ID: 324343
Sample Name: Invitation - Prime Minister of Israel.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 10:02:50
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

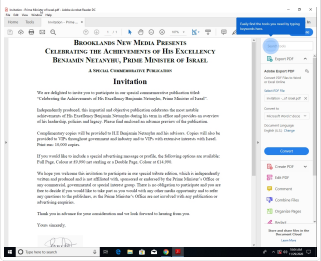
Analysis Report Invitation - Prime Minister of Israel.pdf

Overview

General Information

Sample Name:	Invitation - Prime Minister of Israel.pdf
Analysis ID:	324343
MD5:	e3f4a57d14090a2.
SHA1:	0163a63054fd5da.
SHA256:	63f3f7706c4d6ca..

Most interesting Screenshot:



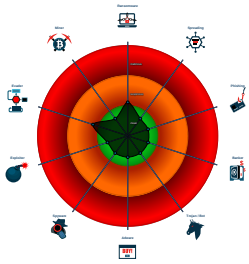
Detection

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

Signatures

- Contains functionality to access load…
- IP address seen in connection with o…
- PDF has an OpenAction (likely to la…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 3016 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5620 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5072 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=1692,5657141681204985935,18091407090887986711,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=18388359474767092242 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6368 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=1692,5657141681204985935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11592911304768251189 --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=11592911304768251189 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6452 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=1692,5657141681204985935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10775127221883232441 --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=10775127221883232441 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6496 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=1692,5657141681204985935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8896761926437382365 --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=8896761926437382365 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6704 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=1692,5657141681204985935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2426508304687755912 --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=2426508304687755912 --renderer-client-id=6 --mojo-platform-channel-handle=2132 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

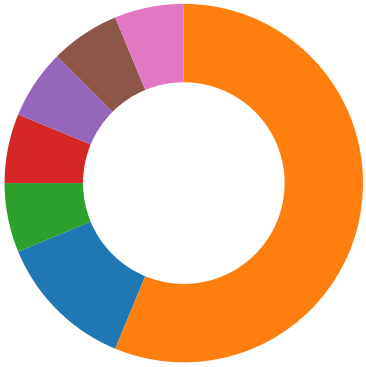
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

