6tX0aVYOFLvEWdwAPCQXba+B7OhKlvA18:RbR162KBJk9HbR16yBJkaP
MD5:	B1C0A73E4ED6D25E10592770CCCE861D
SHA1:	8AA4676A861A6C75C3654F1767F1D08E068304A3
SHA-256:	979DE404BD3B93AD5D649B913C5BD9ABCE3D540412EA97FDBBEE7FF6EE102C43
SHA-512:	9ECFD6BB76B5E8A9F7076A60FFBE11B69B742ECE49F77C449B73969C022D9DA6D0875B8106F5DA6371635146C1C2724834566DE2F8961C6800723E781A387589
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..r_../....."#.DM...u..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....r =x.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D..0.u..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....I .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.580325562604868
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVumQdFt1TK6tgXMs2gEYOFLvEWdGQRQVuM9kuQdFt1TK6tG:B2geRHRQ10OX72geRHRQ39ku0
MD5:	C16F3ABA79EA0EAE0D65DB0058DB2413

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
SHA1:	2A8F9136C8B0F4FD59C69E32C44713A976CE2A09
SHA-256:	CE0E9F9D1030ED8BA042CD4B0688AA53CF5EFE49F7F481A897D665F5995BA1A8
SHA-512:	5B9330ED9A7CC2F583C7B9E8682F52144A2428414BBEA24AC1490C9B552AD7221068A3D37447EA17F23A58458ACD872C401AFCCA819BD33DD2587B0D9A9BBC6
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...c../....."#.D.#).u..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....+.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .SO.../....."#.D..A.u..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.615832929359149
Encrypted:	false
SSDEEP:	12:WyeRlhN4t1wByeRl5At1wtyeRlmMyt1w:WJj4fwBJKfwtJuMyfw
MD5:	CF3FE99A850C7B2EF2A5C73F1FB3E37A
SHA1:	BBAEADCD91F81DAC13224BD8FE4D34AB5FCA67F3
SHA-256:	DE561E31A37F240F0BA95219F6650376BC1D5EFACF8BC04BAF3997FFFB7E6499
SHA-512:	775DD05F8F7BAC2DC32365937CDC2B73FCD624923938A937D6A3222048FD41C06D3C6AA135F93E6E07BCED8D4B8CF50C6C7EA83120CA147BEFAF0DCE207FD6C
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...]../....."#.D<...u..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....7.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .,C~../....."#.D.]..u..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....j.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...../....."#.Dur).u..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.579759365764417
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu9oxCqwK+41TK6t4nYOFLvEWdhwyutZfCqwK+41TK6tO:wRhCUjwK+E0RhkjwK+Es
MD5:	A64DC48C3F82F901D2186888726682E5
SHA1:	90B3943DA20113E1AF2A3BB68ECDBDAC7951F194
SHA-256:	907E4B5E6EF86F46E3F6F8DC941BEE95AE72FDEF29C608A6AD07A2E007247FB6
SHA-512:	ADF6EB0D2134A7DEF9B071CC0799FA692C383D7CEC824F88B30F6FFB0670F0FAE3C0907CAE4235BEE1EA4C365161574373053F28F020CD16033D1D7D3963CB
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..p_../....."#.Dh\..u..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...../....."#.D@.0.u..A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....1.....

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):	690
Entropy (8bit):	5.576353339397787
Encrypted:	false
SSDEEP:	12:/RrROk/3fLErvRrROk/FYfLEwNRrROk/SBmrfLE3H:/PJ/347PJ/FY4EPJ/cmr43
MD5:	4D5FCE05E2FE2ED963AB0E1532A0A3C7
SHA1:	CA123D75F8D35AF2D8E7CB91023D092884F3E972
SHA-256:	BD57068AB96423815FD2F8AF8D8DCA5CEBCA7D570AEDA97C771D9E9ABED1FAE9
SHA-512:	BF46D60F912CC2E3AF9673E2983E5F07BCFDEC198A6F65F4EBD1A3AD2734CACA5962B18280FF6BCFF5203E189E0EA037B1C409FC6B7B112D8E4C218BC85035C
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .f.]../....."#.DM...u..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo...../.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .gA~../....."#.D.K..u..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....5.K.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...../....."#.DrO).u..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....M((.....

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):	558
Entropy (8bit):	5.626041709166186
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIqOi1QPLr1TK6tCf2mDEYOFLvEWXI4D1QPLr1TK6t6EmDEYOFLvq:xqTHjCPLnofBqTxCPLnkqT9CgCPLn
MD5:	870C62E0240998C7A0859C39F4CAC559
SHA1:	970F3C133E4D9037AB838B84BC4F1B804F2A9A45
SHA-256:	5A7F003D507116A6E0AE27ABB83605C1ED7A99BDCADB25F805197EFF5431B5DA
SHA-512:	AFFD0A00D7414294C38549C9BAB67AF151C747C3B44361C05BFE27EC806FEEEF123E51525FA099F5C9EC5D8C5F6FF59A2E00A8D71D15B4CB07BF3FFD3789AB6
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...[../....."#.D.k..u..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....5.}/.....0\r..m.....:...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .Qp|../....."#.D+...u..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo....._-'.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .z;../....."#.D..$.u..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....IK.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.654718675433459
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAu9esEJ41TK6t7S/E52YOFLvEWdMAuu2SoZsEJ41TK6tw52YOFLT:zRMesDxiBRM+esDnRMNsD
MD5:	6942DFA4EB6E43D03BA90D7C54426405
SHA1:	7B9721DE0243A01AAD576E92B95D5FC742AE0D65
SHA-256:	10BF8A88F92B48D93742EA2EC686649DC8A0245BCD7ACD7D68A3F38D02A85001
SHA-512:	1CD67FCFA8A31957C9CCFA197A1A4E530FC4C877FEB5C84FF256D0E8AE69B89F5D9D941870688FEF073854DB9420A5B2E95E7A8D9A0061E8D7568EA2ADE2972
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...c../....."#.DJ.*.u..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....n.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..G.../....."#.D...u..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....g.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..|.../....."#.D..B.u..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):	630
Entropy (8bit):	5.5786650628576195
Encrypted:	false
SSDEEP:	12:6lJRTLgESFoMzlJRaSFoMilJR2AsSFoM4:Y5LhSFoMHYSFoMQE3SFoM
MD5:	B2673D2098F49C54F9372F264FF4A61D
SHA1:	6FC1A88351C921AADA31EF2E50F0539627CF80D8
SHA-256:	93680014A002D07940166736A83DE704ABC11AE693AD6F50ABD1898713D8B1D1
SHA-512:	D0C3936F7FE2CCE8843EFD592AC65924F3139C7D5D046723E127F0908875C2EFBDE4FCB21008F95B220F995EF866C1127E861FD95D2BB0A740F8D41E9F18E07
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .b.c../....."#.Dy.+.u..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....R.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .J..../....."#.D...u..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....\$.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .F}.../....."#.D>.C.u..Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....H.~.....

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):	669
Entropy (8bit):	5.603448963106684
Encrypted:	false
SSDEEP:	12:F8hRrROk/NRce2q8hRrROk/y9p+e258hRrROk/lo90e2:UPJ/Dn2nPJ/y9/2APJ/2B2
MD5:	207216AEB6BD04AE1D67F621A7CAB32F
SHA1:	8E81596532BDA563BF4B461CC972932C2D8378A5
SHA-256:	5FC0954579F4CF8EF717989660C27D474399F47F43E24361456A9521AB32B1B0

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
SHA-512:	E90BF03CDE52724868DE167666228040A1F4FB08F1933916650C1B274355F05C04EB380C931DBDEA83593B555E1D4B31A2230DB394DA33847C291AE8FF4371D4
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..]../....."#.D....u..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....z../.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...~../....."#.D.A..u..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....A5.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...../....."#.D.D).u..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....T.....