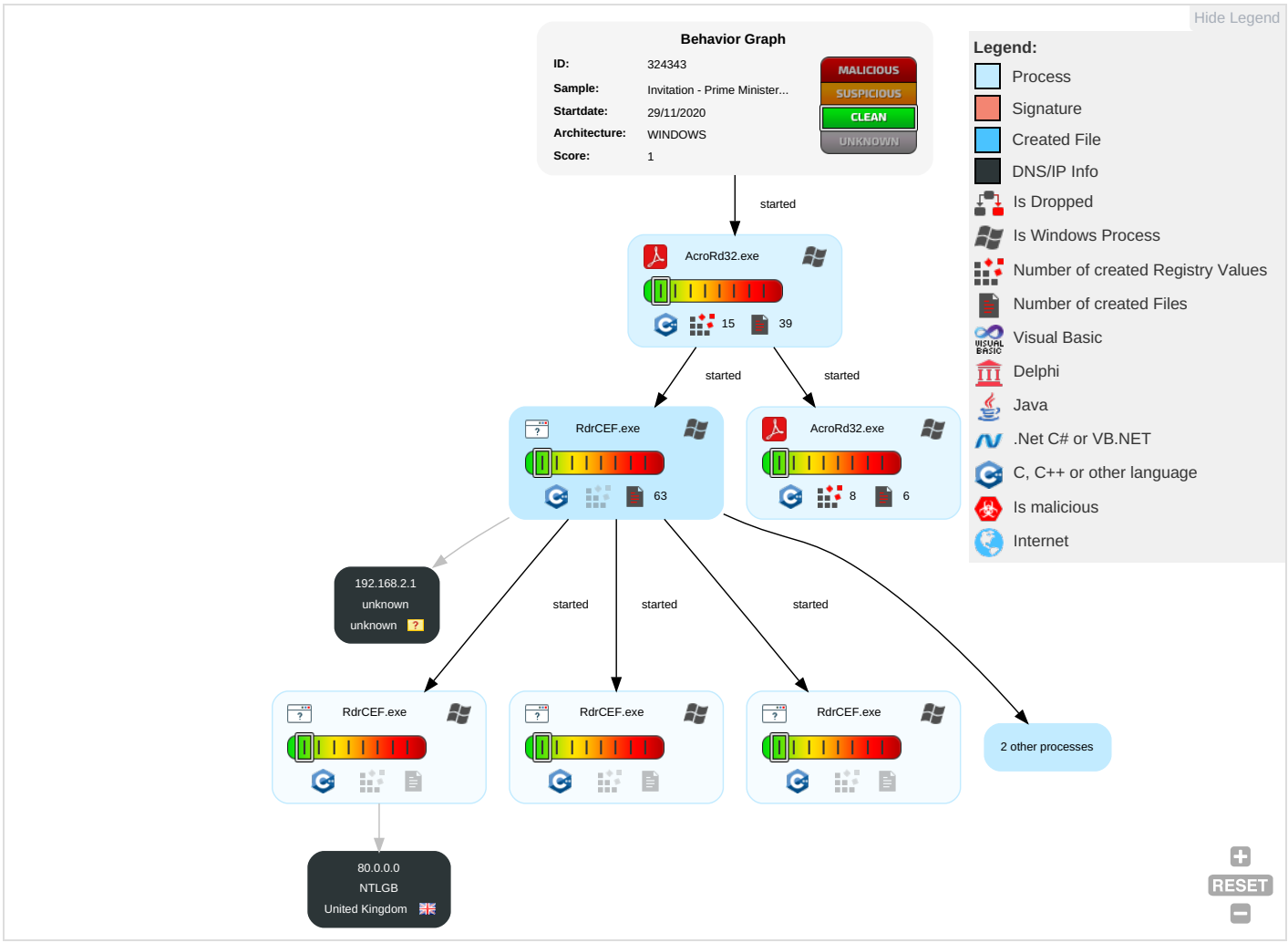
Click to jump to signature section

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

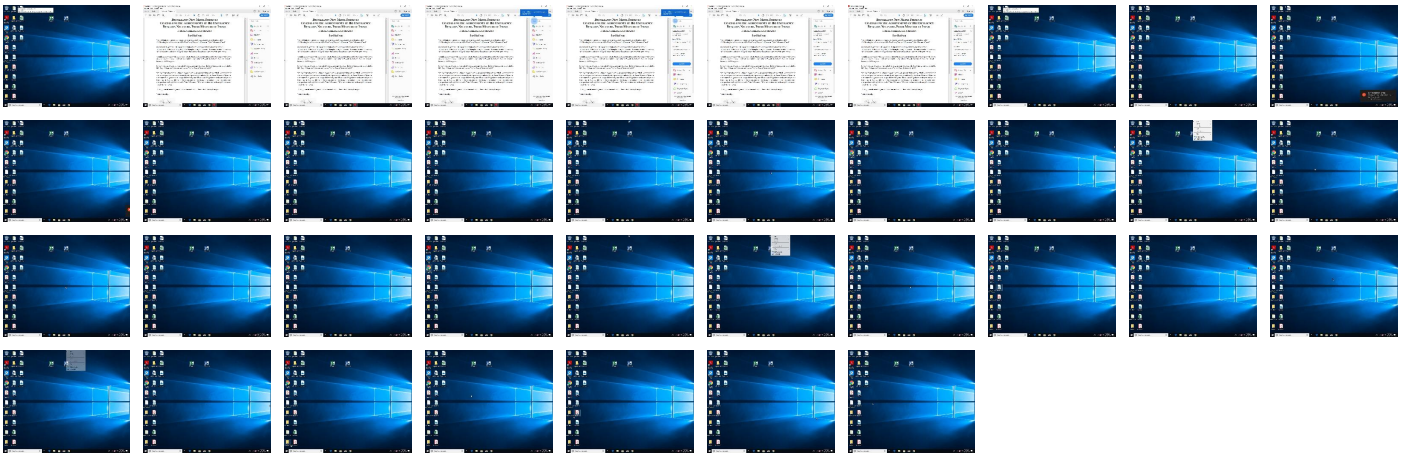
Behavior Graph

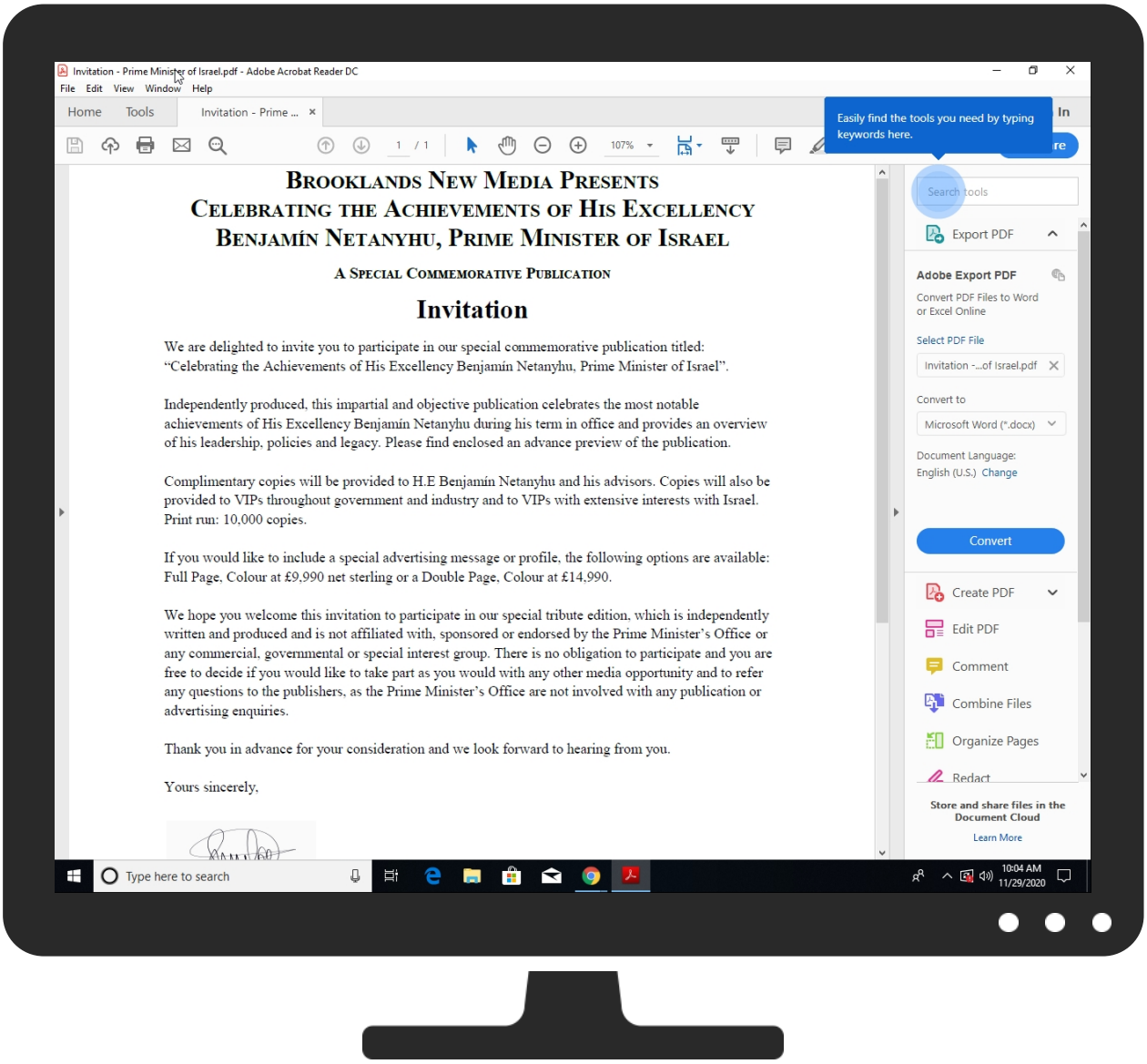


Screenshots

Thumbnails

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





BROOKLANDS NEW MEDIA PRESENTS
CELEBRATING THE ACHIEVEMENTS OF HIS EXCELLENCY
BENJAMÍN NETANYHU, PRIME MINISTER OF ISRAEL

A SPECIAL COMMEMORATIVE PUBLICATION

Invitation

We are delighted to invite you to participate in our special commemorative publication titled: "Celebrating the Achievements of His Excellency Benjamín Netanyhu, Prime Minister of Israel".

Independently produced, this impartial and objective publication celebrates the most notable achievements of His Excellency Benjamín Netanyhu during his term in office and provides an overview of his leadership, policies and legacy. Please find enclosed an advance preview of the publication.

Complimentary copies will be provided to H.E Benjamín Netanyhu and his advisors. Copies will also be provided to VIPs throughout government and industry and to VIPs with extensive interests with Israel. Print run: 10,000 copies.

If you would like to include a special advertising message or profile, the following options are available: Full Page, Colour at £9,990 net sterling or a Double Page, Colour at £14,990.

We hope you welcome this invitation to participate in our special tribute edition, which is independently written and produced and is not affiliated with, sponsored or endorsed by the Prime Minister's Office or any commercial, governmental or special interest group. There is no obligation to participate and you are free to decide if you would like to take part as you would with any other media opportunity and to refer any questions to the publishers, as the Prime Minister's Office are not involved with any publication or advertising enquiries.

Thank you in advance for your consideration and we look forward to hearing from you.

Yours sincerely,

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Invitation - Prime Minister of Israel.pdf	0%	Virustotal		Browse
Invitation - Prime Minister of Israel.pdf	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://www.brooklandsnewmedia.com	0%	Virustotal		Browse
http://www.brooklandsnewmedia.com	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/U	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/M	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/_1~u	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