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):	639
Entropy (8bit):	5.69757486270723
Encrypted:	false
SSDEEP:	12:ehRcbrNJICxlQhRcn9rNJIChhRcPjXrNJIC:ehqJICxGhQfJIChh89JIC
MD5:	2DAC5812C03259C3E3AE9DB29FABA796
SHA1:	04EEAB03EFE92B8261B4623D780A07CEF2E1FE9C
SHA-256:	2C3C0A08079B2579B009F3070184962DCC69B4DF01F7638985B4DDA8F4CAC057
SHA-512:	FA8E776A807FE6F59FF9D96AB46C56D399CADC9451513C9A41EABCF67B2039ACA9318674037B60C3E78BF63B7E1E4F789DA3D93AB14C139F4F53C7AF94AE63 9
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .`.]../....."#.D!>..u..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....o.4.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .1G~../....."#.DZ...u..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....'mS.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..9.../....."#.DK.).u..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.602548678447639
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuSm0oGLzgm2d/1TK6tcOEYOFLvEWdrIhuFl92bLzgm2d/1TK6s:0RQmuReERZo/ReNRtsk3ReX/
MD5:	627148E944941169F275421C152F27F4
SHA1:	7EAD206A8C7752A2675460EE40E0AE786D0E5513
SHA-256:	DC4E5DA7BD3FCF1C78ACBAA0241BFFB82E8E27DA649384214942A37A2B10B7B2
SHA-512:	2CEB9181C9332789319CDF362F9A02FB7150CCEA433FAAA0148CA669849530E8097A8D898A96FBED32275A6D4FF470F8446C64A2DAE265AFD530AE5FD545338
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..[]../....."#.D.W..u..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo... ...6..F.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .G.~../....."#.D}...u..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....n.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...../....."#.D@.).u..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A.. Eo.....A..Eo.....D{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	752
Entropy (8bit):	5.625513041419824
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KcLXkx56uvp1TK6tbt5AElVYOFLvEW1KQkx56uvp1TK6tyMAElu:6JJK6YZJJKHQwJJKx9wW/KJJKsF3IV
MD5:	378ADA1377236ED01BF029E04064FB56
SHA1:	CBBC258FD6242B7D754C8483CDB7D9E27D26B736
SHA-256:	6F1DE5DBB69944F7AFD6FC6C1C0BDF32263E8ABE0708C15416F1EFCBF8025EAD
SHA-512:	04AACC941BE361589E5F4BD307ABC92E2C2A0477B1A96202FFD798F5F9DA9AAB119282B8B364BE87E4CBA709D3E0D8B2B0359E65C6CB32C9D040A5DC6D28C 2A
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..C$../....."#.D\.S.u..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....u..Y.....0\r. .m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...R../....."#.D...u..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....;c;.....0\r..m.....<...)6. ....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..:s../....."#.DO.h.u..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....)o.....0\r..m.....<...)6..... ._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..b.../....."#.D6Z..u..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....vU.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.632481583736704
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuTlNNhUDLYtmOZn1TK6tmEWYOFLvEWdBJvvuThCvhUDLYtmOZQ:xRBJYkDcFZLWRBJQUKDcFZL
MD5:	CC6B2C9E54CE98C0C45898719CA7D285
SHA1:	ACFBBDC681DF3BC9D7C8426FAD49D15DCB41922E
SHA-256:	5D67628ADC5BC250BF30487A2B6386E04C4B0F72F62408F9532D3A1A888AD15F
SHA-512:	F1137184A87B9B066FC0B4F3A3B4D7C0179A2ECA65E475EE3FA3C6575833D1BC718083A94813635F95E5802D0C27ABC914F6DE3AD05606ACA9520E54A8928BE
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ._.c../.....''#.D..*.u..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A. .Eo.....A.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..r.../.....''#.D..B.u..A....t.q..W.EZ....1...[.zC.7mD..A..Eo .....A..Eo.....:.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	844
Entropy (8bit):	5.622719268622842
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp72boHVPu1TK6tKEsRPYOFLvEWIa7zp7lTGVPu1TK6t7kl2sc:BPHwbCciPHjacelRPHKRc8PHiLrc
MD5:	14D3B9020764A48047AE5EB105F9FE10
SHA1:	7B4BDB7F66D60D2F456D14459D2A33D0A0133C56
SHA-256:	926FEB87090A35D1587E41C4097359B72A95130C9D36FD75C44023D285119273
SHA-512:	3E8ECF5A7FB736F40BBD8B72D51C8C3CB031AEEF1EA6B6063A4312C4C397DCA142358D85B82699CFD4F9E9C7EBC5279CE9B11495B381EEEB7C0F8BFB0F9E2 F84
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .z..../.....''#.Dg...u..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo .....<.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .o.P../.....''#.D3..u..A...L...Im.@.....E.nW...IP..A..Eo..... .....A..Eo.....{.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...p../.....''#.DZ*T.u..A...L...Im.@.....E.nW. ..IP..A..Eo.....A..Eo.....3.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .t.../.....''#.Dqu..u..A...L...Im.@..... ...E.nW...IP..A..Eo.....A..Eo.....f%.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.60460127510047
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QBk3NiM3Y1TK6tuMKPYOFLvEWdENU9QfoCriM3Y1TK6ts7:bJRT9Ukdr0sJRT9mr0e7
MD5:	56C526BCAE014C9986DA7FE5C0D996DF
SHA1:	2EF0D9A5FA518F0C8A52354B7F0C2E7F8D2BCBB2
SHA-256:	74960BA0E64988F77C645E9665536869E4E35B83C3A320151D89CDAC85A52EDC
SHA-512:	A4D54C16D40D331C086DCFFEDD0B7678DE891EA17C4E57A9A7D4B454837C402123B5558BD856036051C777A3BC266A8B659C1FF3050BF7D7EF7952A288CFD5
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .''._../.....''#.D....u..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.. .....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...../.....''#.D.!4.u..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... .....A..Eo.....F.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.6206343585508645
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQpcjBRCh/41TK6tiQt6EYOFLvEWdccAHQ5NoCGDjBRCh/45:XRc98cDi/ElRc9WIDi/E
MD5:	3ABCE2A065E2233F48948BA1033A8BEE
SHA1:	656516FA42A39EDEAD6B5D36960A468B74C97342
SHA-256:	1E9CE727F4AFE172841F86D80583FA863E719217CA14135914A0FE8D2876253C
SHA-512:	3D4795C40CA5DF9A560ECA2B65C13CB810296BF8498DCC5B07E9B3A0CF62032DB5E863B5DF751B5CEF5782A075006451B05F59B8B6034133FFE26405B558F44
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...d../....."#.Dd]4.u..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....a.c.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .g..../....."#.D..K.u..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....y&.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.538402004951801
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhurpZX0ULlF4r1TK6tuN:bs6xRkinRLlF4nUN
MD5:	AD3F7F55680A2C0CD7E4F2E71FA82665
SHA1:	7D1D4318F8F2285A0DFB516982A5EC2A34519897
SHA-256:	9F3C91DBA3271F2F14C9D4873F54FD2B738E99A1DCB4CFCAC49250357B8CBC7F
SHA-512:	B6CBF9E1CA699C47199DF6CB056CFB6472ED680AEA773F0DFD677D09A0F66AB4275A90639F0F78684A4089EE5EB044E88A1C085E99369195DB0A1A2D53E9C920
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..~../....."#.D7n..u..A.P...#4..l....5...5..).w.. .h.~ ..A..Eo.....A..Eo.....pJ.1.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.550665185528169
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuBY941TK6tW8//MhYOFLvEWd/aFu1oGClPUqY941TK6tYb:WR89EUdR81Pm9Ea
MD5:	60F3D3CBD074BAD037C875B2F2832D66
SHA1:	3589995215201B0BEB0904C862CEDEAFDA9FD8C4
SHA-256:	F81826071B6C4F75456F699456C5BC317565EBE3A2B2C4A2545EBD69D9185072
SHA-512:	6F22EC19D119B2C5B606108F9A8D5A660BB082B561C6D23C7779D94DCF4AB487A2E8319D9DB77938B2EA6174DFFFE49137C9F7978A1E9A2E3F6FD1A383DFEE8
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..=f../....."#.D..(.u..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...../....."#.D#.C.u..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....1>.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.535139260156776
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ0oBMqVd3G4K41TK6ta/2R9YOFLvEWd7VIGXOdQ3OC9YGh:2DRuRWB9Vd2k8/mDRuRL5B9Vd2kq
MD5:	E55FF8B84862403FF475C1125FCB132C
SHA1:	71C7352A05CD751BA2783F81A2FC99E652EC4798
SHA-256:	77170E789169A8DE829B247C17A220223CCDA61D12B4A59C98ED229D0E366E8F
SHA-512:	2279FD5C30D3625A119D5D7830CBE197C65D757A71225C45349986FC00AC63D427794886A15093262440AB657C49F3B28664B50B623C62065CE1E72F803F0351
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...f../....."#.DYi(.u..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....Z.....0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...../....."#.D.bC.u..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.630379844328369
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QAOowuA424r1TK6tn/l2kqYOFLvEWd8CAd9QE+wnOuA424rT:+RQzrnqRQVrnpRQU1Xrn

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
MD5:	8D83AA697E86A95C1690BCCC5EDB5AFB
SHA1:	EFF99231602CBFE3B7564DEC6C44C1A9F8195796
SHA-256:	8AAF07CC19B5457D13E832AC9DBAB1F811EC3FEC4BD733900AB344CD11C3B5B7
SHA-512:	3471A8BCB7C8ACFA2B6623274225CEC0E7FA24C65D92F1576E0742C5F779A0944A6E3507C94E17597E31BBA02B7B7B1BF9057F276740243EBB0A2CA6BE728B9A
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .B.e../....."#.D.C0.u..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ./..../....."#.D...u..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...../....."#.D.&L.u..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):	420
Entropy (8bit):	5.580871085694729
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAu3FW9yC8n1TK6ts8oXXYOFLvEWdENUAuEwJXyC8n1TK6tM:xhRTZq7QKDhRTuwN7Q
MD5:	96CC134C5FB605FCB65A0CFFDD5EDCF1
SHA1:	C33FD3A0867771766DD35B469937FDD1BA0765DF
SHA-256:	4371FB8BB8D4933988F14636EE7F31AC23ADE7980E62708A879B9EB040165C13
SHA-512:	DBA58F73DDD88A06012AEECCD0A8021D2FEFBA60ECAE8260002B3C25196428B495FF7E0050D3469A67A901F88F77F446DC8C3DCC26BD26C0E2D724B1573AC3
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..g_../....."#.D.D..u..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...../....."#.D..0.u..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....T.....