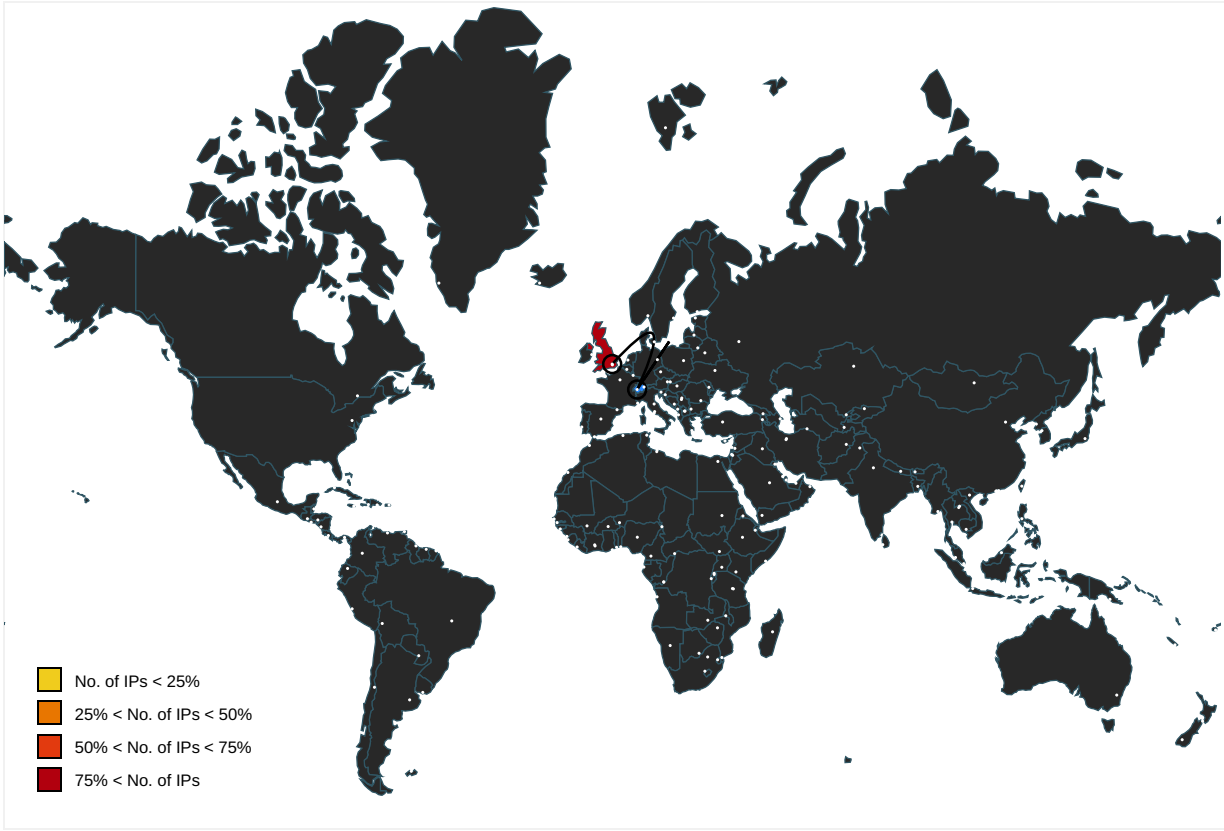
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://cipa.jp/exif/1.0/.0/	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/k	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/Dr	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/Pr	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false		high
http://www.brooklandsnewmedia.com	AcroRd32.exe, 00000001.00000003.366318568.000000000BBA3000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/U	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/M	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.382102912.000000000BA74000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comRL	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#$$r	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.381233649.000000000B7B9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	AcroRd32.exe, 00000001.00000002.382102912.000000000BA74000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.372265312.0000000009830000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/type#U	AcroRd32.exe, 00000001.00000002.382153497.000000000BACE000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/_1~u	AcroRd32.exe, 00000001.00000002.381813017.000000000B9AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.368797608.0000000008050000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324343
Start date:	29.11.2020
Start time:	10:02:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invitation - Prime Minister of Israel.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

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): 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): 52.147.198.201, 104.43.193.48, 2.20.142.203, 2.20.143.130, 92.122.146.26, 51.104.139.180, 92.122.144.200, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.190.129.2, 20.190.129.17, 20.190.129.133, 40.126.1.145, 40.126.1.128, 40.126.1.142, 20.190.129.130, 20.190.129.128, 93.184.220.29, 51.104.136.2, 40.127.240.158 • 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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, login.live.com, a122.dscd.akamai.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, acroipm2.adobe.com.edgesuite.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, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, blobcollector.events.data.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
10:03:46	API Interceptor	10x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	CHoyU.pdf	Get hash	malicious	Browse	
	ggBNN.pdf	Get hash	malicious	Browse	
	KKjNA.pdf	Get hash	malicious	Browse	
	IFPoj.pdf	Get hash	malicious	Browse	
	MXNYB.pdf	Get hash	malicious	Browse	
	npmiu.pdf	Get hash	malicious	Browse	
	sCpYf.pdf	Get hash	malicious	Browse	
	sIdiW.pdf	Get hash	malicious	Browse	
	UsBzT.pdf	Get hash	malicious	Browse	
	VFznx.pdf	Get hash	malicious	Browse	
	mGhdt.pdf	Get hash	malicious	Browse	
	b6egewgab.pdf	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	http://post.spmailtechnolo.com/f/a/h2coVlte-PnQgGolAw1FlQ~~/AAH5oAA~/RgRhk9ssP0QiaHR0cHM6Ly93d3cud2F6cC5pby9kb3dubG9hZC82MTI3L1cDc3BjQgoAJyxWsV-4NRnDUhVzY290dC50YXlsb3JAdG1hZy5jb21YBAAAAG4~	Get hash	malicious	Browse	
	5wnaEGcbc7.exe	Get hash	malicious	Browse	
	Kpw6TB725f.exe	Get hash	malicious	Browse	
	LWwoiTLRjW.exe	Get hash	malicious	Browse	
	Gt2YstXx3K.exe	Get hash	malicious	Browse	
	ForQuotation_RMS22100.exe	Get hash	malicious	Browse	
	http://www.dropbox.com/l/AAA5d-90vlipt6OAJjh2DZ1FLO-gN1n6Y0k	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	CHoyU.pdf	Get hash	malicious	Browse	• 80.0.0.0
	ggBNN.pdf	Get hash	malicious	Browse	• 80.0.0.0
	KKjNA.pdf	Get hash	malicious	Browse	• 80.0.0.0
	IFPoj.pdf	Get hash	malicious	Browse	• 80.0.0.0
	MXNYB.pdf	Get hash	malicious	Browse	• 80.0.0.0
	npmiu.pdf	Get hash	malicious	Browse	• 80.0.0.0
	sCpYf.pdf	Get hash	malicious	Browse	• 80.0.0.0
	sIdiW.pdf	Get hash	malicious	Browse	• 80.0.0.0
	UsBzT.pdf	Get hash	malicious	Browse	• 80.0.0.0
	VFznx.pdf	Get hash	malicious	Browse	• 80.0.0.0
	mGhdt.pdf	Get hash	malicious	Browse	• 80.0.0.0
	b6egewgab.pdf	Get hash	malicious	Browse	• 80.0.0.0
	purchase order.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://post.spmailtechnolo.com/f/a/h2coVlte-PnQgGolAw1FlQ~~/AAH5oAA~/RgRhk9ssP0QiaHR0cHM6Ly93d3cud2F6cC5pby9kb3dubG9hZC82MTI3L1cDc3BjQgoAJyxWsV-4NRnDUhVzY290dC50YXlsb3JAdG1hZy5jb21YBAAAAG4~	Get hash	malicious	Browse	• 80.0.0.0
	5wnaEGcbc7.exe	Get hash	malicious	Browse	• 80.0.0.0
	Kpw6TB725f.exe	Get hash	malicious	Browse	• 80.0.0.0
	EnklyRDCVr.exe	Get hash	malicious	Browse	• 62.31.150.202
	LWwoiTLRjW.exe	Get hash	malicious	Browse	• 80.0.0.0
	Gt2YstXx3K.exe	Get hash	malicious	Browse	• 80.0.0.0
	ForQuotation_RMS22100.exe	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):	5.669726917857802
Encrypted:	false
SSDEEP:	12:vDRM9D9OZiEAtDRM989rZiETQDRM9q1/oeZiE1:76rEwf90ETmzobE1
MD5:	0C1B49630A2C5AD47967DFC195597C03
SHA1:	359615C2CC479B02E42ABB4E338F0AE82F1281FF
SHA-256:	998AE633EDDDCF369E3E9D72631059F705172D4DBA1B4BA6B90D0083929F77C3
SHA-512:	04F30E86EE495AC455BCBC91D5734E518C0CDD59B1BDF25C73FAE185F17791F44675D4BE001D37703CF281C8AB6B5AF054D7DE23D7E7348A8D194C0CEB65F9 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...K.../....."#.D.K....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... (.........0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..|n.../....."#.Dr6`....A....d.{v.^.G...d.W.:...P..k%..A..Eo..... A..Eo.....C.....0\r..m.....M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ._...../....."#.D_.....A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....A..Eo.....s.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	5.616218049714297
Encrypted:	false
SSDEEP:	12:V9zXi9PQ0H9zOYUw9PQftH9zT3/549PQy9zT59AC9PQ:XzXi9PQ0dzOm9PQf/zr549PQuzzr9PQ
MD5:	3B71D80DC65E23D1C9D9E9B969235917
SHA1:	9151DD802C14B619830107BCCFBE750D09DD2F69
SHA-256:	DB1BC0CD4E420E9E86FD839E1E5391BD68ACB0D850305FE319E449A41A5D0B4B
SHA-512:	67801E977F890027794E8DC816329B035513049D3E7549273516C08B5DCB49B071FC142A21520DCC4B8BC8CBE1A560485D349B358237E740C71F06767F262CFC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...../....."#.D.6....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....=.Y.....0\r..m.....,....._keyht tps://rna-resource.acrobat.com/init.js .9.7.../....."#.D.1{....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....A.....0\r..m.....,....._keyhttps://rna-resource.acrobat.co m/init.js ..._.../....."#.D.."....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....].....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .|.q.../....."#.D%!n....A.1.x .'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.629647744389177
Encrypted:	false
SSDEEP:	24:tB4v4eeSB9dB4v4b6SBdB4v45kSBrB4v44rSB:nMwSB93MJSB3MNSB1MnSB
MD5:	EA93D80BF3FA4E55C77A1E700099AD02
SHA1:	621E2570B3E50812792E1CECBDAD5169207890F3
SHA-256:	195624A49B0CB52310B5CC0589E9BD225716C3EAD836E345253D5738700EF815
SHA-512:	1160535F521DE20D5AF41EA949571F3448C920B04161A080884B8D598A68CFEC1F782BB3778B27962403250F0966367AE9D4DAFD48F1778DA4306EDCF7B6E0C2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .."...../...."#.D_.)....A..hvDO.N.t@....n.*..... ....A..Eo.....A..Eo.....iI.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..5J.../....."#.D.....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 ...m.../....."#.D.*_....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....R.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..v..../....."#.D.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....2.....