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):	663
Entropy (8bit):	5.62706028457398
Encrypted:	false
SSDEEP:	12:nRrROk/VvUQMmiRrROk/VCm4fRrROk/V+FmZGc:nPJ/5UQhiPJ/N4fPJ/5Z
MD5:	55D3E8B1E325DCF2BE07D496ED79B785
SHA1:	C08239426EE85629C9A3167638590841F6C0E188
SHA-256:	1BC3AECC822695D7D4A82ECA532957D49F0683B289E30CE610BC86D3A7AB7A95
SHA-512:	7390B12CE378A2E9A21FE075EB34748BA7403FFA3A617D84626084A0D39C5EF2D0F2C3C35546DE8861AE85011D1071A94DB83DF0EDCE2D9DFB0C1F8E9B4DDEF
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...^../....."#.D.q..u..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....'B.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .L.~../....."#.D....u..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....4n.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .+;.../....."#.D>.).u..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....r.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.608337272831616
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu45mw8MLh+Adm9741TK6tXZ/lXYOFLvEWdccAWuSiAdm972:qxRcmcAdu7EZxRcnAdu7ERl
MD5:	84639D84BB6F5C38E1A18FDC271FB099
SHA1:	B92D3941582273D714FB76E67138D3A14E5DE05C
SHA-256:	31052D6BDDF0C7667C31080C940C19B097F1D0E396EF12731D9902D5AFA55902
SHA-512:	C8FAFB22D72833B0551B1F328CE390EB5C70403B5BF8E99F6FD41B00FD65A83D7B19DA1581732A5340370F79131E23934F3D45FCA1A0673B726C07F01CCDD294
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .Y.c../....."#.D..).u..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....(.f6.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..*.../....."#.DP.B.u..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.594591493808874
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuC6LM4Jn1TK6tc+MOYOFLvEWdwAPVu58E4Jn1TK6t:2R1+PL7R10eL
MD5:	E5AA00802C04962F6340B18ED38B08F5
SHA1:	7A342E2BAABCD9BA2059D97E4861AEFDC9E9DAD7
SHA-256:	0C669BB80884AADC03C3DD61E717C2C1EF3119E971DCAEB8ED77DA331C8E8B23
SHA-512:	877DFCBB1E995E511918646D311486AA5F2B5F8E35E001BF14CA5F439C28E3BBD179D7937B997671070A9F281CC6770CCD53DB76E2D9CFA9E2F1F1CAC36E1D4
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..1_../....."#.D.(..u..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... .6.!.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...../....."#.D%.0.u..A.....k....F..D..O.n;[.1m.....=..A..Eo..... .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	424
Entropy (8bit):	5.63610136989123
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQHr2zhcsBXIh1TK6tl3PXYOFLvEWdBJvYQ7w2zhcsBXIh1Tq:mxRBJQO2DB03xRBJQmw2DB0
MD5:	337FB5CBBCDE0DC113CC115F3EB7CD1C
SHA1:	E8853DF75BD593B964CE52B180E9A82A49BDE3B1
SHA-256:	1C1977A2A0E1757A5AD1418CAA3DEFC2781DBB06505097586A707562EEDB2E24
SHA-512:	B6ECCD3F7E24C83E544C8BD4B39EE04D04DFDCEDF01859C236D7F4CCAC92D3834352F5E2FC5A09CD761E255B0DD7C6AEC78D4A1DB239A59D8FECCA08258B7A
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...d../....."#.D.n+.u..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....i... .....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..*.../....."#.DB.C.u..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.. .....$.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	684
Entropy (8bit):	5.598498378511523
Encrypted:	false
SSDEEP:	12:3RrROk/ssLcRRrROk/sB0vcDRrROk/ssVbglcNWF:3PJ/r4RPJ/CDPJ/jtj0
MD5:	A3F59D7C15A5CB1A04FB05D88D364670
SHA1:	318E6C17AAFCA9A79331CD1DE4B457343979A8C4
SHA-256:	E12664590F65C08ED5F5D230DB4F28740FCE4365D570429F945B2F0861BF2D69
SHA-512:	DA32BC301D6AADBFC436ED31D8333FAF125944F7B165AE23A0E1B6679F23454017CAF159A6829731BAEAA127885512B0C5F4581416DB513AA8FEEC579F58944
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .o0^../....."#.D....u..A.....9Q].8O.z....=..:.N.{....N{.A ..Eo.....A..Eo.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .Q.~../....."#.D:..u. .A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....nGj.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select /js/plugin.js .I<../....."#.D..).u..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....>q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2064
Entropy (8bit):	5.2862161240766
Encrypted:	false
SSDEEP:	48:h1zZ4+dsp6ili4lY+lUCBlylOl2lalalKBly/lolcl8lQlXlwXl9lllvAl1rB:hX4p6iFO+/QEc8U0k/eei6dkb/CX9
MD5:	9122392DA58BA259666BEF74A2E30D56
SHA1:	04EFC60F2D81E44C18123D4A741DE315BE56E6D4
SHA-256:	835B263D88B079B7E1B8A5DBE8F1109297100DF5B71F4073D886292CD4922075
SHA-512:	F298B8C60A8FDF59927DBFDF328B089B3891709894F33F81D191AEF8E95D998C802091F03381B28D73194968BEB8EE597BBF40C1FA6051D26885F3F9884AAF52