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):	5.598187952426353
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsu1/P8iWulHyA1TK6tl:IbRkiDxPtWuss
MD5:	F8D88AA39B138DBB83E4802692327B3C
SHA1:	5BFC8B5971A72083495E631416B4871FF590F361
SHA-256:	9B050116B057D6F53864F9C8787E964DFCD80388164F0E994B166CA142EF40B6
SHA-512:	7DB1BB51AA7C0E129D2D70E6B4D20521BD9121D70E4BC8910B6ACC2160B0E2EA68C88448762F1577B4C2EC9B93DEB08AF93D571C30CB0F7C83EC643D0930E0F3
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 ..zt.../....."#.D.x....A..8 P..a...R..Y....7.@..2Dm{. .A..Eo.....A..Eo.....tn.....

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):	5.618106732823203
Encrypted:	false
SSDEEP:	12:pyixRuqqOV41TERl7yixRuu8liV41TEt:NCo4xEDjT8/4xEt
MD5:	756CE3F1DAD9730AC1B5C3AF3094AF31
SHA1:	5827A88AB799094BD0804D4D07A5A65B85462BE7
SHA-256:	8AB2B1D669C515A8987A88503816EDD4016486ED5500FA60E29E2AFF0A120967
SHA-512:	1DEF81E9C36C66548CAAE4594FCE66C1D43ACB1FD721A413D8C5A560FAEF18053FFE255D6FDF046A0EF9AEF2C1B80B78568D1EC2A596386131AFE574A69189E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...K.../....."#.D{3....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.. ....S.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .@..../....."#.D.....Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....MG.>.....

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):	648
Entropy (8bit):	5.642640362554876
Encrypted:	false
SSDEEP:	12:0RhkzVCLZCVWRhkN//x4LZCXRhkTMLZC:0fIVCLcIfG//x4LcXfoMLc
MD5:	15B69862F7B6C702C73B76B0BB519615
SHA1:	992555760E4446BB2684261E577F1D807A3C1072
SHA-256:	60BEEE09D1077187A4588EC45EA6D321E54B3037BA1E339242E7DD0F99655BD1
SHA-512:	32E4A7328ADFC8C1A6629F4EAF5ACCF4CA31BAE71C80CAED16B8A3863382C3443D14EF216E8529137D9D3FFF7AC863DB700ABD598B962E2452B2DA4AC23FE8B
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...../....."#.D.....A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo..... r.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .a.E.../....."#.DH3.....A.].>....uUf..N...k.....c..l.A..Eo..... .....A..Eo.....;.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..5..../....."#.D.....A.].>....uUf..N...k.....c..l.A. .Eo.....A..Eo.....|z.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.558210230470493
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQz9r6g1TK6teJYOFLvEWdGQRQOdQ0l/JX76g1TK6ts:2RHRQCO9r1ARHRQCLl/J1K
MD5:	7ADC56B2F0A9E29DD2D2E73111B1D6A3
SHA1:	6B93FC87F8172B2CD346708FF20884F973C5870D
SHA-256:	777D450DE71412B118276FEB5CBD0E372D0DFA0A4656AD58CAACC37E47D57D93
SHA-512:	1333D01779AEB9CA7E1A866980A4AFD40B9B418AE1EF7AD233946DBCAA4AEA5F727B9B1E25B58F496EFA9AD5C1679737719974797E1A78A2554702E3A80BA47E
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..K.../....."#.D$b....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....P..Z.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...../....."#.DD1.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....m.....

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):	5.638552931988914
Encrypted:	false
SSDEEP:	12:Z5M0MuR/Ef5MViMuR/Ed5MmT1/dhBMuR/EL5ME9BMuR/E0:ZStuR/EfSV7uR/EdSmxiuR/ELSCGuR/b
MD5:	6FF7B507459EA0A6CA4D2418F4617E91
SHA1:	7DE540547BDB40A42A3D2724A50F0A4A375CBF4F
SHA-256:	76C98729DFD54A25E46E8E5EF26607D07D24459C8A1358A01731D9672F09E37D
SHA-512:	CD92F83345EAB53B94D920E395F580AB00370B53F13EED595F0E805D651B11D89CF05FC328AA06E033EBB6C2A6DD1EB6B98D41F21CFFE6931768DB2EBF2D712
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .H...../....."#.D.77....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 ...7.../....."#.D.I{....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 ..._.../....."#.DW."....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....pb.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .[.q.../....."#.D..n....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):	5.609563155187699
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAutV+l/CHiSm0bbsIDMGH41TK6t6/:XfRM9+l/CHiRKsIZEM
MD5:	AC2727B7477B3C8E79B0E3DB968B9E13
SHA1:	0F10DEBF49545A408485A822518FB04EF654F2EC
SHA-256:	CBC6ED08194E5E134BDC49FF8640B8992281FB9D0802B96D996ED8E9B6A51E01
SHA-512:	15C12E10B5A268B81D6B2EF72B00E2C14524997DAF17756D1746874719B94E00DE294C94372D702E2271A954A92C0BE6E2B30F8DA322166E93ED8AA07015E72A
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ."iS.../....."#.D.....A..`....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....d.F].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.547425485817038
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtulKXVyuby0zBUKSAA1TK6t9U4fPYOFLvEWdtuw/l/wbby0zBUKA:pRKKXYubeLRbt/ebe
MD5:	FA6FF8346C66C11DBEF1C71FB5D37799
SHA1:	6EBD54951AD8947F6069888BFCA59358863C74CA
SHA-256:	101005B6740519F52AF11293F2907C5905D78F49FE778390A9558E22BF7F3A1B
SHA-512:	B58CDB9F5843DCB93731C67C81FDEC75438C312BEE768AC463AF3CC8F3ACA4E56F139C3103608424FB8E310AA77DF68715FBEE309F2AFF5D1504BE0AC639D0E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..!L.../....."#.D1.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....pr.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...../....."#.DG.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....X.>.....

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):	5.573550002060252
Encrypted:	false
SSDEEP:	12:KkXxKMSCvUtUl2ikXxKMSCvo9wotUlt4kXxKMSCv+l/xmtUlrFwkXxKMSCvfTtUl:KkXxiCMWRkXxiCA9TWt4kXxiCGtxmWr4
MD5:	9D18B0673DA447D4D6C423692F2C3B05
SHA1:	B08D1D97265ACD6CDFCDFFF5E7628D9FF5292F9B
SHA-256:	EFB3213AD4FB5D5B8D975D6F8B58954FE51D4ED39054C8D50C6F1B372586420B
SHA-512:	16E4D1FE86985CF098B9024D5D793DE32C947869E9906A5CA47FAF998D03C0716DC96E174452A2F620F389622A658728E8CA389F38F263F2808FC49EB092A2F0
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...../....."#.D0/7....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 .5.7.../....."#.DpB{....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....2.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..._../....."#.D.h"....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....W%T.....0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .3.q.../....."#.Dv8n....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....5L.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	748
Entropy (8bit):	5.615662144004926
Encrypted:	false
SSDEEP:	12:5h6OLF8uZqkRzh6OLp8lSUkEh6OLpE2qkAjh6OLf8wCXqk:5h6G8uBRzh6blSBEh6z2/Ajh6K8V/
MD5:	EE80B43EA5C15EFB9F00211A2DD8A167
SHA1:	3426E5ACD6EE2993D3C38090477051D78764051E
SHA-256:	B71B394D12E25E4C952204FD0661CC49CCF2D43B0D631D6857D358EF305FF5E5
SHA-512:	5C8449C0E35887DD6CCF6F8FEB5C1C28C13D527400904ACA8E9EFA6851904AD582117AF516884B676ADBCAC28DEAD63FD10EDC8F8514A7EBE77AE0CDE901882
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....g.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .&.B.../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...j.../....."#.D..N....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....j.i.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .GW}.../....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....@xS.....

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):	5.626721122242959
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFhtlwSeKaTLnWRVFAFjVFAFUf2wSeKaTLnLRVFAFjVFAF3/n4wSeKi:UB4v4htlwzXLnWB4v4Uf2wzXLnLB4v4l
MD5:	D02FC59AD0128D93355EFEACF5CED347
SHA1:	B1B828340A11E34729ACBE1CD6DDA1A3CB66388A
SHA-256:	9C56CAC646AEC7195FFF4863185467E507E597A689A5508F06B59E143F0CEA34
SHA-512:	58CFB738249781331115F752533666FF0FE89DFA81D8879C0E8789A7789C9CE656E2043DD3DC08A56621DBA72283DC0196464C9E70E6B08FB1286FB61999F8E9
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...K.../....."#.D."....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .B~n.../....."#.D.8d....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....A].....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..^..../....."#.D.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....q.....

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):	5.542418654825749

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQWlK//55GFCaa+41TK6t:NRMHdv8//55Gda+E
MD5:	13BB9C686FBF6DDCD2BF5A924CA1A35C
SHA1:	45169515FC48891473DD04F80D9768484F454100
SHA-256:	45F315488D85630E0B658EBAB6EE2F2B9D573CDB5C600AD39421498893EC1A58
SHA-512:	3C01F2964209D7D1A32511C743190BF7E8C6B5A0B8DBA77D64F0470B0EFCF1A69E1BADC22C9C19999B62AA68688E0D725064D87D02FAC9055593FCE1646BE3F C
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .\.S.../....."#.D.$....A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo .....5..D.....

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):	5.502789009570033
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuqXdy11TK6tss2VYOFLvEWdvBIEGdeXuwm1//O11TK6t:BsR2Ese5NgdsR2Ese5m9c
MD5:	F0E2A38B120EA7831095B306E70598D1
SHA1:	A87B73E22BD8F9D180EE1B048E559055225E3F2B
SHA-256:	57766CA512D592E90C6EFB32D92F611BF0351B89DF3E9A86BEC7F5A5E9EE131C
SHA-512:	251D57B0F19DC4636FB1C40BC0395AF9E69D4C3D15FAA50AD50905F0866086D07EDF18F6AF01B82081EE3328A9F6434EC9943AF24E9917288D298A2417DAAEF5
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..;J.../....."#.D;.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo. .....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...../....."#.D:....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A ..Eo.....W.oo.....

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):	606
Entropy (8bit):	5.697909419876918
Encrypted:	false
SSDEEP:	12:RbR16tRJka/bR16u/dSJkkbR16kATJkO/:RbIRma/bf/dSmkbJkm+
MD5:	AEF288497B35F92D591D2C1F99FA31A2
SHA1:	40F98CE27CAB3D8C9D502E1F2389F18CFC336A6A
SHA-256:	EC3C0045E9A327ECE478D6AED9A14EDB04696B40D1B4D58F299AE5692A91CBAE
SHA-512:	F1E1438BEB8BD91D4859324D581A8FCC3B4F129A04B55F80FE06596D51DCBD2DD874E16ECB205DC0F6897B0F5BFF17C8533C90558386CE87543691079C2E014
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...../....."#.D.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... 0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...E.../....."#.D.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... 0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..1.../....."#.D.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....E.%.....

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):	5.594210296472309
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuGQejQdFt1TK6t8Es2gEYOFLvEWdGQRQVuB1/MMGejQdFg:B2geRHRQXH0aT2geRHRQM9Ms0W
MD5:	4A18FE742A1AD591C0B5290E7099F740
SHA1:	BC31FE98D0182D4A0475442C2DB28E7C16EFA9AF
SHA-256:	396C75876B96F63ACF6F03BB740BB6E4247F96B3CB850DDFFB6D53B29868B3A1
SHA-512:	D6AA0A7DB4CC379F3842C6226A2FA94649A261D005E9ED3BE62488E429A25D9A642ED243F8ED8A46DDF154A033E12B364123C033F1AF19BDB40C4CE54E864C 9
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..9J.../....."#.D/.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A.. Eo.....fx.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .}...../....."#.D.....A@..{o]...9o|..qY....T....{..u.b..A..Eo... .....A..Eo.....L.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	824
Entropy (8bit):	5.661606297468752
Encrypted:	false
SSDEEP:	12:WyeRluq3t1wZ2XEyeRlj6t1wmyeRli7Rt1wXEyeRle4pt1w:WJWq3fw00Jr6fwmJa7RfwXEJrpfw
MD5:	DF2A4578FE71D36C8683EC3C9A93F938
SHA1:	0BAC1685059631DDFE9A0B11FA127360A8443C6E
SHA-256:	07A41BE7375020CBAFD5B9F3D7E638C9758F4EA039522D3CED5043DA3149F794
SHA-512:	3B21FD8D0CF61A13494D606BD436155EB0167A03690E9E6F8C0A0F0CFFFED38984848719571909AEC1A9F7FAFFA3989570AF59F53297119D831235882E3DBE7
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...../....."#.DOw....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... .E.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...D.../....."#.D,.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo. .....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .T.l../....."#.D].U....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A. .Eo.....c.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...~.../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .A..Eo.....G,.....