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+...._#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0.....oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.189550583826916
Encrypted:	false
SSDEEP:	6:m/X13Qt+q2PWXp+N2nKuAl9OmbnIFUtpIX1I+ZZmwPIX15TlVkwOWXp+N2nKuAlz:YX1AovaHAahFUtpIX1fZ/PIX15E5fHAR
MD5:	0AEB5B78D0218BEE40F1E930F629E3E8
SHA1:	D7674A0C905B2CAF158217F58EC0F95113B1F6C2
SHA-256:	B2C02F6CB5506BB4C2DEB9E514203D2D95BE4AE6C1184A90BB45017A6E2CFF0F
SHA-512:	F43267BD31FBA6EE1DA0EFDCCE5930467B6D3FD1A6A7B8A5F7404C119ADA25688CE4E98CA521734C16821575AC1E70F0A66A207787C5A2B4DB440D56182D2B B
Malicious:	false
Preview:	2021/02/23-20:31:53.037 1998 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/23-20:31:53.038 1998 Recovering log #3.2021/02/23-20:31:53.039 1998 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):	1441792
Entropy (8bit):	0.008902857563227258
Encrypted:	false
SSDEEP:	48:TGEiaGEiaGEiCEhC9EhCrQEhCrQEhCrNsMhCr+sMhCDo+sMhCDo+sMhCDo:pIIKnonono
MD5:	56D90782BB1D8D635D484F6740FC699D
SHA1:	54780F7D3D4FE684057F8625FE19BFDDC237E757
SHA-256:	9B692B86695399B03842D36BCA3CBE2A917F774567CBAF14BC97CF0E182D7750
SHA-512:	8D75665C7F8C7CAA4371F06D74BDF18498B9503E7F0A12B86B2875528831CC1EEE5C37BB56C56A55057033A54C64E43773BBD53AABBD6F56C4DAF7DF8273F77
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2102240043146Z-247.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 114 x -152 x 32
Category:	dropped
Size (bytes):	69366
Entropy (8bit):	4.954106817934743
Encrypted:	false
SSDEEP:	384:e39hCMn9g7CiXUm0bh+KC3vF+y6AzpJOfu6bOQOmj1FrzME8uuG4g9gGuApiLZN6:eTCMn9mKC30y6AzpAfuLI0Afpi36
MD5:	20D09D1F88B895A0CB90B86006FA628F
SHA1:	AF43357A05CB7A02D65726430B976A5B048997ED
SHA-256:	F3A5CCC85305239393BD3649F27FB58A01A76B51A3C2EB2A00F86B73370F303F
SHA-512:	FD8B10640A2C0B833C4CFB0CF541DDC908C99B80F703F9074167E35A513114629B6D11639AC885CC420B21BC298D0B12C777AD312A969F78ECF905ECCB4D846
Malicious:	false
Preview:	BM.....6...(...r...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	32768

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Entropy (8bit):	3.3867533558070524
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQLOhFVCsL49IVXEBodRBkR2LOhAVCs749IVXEBodRBkl2LOhWt:iGedRBVedRBwedRBQedRBp
MD5:	21536609B5A1E018107E0FB291378C55
SHA1:	0D8DCEE75C89B6FF9A728EC0CE39131B4625304A
SHA-256:	C1CE14069F464DED76D41851FCFFF380E20DECC1DB33DA93B7D25A2729F2A667
SHA-512:	642569D1AE0D766C7D7EED36B9AB3CC317FB5BE77A081F33A001BF53A4AF984FA8A9D21B8BC37D78852941ADE546225C154EF9A11151A2A7BF8C408FAA8FC2 4
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.2013773017433658
Encrypted:	false
SSDEEP:	96:P7OhFVCP7949IVXEBodRBkgRLOhFVCsyLR49IVXEBodRBkQ2LOhAVCsYd49IVXE8:PHiedRBDhLGedRBpCedRBSyedRB4
MD5:	AB3E6DE6D3FC7CFD8AE52CB5D47C71DF
SHA1:	8B1139909B6E4340970B4AF38205C51B2389F83B
SHA-256:	99A888C04366E56DB243A5291FFA68F3257BF41FC7A42FE0BBA1FCEB6BB24683
SHA-512:	1C074A163923B1C4ABA3C2BB63F82747F188A2DF60239D858CB0A75FA1A8C2C1B68876C7AA6E4E5BDC9DAA18C4B0C3700ED85ECB313EC14DEC5D6225CACF5 0BC
Malicious:	false
Preview:	.....i..d..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1064	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.Na meArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleN ame:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.N ameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-Bold MT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

Static File Info

General	
File type:	PDF document, version 1.6
Entropy (8bit):	7.910095145442616
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	IMCS Covid Program.pdf
File size:	903265