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):	654
Entropy (8bit):	5.601966420766821
Encrypted:	false
SSDEEP:	12:wRhNtAkwK+EHRhH1/5dywK+EhyQRh5mBUwK+E:wfNtKDEHfH1/5dBDEhPf5m1DE
MD5:	25ED6A09D38DAF855AC71F483DDAF291
SHA1:	C5911B37D9EE4AFA03CBD13F98CA4525E60AD838
SHA-256:	EE01FE0B310374F8F1A0C0863A830516F7EFF7E810681B4F792A59B2F12196BF
SHA-512:	F6D7805F0CC6EDC5389B02448CEC8517187A3E553DCDFEEDB70DD46851648D0348E4463564477138B34C9A1DFE92606C50EEE62A75C966181293464FD19998C
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...../....."#.D.....A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....f.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .e.E.../....."#.DC.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....RW.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...../....."#.D.....A. .....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....n.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	920
Entropy (8bit):	5.574449133744067
Encrypted:	false
SSDEEP:	12:/RrROk/RhYfLEuRrROk/z1mpfLEDRrROk/J+efLEYwRrROk/jrmfLE:/PJ/RK4uPJ/zYp4DPJ/ce45PJ/jK4
MD5:	385C52EF41A91173B5044B6D2709B0A7
SHA1:	297A3FEA3DF67BDB0CF10F66711412EC93B9F01A
SHA-256:	368DDA4341D4CF063B3F063575175F25A7FB6B0EF03B50D8F4E42397F01C0295
SHA-512:	0ABCDC69D4C22A2720099FE9BE5D5314DF1FC00EA14A635FA3EA9969F0E927202941BCA0B70C7A0F58D82F2BA03FEE0B636DF58D51CA3E52F345A416B350054 3
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..t..../....."#.D.|.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....0.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...D.../....."#.D.....A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....Hj~.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js . ..l.../....."#.D.{U....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....2..i.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-fi les-select/js/selector.js ..l~.../....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....~..?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	744
Entropy (8bit):	5.637082157547556
Encrypted:	false
SSDEEP:	12:xqTO24NCPLnVBqTXm9P4NCPLnGTqTJ9v64NCPLnuAjqTdtV74NCPLn:AeMn+gKMnhzvZMntmbEMn
MD5:	4FAD62328ADBB12C10F9E5EBA5A9EEB9
SHA1:	57AB8843415800F405873F0A6F10AE25CCC11C4D

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
SHA-256:	B6F195333C284F96A40CA612C9102603E9B6CC4A4F04FECB032648C233FA0137
SHA-512:	29E041131E7E6866C4D12A823C79C12A63220C684A52F382FFCBF136F959CFAF2E0CD55B9C8BDBAB3CA90AE4BC9911411A3444908D3956A61B9E4D83E92C7B6
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .@`..../....."#.D<M.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....I.5.....0\r..m.....:...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .).B.../....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .z.j.../....."#.D..N....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .+N}.../....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....v.....

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):	5.6403465864757125
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuIkBwWsEJ41TK6t452YOFLvEWdMAuKfXVnnZsEJ41TK6tW52YOM:zRMykBwWsDHRM6XVnZsDpRMjmsD
MD5:	F80532EC90BFEF7E91AE1F7DA55760CE
SHA1:	32C757167F97D2B9E3CDD84FDF917B83CB1D1312
SHA-256:	64542AE03485C682BA16AAFE3C1CEF9FD83AB5C407A65DBCD964B8F862B3DCBA
SHA-512:	3DEA58CFE9B10E2B8C4BF3F9CF74176D2FEA5E77B3FD467DE0DF6559DE1DF395AF424B611E9D8221D830ED697518353AC14647CA188DB2E06DBE7FE550A63E4F
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .X.J.../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....(~.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...m.../....."#.Dr.^....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....gf.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...../....."#.DY.....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):	5.596446723881849
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuG/1Kl2Fong1TK6tkYilPYOFLvEWd8CAdAu+93J+Fong1S:6lJRx9HoMqlJR59WoMclqlJR994IoM
MD5:	6F859FC583240F151EC47556C1B09D21
SHA1:	83B18F9BB868BA644ABBB29B8F559C0931F8D465
SHA-256:	9BC1CE8C213DC1DF3D5170DAC4040150ECA7D23BB3CA6745C3145D7F5258A0F3
SHA-512:	54E634B881ABC9F81D1F748A03AE1D57F67215472CF0905DBE17F627A131CFDF9656E016ECD2E124439516D12E48A459F8ADC570CF85E29F9BE2D872781FE0C
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...K.../....."#.D.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....).....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...m.../....."#.D..._....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....=.#r.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...../....."#.D.2.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....U.Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	892
Entropy (8bit):	5.628366918271756
Encrypted:	false
SSDEEP:	24:UPJ/3i25PJ/bkf2dkPJ/H922dPJ/x3kn2:cJpNJQ+dMJzJJe2
MD5:	9B1518318538 18AE4A5DEED9432116A4
SHA1:	833BBE99ED4C468089ED3F04CBB19CDAB3B43169
SHA-256:	E2C2DDEF3280F98E3B75192694F9FB704CF6AE13FD513F344A0FA63B418A76A9
SHA-512:	8B8F1A87A654AF9854FC37E35A54294199B6AE9E497601746F49A6380C627371F44703D55B79ED19FB2D80FB267DD411E5463193C724810D5A04BC7A409271B8
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ./b..../....."#.D."....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...D.../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...k.../....."#.D]NU....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....n@.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .pc~.../....."#.D%z.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....2..h.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	5.687498004368286
Encrypted:	false
SSDEEP:	24:ehp8v7JICXh81JIC5hN887JICph6q1JICjl:ec5X+5T9pLjl
MD5:	D0C09CDD7D0FCF9D1E1F558C4131A41F
SHA1:	7F42EBFFDB25E421F8A0F4BB8AF3B4372107BF36
SHA-256:	7DE1F8B3D0BE15E288663695E4747BF41BE325B43EE56212DD0C956D2815F170
SHA-512:	105EB2D76EA8475DB88AB252F589623EB3BF63F4B38BDA59E9BCC4D195BB56D9B4A49D733D7C24CB4CB3118415459975223BCCD0244D56B630FB760E2D9889 7
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .w...../....."#.D.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A.. Eo.....DiW.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..CD.../....."#.D4.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.. .....A..Eo.....f.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .k.I.../....."#.D..U....A.;"./N_.,.:C..2....9L.H...3 :...A..Eo.....A..Eo.....<{5.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...~.../....."#.D.....A.;"./N_.,.:C..2. ...9L.H...3:...A..Eo.....A..Eo.....%.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	832
Entropy (8bit):	5.637656533123545
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhurfXLHzLzgm2d/1TK6tYOEYOFLvEWdrIhuZ0qkTLzgm2d/1TKw:0RRPbReYRYqKReBR0/+ReRR2tqWReG
MD5:	3A4B0637FC79109A443709080BF6F8EA
SHA1:	75F8B5A2ADD366AE0292DA596885E59417AF4474
SHA-256:	AF0DCD4DEE299791EA79D9B033C9060C3A9FCFB5B30C2E5A6BD0D985E95D65B0
SHA-512:	03E636194F85F5EC47D8E41E37CAF48C1265D6BE3F20A194A77542AFB36E64AC432F01E4BD79D26E57E34D9F124334DFF2E21E0D5B8E3136A46694D58086247E
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .$!..../....."#.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo....../.. .....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...C.../....."#.D.f.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A ..Eo.....2.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...k.../....."#.D..T....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..... .....A..Eo.....k.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .aJ~.../....."#.DW.....AZ.Z}Q..4.o....0+..[|..n:*. .U.W.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	752
Entropy (8bit):	5.6578173234021545
Encrypted:	false
SSDEEP:	12:6JJKrn2InJJKWqt2IRJJKg+Nn2ISJJKRGr2IoX:6JID9nJIWqt9RJIgwn9SJIMr9o
MD5:	C453CBDB88219DDD358FABEF9B145804
SHA1:	266F0F492ABC3BA6646D454616385407F57B4DAA
SHA-256:	3C4CD68E666EF27E23C1C4ECED6988BD19E9A53672023D5EF50F831E965FA2E7
SHA-512:	7AC5F71382D48ECDA8B77E2D8D1D7F09538FAB4F9898FEE6B85E03CD32043FE0CC87D9ED37C692F9AE3DAAB8D904D2960267EFFB4EB7ECEAF2901E002DA2C EA2
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.D?.I....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....N.....0\r..m.....< ...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .ag:.../....."#.D.n.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._k eyhttps://rna-resource.acrobat.com/static/js/rna-main.js .Y(b.../....."#.D<24....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....^.....0\r..m.....<...)6....._keyh ttps://rna-resource.acrobat.com/static/js/rna-main.js ..!t.../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.647539995399082
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuckOikrhUDLYtmOZn1TK6tRWYOFLvEWdBJvvuX//hFvhUDLYt5:xRBJVkOidDcFZL4RBJYhFKDcFZL/l
MD5:	CC333E629E134E584FF993B745D978A6
SHA1:	F007226801D400A651DE751097C320521F2207BF

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
SHA-256:	9550176E07293ACDBBBE66BE9392C340E00258F75604456E41914BE5B35D1374
SHA-512:	C04A294FD424EAE811FF5255AB3BCF297CB6B3F24C5C95B367A55BFA016C2B393900D9BF8F6796143BE910A4A90BFFAE7BF14CF66EFADCF205FF201BBDF6E597
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .t=J.../....."#.D.1....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....(9.~.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...../....."#.Dm.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....o.t.....

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):	5.634650687572027
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7BsWkdaVPu1TK6tr/sRPYOFLvEWIa7zp73a/4daVPu1TK6tQ:BPH35kkcCPHhq4kcdPHb/YcOPHE0ec
MD5:	E2FD9CCABAE3A31860B98E37BE6E0D1F
SHA1:	618D2EE4D536CA5C9B63490CD65B8D0D10F0F93F
SHA-256:	5CAE732DA52DB498D1B750353DDF32B47061AB1B1E1E26DAE6E7C3E553C082CB
SHA-512:	E32FFA7B6036EF9BE6B429C2235FECE636691CAFB03A7D2A74CEC9028EC9B81375E18C53A305B1494378E3ABEB333BD60F20CF7D47D395AD93B5B5D7DFCB1716
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...../....."#.DRb7....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....m.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...8.../....."#.D*t{....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 .i._.../....."#.D..".....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 ...q.../....."#.D..n....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.646295261121077
Encrypted:	false
SSDEEP:	12:bJRT96uRJr0NTJRT9c/Ir07C5JRT98Udr07:9NwuR+NVNW/F7oNiH
MD5:	7CDE46AB20C55F30D9182D7C29A68606
SHA1:	1A0BD1C28083271937B693043A3D086C94837D13
SHA-256:	CE31DE7FF8CDB9976526816F587CA70A7E1E6415C5A9FA62D2AB7A226B1A69BF
SHA-512:	E6E250BC0E1D484DE87BCBB9EAD2EF38AE5D7AF43B621C9898B2D12DD9189A0C8D0C00D183E04CA194FB0D6A467B736220DA2815F706E59D40358DE032C46D
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .B7..../....."#.D.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....9O.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .b.E.../....."#.D.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....Gc.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..4..../....."#.D.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....`.....

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:	modified
Size (bytes):	416
Entropy (8bit):	5.622358144552465
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQjH96jBRCh/41TK6t0Qt6EYOFLvEWdccAHQtna/S0jBRChU:XRc946Di/EPRc9Sa/PDi/E
MD5:	3328A679255A5D28D5068DF8BE1D7744
SHA1:	FFF2901C4683E31D48FDC7F41A5B838C3D5F3410
SHA-256:	A7F75A66540DAA183330A892A1F8BBE31CB89118010822AEE81A12A07CDB863B
SHA-512:	D91D8B4E924E5F11DD68A2FCA9E3E10E40ED028154C2BAD0A318816A01F59938D4381FA8C4C3D59FD9986D813FBE858AD1B5443CDC1BD1C03F3765D146AF3D1
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .y\K.../....."#.D*.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....>.D.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .``..../....."#.D.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....E.A.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.593663526228214
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhue6qkVl0ULlF4r1TK6tBgqs6XYOFLvEWdFCi5mhux0W+N:bs6xRkiAkVpLlF4nhs6xRki4aLlF4nf
MD5:	51EB4552188FE08F13B5DCA669D5BF41
SHA1:	2A04A59B04313A2AC6FF04A43E7BE0C7BCBFCD0D
SHA-256:	B217C08014D9407E85CB382F4D02271D8D4E8B1F71D17704AFC497736BB46392
SHA-512:	8C751F8EF92675A26E6F755CD26425D0B3F2D01AE66FD5FA83E1FBC6B2AD49BCC089BF0295B6AA43CD7A6B73D1AE2EF0CC6F9359FA12A8C889D3D9483AE61 3D
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .lG..../....."#.D|d%....A.P...#4..l....5...5..).w.. .h .~..A..Eo.....A..Eo.....|.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .>dl../..... "#.Dy.W....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....s.....

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):	5.526345671038666
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuOBqth941TK6tWhYOFLvEWd/aFuR2a/m941TK6t:WRXv9E4R+a/m9E
MD5:	E741ADB22B89BE80E4CFB1C05DADE6E3
SHA1:	15263279502CA4CA5D5E4D91B1B3DDB37319B529
SHA-256:	E1CC28F69FDB35CB73F05DF50883EE5EEFFAD7F7033318306EDCACCAA86C0121
SHA-512:	0C001036B8813000E3D3C2E955073DA54F4AA4F34DBA61284FC57E7DA4C39212129A755C1DCF0E6874834CD713173A9A8906928C0C5548EAA0EA0C72824773F1
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..0L.../....."#.DD.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A. .Eo.....z.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...../....."#.D]......A...a.f.m.i.o.p..3U5.....^...I.A..E o.....A..Eo...../..c.....

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):	5.5787314336949905
Encrypted:	false
SSDEEP:	12:2DRuRMBtYoB9Vd2kpDRuRd/NGoB9Vd2k:8FBtlbdTt0NfbdT
MD5:	0DC9457E3702116E4B2FDEDB146433B5
SHA1:	CC7A0C7F227712CA9C2D68E43EF84C1484ABFA95
SHA-256:	5795517BE74CA4662613B40E62DFD865DB3D38AD239FE70D258B3D1510981734
SHA-512:	87E76ABFFD0A30AEFC792595F5FF1156F8A9B410D7C5168DD1ED3756132DFE93F185C5C764979F7773374C082633DBFF3A5819A0B2CDE08E2D365CFF5099CD2
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .[.L.../....."#.D.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....s..... ....0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...../....."#.DR.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..E o.....?!M@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.61992633062428
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Qi9yxxHlouA424r1TK6t4/EkqYOFLvEWd8CAd9QrgilouA4r:+RQR0PzrneURQGgGzrnHORQ6/wzrnB
MD5:	A7FF1325AE4767FC1DA8004F8DB78443
SHA1:	CDBBAEC867D7AF2C1E5A517C2FDA6A3726158690
SHA-256:	7EB7FA0F359238A710ED84B25E2BB39C816C6AFA8A7A57A0BE8DA77A9E6CF053
SHA-512:	A38198B1037207DB16683790A44C8DAF4BD8C3B5ECABCDDC5C8247FD277F656B7762D7E7120214A46D9E3AB25D1C12A2DAC9A64022B1380B958E8164DEF1A5 4

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...K.../....."#.D.....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 ..In.../....."#.D.kb....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....i.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .k..../....."#.D.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.. .....A..Eo.....t.....