General

MD5:	7442f0868b88e0b31172b1fb0ae2e6ea
SHA1:	fa961cb1acb493b0b2ddadd16b09e703a8a80af0
SHA256:	2e6363947ba418fc8cad403a195bf29dab61ee65f3d01b66edc17af92ff80336
SHA512:	16dd0e2d614da39e6186f226bf68be523a25d01c2a0122f16e6c3a44d9f81b9c9160af16a5b4a0daf67acd8d14e4b1891408338b612ffc4491e864eb8a58b38c
SSDEEP:	24576:o0WJ0oJTpDhy9yH6ODkTPOypvIMw7pD2r:ojHVpzPO8pD2r
File Content Preview:	%PDF-1.6.%.....58 0 obj.<</Linearized 1/L 903265/O 64/E 250483/N 2/T 901990/H [5676 631]>>.endobj. .xref..58 269..0000000016 00000 n..0000006307 00000 n..0000006441 00000 n..0000006512 00000 n..0000006543 00000 n..0000006628 00000 n..00000

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.6
Total Entropy:	7.910095
Total Bytes:	903265
Stream Entropy:	7.948906
Stream Bytes:	849859
Entropy outside Streams:	5.225136
Bytes outside Streams:	53406
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	326
endobj	326
stream	150
endstream	150
xref	2
trailer	2
startxref	2
/Page	2
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 20:31:29.563656092 CET	51281	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:29.582798004 CET	49199	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:29.615242004 CET	53	51281	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:29.634466887 CET	53	49199	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:30.757627010 CET	50620	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:30.806653976 CET	53	50620	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:31.687800884 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:31.739399910 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:32.490720987 CET	60152	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:32.542532921 CET	53	60152	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:33.280886889 CET	57544	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:33.331286907 CET	53	57544	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:34.111356974 CET	55984	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:34.163017035 CET	53	55984	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:35.331027031 CET	64185	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:35.381305933 CET	53	64185	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:36.993721962 CET	65110	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:37.045511961 CET	53	65110	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:37.941169024 CET	58361	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:37.990246058 CET	53	58361	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:38.810978889 CET	63492	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:38.859884024 CET	53	63492	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:40.051532030 CET	60831	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:40.100361109 CET	53	60831	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:40.837996006 CET	60100	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:40.886749029 CET	53	60100	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:41.670758009 CET	53195	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:41.719501019 CET	53	53195	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:53.427938938 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:53.465099096 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:53.486603975 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:53.523530960 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:54.425487995 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:54.472450972 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:54.484162092 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:54.529702902 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:55.473656893 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:55.518596888 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:55.534152985 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:55.577883959 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:57.468888998 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:57.518802881 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:31:57.526278019 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 20:31:57.584482908 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:01.474550962 CET	50141	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:01.521220922 CET	53023	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:01.537311077 CET	53	50141	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:01.580780029 CET	53	53023	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:02.905608892 CET	49563	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:02.957257986 CET	53	49563	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:03.702331066 CET	51352	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:03.754076958 CET	53	51352	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:03.910799026 CET	59349	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:03.960180044 CET	53	59349	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:04.530754089 CET	57084	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:04.579540968 CET	53	57084	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:05.739649057 CET	58823	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:05.788454056 CET	53	58823	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:06.934957981 CET	57568	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:06.983720064 CET	53	57568	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:10.301928997 CET	50540	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:10.365494013 CET	53	50540	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:23.741373062 CET	54366	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:23.806509018 CET	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 20:32:40.694973946 CET	53034	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:40.743796110 CET	53	53034	8.8.8.8	192.168.2.3
Feb 23, 2021 20:32:44.102663040 CET	57762	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:32:44.164606094 CET	53	57762	8.8.8.8	192.168.2.3
Feb 23, 2021 20:33:15.602477074 CET	55435	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:33:15.654114962 CET	53	55435	8.8.8.8	192.168.2.3
Feb 23, 2021 20:33:18.233072996 CET	50713	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:33:18.303383112 CET	53	50713	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:26.266496897 CET	56132	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:26.358736038 CET	53	56132	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:26.985027075 CET	58987	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:27.051615000 CET	53	58987	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:27.706301928 CET	56579	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:27.808837891 CET	53	56579	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:28.527024031 CET	60633	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:28.587480068 CET	53	60633	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:30.447530985 CET	61292	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:30.504889011 CET	53	61292	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:31.084712982 CET	63619	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:31.141882896 CET	53	63619	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:31.729418039 CET	64938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:31.791547060 CET	53	64938	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:32.674205065 CET	61946	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:32.736167908 CET	53	61946	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:33.529113054 CET	64910	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:33.588371992 CET	53	64910	8.8.8.8	192.168.2.3
Feb 23, 2021 20:34:34.017271996 CET	52123	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:34:34.109728098 CET	53	52123	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:23.150626898 CET	56130	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:23.203739882 CET	53	56130	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:23.435056925 CET	56338	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:23.483917952 CET	53	56338	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:24.079471111 CET	59420	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:24.152151108 CET	53	59420	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:27.037327051 CET	58784	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:27.111720085 CET	53	58784	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:30.481322050 CET	63978	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:30.559454918 CET	53	63978	8.8.8.8	192.168.2.3
Feb 23, 2021 20:36:30.923650026 CET	62938	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:36:30.975778103 CET	53	62938	8.8.8.8	192.168.2.3
Feb 23, 2021 20:38:47.383773088 CET	55708	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:38:47.449270010 CET	53	55708	8.8.8.8	192.168.2.3
Feb 23, 2021 20:38:47.955331087 CET	56803	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:38:48.007312059 CET	53	56803	8.8.8.8	192.168.2.3
Feb 23, 2021 20:39:20.645489931 CET	57145	53	192.168.2.3	8.8.8.8
Feb 23, 2021 20:39:20.722194910 CET	53	57145	8.8.8.8	192.168.2.3

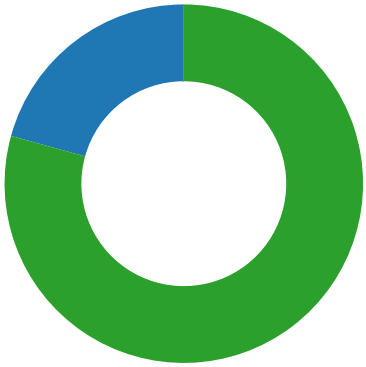
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 20:36:23.203739882 CET	8.8.8.8	192.168.2.3	0xae99	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 20:38:47.449270010 CET	8.8.8.8	192.168.2.3	0x7220	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 1560 Parent PID: 5636

General

Start time:	20:31:36
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\IMCS Covid Program.pdf'
Imagebase:	0x940000
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	9765C3	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	99AE05	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	98EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210224043146Z-247.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	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1064	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock1560.1.2139092665.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	9C2657	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A083C8	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	A083C8	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	A083C8	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	A083C8	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	A083C8	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	A083C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1p8undk_1bj6rhq_tk.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	98EA85	NtCreateFile

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R12se1r8_1bj6rhr_tk.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	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R10w8qyp_1bj6rhs_tk.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	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R101je53_1bj6rht_tk.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	98EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ri42ejm_1bj6rhu_tk.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	98EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1064	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	9CD405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	98CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	98D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	98D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	98D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	94EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	94EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	94EA55	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	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/IMCS Covid Program.pdf	success or wait	1	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	IMCS Covid Program.pdf	success or wait	1	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	99DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 49 4D 43 53 20 43 6F 76 69 64 20 50 72 6F 67 72 61 6D 2E 70 64 66 00	success or wait	1	99DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 33 32 30 33 31 34 35 2D 30 38 27 30 30 27 00	success or wait	1	99DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	903265	success or wait	1	99DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	2	success or wait	1	99DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	99DF47	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	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	99DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	99DF69	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	99DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	99DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 1064 Parent PID: 1560

General

Start time:	20:31:37
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\IMCS Covid Program.pdf'
Imagebase:	0x940000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Copyright null 2021

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 5112 Parent PID: 1560

General

Start time:	20:31:44
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0xe30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	F259E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	9	F383E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	75	F38447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	216	F259E2	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	7	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	23	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	16	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2170	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	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	6	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	3	F259E2	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	3	F259E2	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	3	F259E2	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	3	F259E2	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	18	F259E2	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	3	F259E2	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	18	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	3	F259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	41	F259E2	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	3	F259E2	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	45	F259E2	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	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	F259E2	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	167	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	F259E2	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	8	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	F259E2	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	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	3	F259E2	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	F259E2	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	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	15	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	16	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	F259E2	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	323	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	42	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	15	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	201	F259E2	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	3	F259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	149	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	32	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	180	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	215	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	10	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	F259E2	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	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	2	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	F259E2	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	F259E2	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	F259E2	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	F259E2	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	F259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	F259E2	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	F259E2	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	F259E2	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	F259E2	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	F259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	F259E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	F383E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6240 Parent PID: 5112

General

Start time:	20:31:47
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=3499109752215329224 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xe30000
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: 6264 Parent PID: 5112

General

Start time:	20:31:48
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,17899945495974257541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4017212095282925109 --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=4017212095282925109 --renderer-client-id=2 --mojo-platform-channel-handle=1756 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe30000
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: 6344 Parent PID: 5112

General

Start time:	20:31:50
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,178999454959742 57541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10025927610161177688 --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=10025927610161177688 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe30000
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: 6504 Parent PID: 5112

General

Start time:	20:31:54
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,178999454959742 57541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4937386989897175714 --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=4937386989897175714 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe30000
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: 6668 Parent PID: 5112

General

Start time:	20:31:56
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1720,178999454959742 57541,7031488614954161980,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=865829887153264502 --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=865829887153264502 --renderer-client-id=6 --mojo-platform-channel-handle=2124 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xe30000
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