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):	630
Entropy (8bit):	5.60555649094796
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAu2tORyC8n1TK6t6eoXXYOFLvEWdENUAuCl/KsMyC8n1TK6tY:xhRTIa7QGhRTgl/o7Q7hRTxtH7Q
MD5:	D856F5169F2BC7E956B85F3E033AFBB4
SHA1:	4F2DA9BDF881724A9EB60C96126B14B53EA06F02
SHA-256:	9508DEA5614D46FA9DD91577B45FDFB048D4A640F65579768D1096CD1015DEDA
SHA-512:	8BEB90DC49C0B2AA72A66479917445937943AB41CF4BEFF8433605543EA309CA2B6D43A5E25B971F6D918662D308E108AAA15FE4EC74AF140B95282AF32D5100
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...../....."#.D.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....J..a .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...E.../....."#.D.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.... .....=.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...../....."#.Dn.....A8.../...;.\\o....1.....+..A..Eo.....A ..Eo.....5.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	884
Entropy (8bit):	5.628168826551707
Encrypted:	false
SSDEEP:	12:nRrROk/Vu80mcRrROk/VzWmv9/dRrROk/VS+DmQ1RrROk/V2Tm:nPJ/g8JcPJ/p3v91PJ/A+CQ1PJ/Yy
MD5:	D846EE5FBB37DCB883E531F832C2A5AE
SHA1:	3F2F1EEA9928C62C4C172D7A0247239D855B7401
SHA-256:	650736EBBEB38859F508ECA9717B59526BE21C6D6717990F500ACDD79635057A
SHA-512:	F542F1D327D74939805804DE8557A2068E8F012C1BCBF3216DD4FE215C0BD4CBA982331F2DCBE902126524A9DC2AE1DD27FB3D5A649689B2C005EFAFB05CB7 1
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...../....."#.D.k....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A.. Eo.....K.u.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .*ED.../....."#.DJ....A ./.ev.....N~..6.b.....$.j;:C. ..A..Eo.....A..Eo..... {.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .r/l.../....."#.D.-V....A ./.ev.... ..N~..6.b.....$.j;:C...A..Eo.....A..Eo.....F.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..~.../....."# .D,-.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....T..L.....

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):	630
Entropy (8bit):	5.616930157147604
Encrypted:	false
SSDEEP:	12:qxRcQ9du7ECgxRcuvlqAdu7ETxRca8ZQdu7E:UTHu7EBhqeu7E9T8ou7E
MD5:	1EA4CA10A7185079F8BCFDDCEE6A8C37
SHA1:	C0A561B8B2F17A1989600BF85F4D3CB846851AF7
SHA-256:	689B9FF8B041343150130745DA644B9BBA3F6BCA7130B0C64B54253A529C82FD
SHA-512:	56D9AC7AF21C0155FAD1D4093FC02B6A75EA9B0CACC3756AAB22163F2689A1508043B1015C4C0C11B5C5C5A3ECCA88FF6623FC0B00B2D4F25C3D3DCB5ED2A 74
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .)."..../....."#.D.8)....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....&.].....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..8J.../....."#.DJ.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo..... .....A..Eo.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..j..../....."#.Dp.....A...U...I.>P...X...x..0U.~;m.x.k.A. .Eo.....A..Eo.....L.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.5690822676194225
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuHVK3Jn1TK6tA2MOYOFLvEWdwAPVuMXll/De3Jn1TK6tOMOY5:2R1iVKZLzR1Pv/SLkR1fkyL
MD5:	90C8691E65257874A9AA23A8068470CD
SHA1:	4595BDFDF3E2DDFAF8A84437A71BB8DF31B1A1E1
SHA-256:	4EEA7B50053A9C3322734308DC971F3945A0ED05EF34B38096CBE1496D2E6D49
SHA-512:	E5D94DEF72F415858AAB33F551E891A8D4498335D52AFEF55E8B766FF0769DD3226336B308C442232A0A81F23FEEBD22ABB41F841ECA666E0BA5168FB9386B89
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...../....."#.D,~.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ...U.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..YE.../....."#.D.J.....A.....k....F..D..O.n;[.1m.....=..A..Eo..... ...A..Eo.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...../....."#.D.|.....A.....k....F..D..O.n;[.1m.....=..A..Eo..... .....A..Eo.....pf].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.638958476103755
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQDWq9xfzhcsBXIh1TK6ti23PXYOFLvEWdBJvYQba/lByzhcU:mxRBJQxq9xfDB0hxRBJQX/l0DB0C
MD5:	568E3051D9423791E27C611AABF617A5
SHA1:	D311B3482F85A0EB5E7D7F2104E48138ED7EAA8D
SHA-256:	23ED868A9DE65B8508266DB1D3EA189DE7DC53B3A89A2ED4CD8F62C29F9654E8
SHA-512:	F6F1FD837386CE93BA52F991D3C3E345C75363564FED7F2F837816D88B97BB0EF4C59A04F846E0D921B1FF46F8E9BA2C68F7C10C8A5A72F74940210A1FBF2AB
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .r.K.../....."#.DB.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo .....euU.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...../....."#.D1^.....A...k..`..N3.... ..d..$[.....{.A..Eo..... ....A..Eo.....K.p.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.619509658831574
Encrypted:	false
SSDEEP:	12:3RrROk/sJZlcBRrROk/s8td1cXRrROk/sm+mlc6RrROk/syW9lcb:3PJ/OZOBPJ/Dv+XPJ/ux6PJ/N1
MD5:	7C0A47640BB3793508731AA6128BCAA9
SHA1:	8DDF756121BADC5EE392160576AF692999787B59
SHA-256:	13BF3F19FDB976A914FD534600349BED7A6B4C6704DDED817CAB88B5DAA29467
SHA-512:	98142B919955D9FA430095A9F53A9B92B08CB49C6E98A5CB3440F294B9B23BE8F9B70C68F10DF08EE113D3ACEF35DB71194B7CF08B9CB91C56915B06F0CC1BC B
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .z...../....."#.D/.....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 ..FD.../....."#.D%@.....A.....9 Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....=.0.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plug in.js ..0l../....."#.D..V....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....L..i.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop- connector-files-select/js/plugin.js ..~.../....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....&.....

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):	5.210640607965078
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QP+UXBdJNtMfxz9pKiVBb:h1zZ4+dsp6PUX3tEz9p1z
MD5:	555E99AECE828C3C7821C2FA4E3A5AB4
SHA1:	93BD8DE42E3BF7E25B1461D03B621F3BA0DC8D2F
SHA-256:	BA25C7659F4BBEF94A707F7C9237DFFB275E18CC9417C9A77EC4F2D350819962
SHA-512:	AEF04DCE53BA5B96F8946F7942DF76C5C46A2EC99A6B9FF426C973BFCA13952588F69B1B91B3DD50FB571DCE1E679D203EAEA4098E328ED2164A30A29E17BE 62

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):	5.216117512722661
Encrypted:	false
SSDEEP:	6:8URtoM+q2PWXp+N2nKuAl9OmbnIFUtwLU4EtZZmwyLU4EtMMVkwOWXp+N2nKuAlz:nt+vaHAahFUtw4jtZ/y4jtNV5fHAaSJ
MD5:	9D521B6E676D13027B52D85E5B9A57BE
SHA1:	9316E872ACB3FB4D069CF02B3BD1D3DD54F7903E
SHA-256:	6F377B40592B3DB5A7358CB88B8605298E555B4772F60ABA26803C99D5C66F8E
SHA-512:	658DBB097F4C1CF5E5DBA0AF311A5D17F98C3E9A404C8B644BD8EA5885DE79B4818691A751BB0ED5051A0AF467CA8785810FC151226221E58922365DC842A62
Malicious:	false
Preview:	2020/11/29-10:03:53.869 181c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2020/11/29-10:03:53.878 181c Recovering log #3.2020/11/29-10:03:53.878 181c 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):	1703936
Entropy (8bit):	0.009034856540883936
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMiCsMiCsMi9sMhCAsMhCrNsMhCrNsMhCrNsMhCrNsMhCr+sMhCDo+v:JKKKKnono
MD5:	02D75DF3CF23EE0F2EF72205A2F48E72
SHA1:	DBE0E88B2A1860F5654961C4FB0170C5773943EF
SHA-256:	C7C5A16888DED312800436FE25EF41A697CDE09FB91D70736CE2ABF454D4A8F3
SHA-512:	B34FAE483D160613A73AFEC919794CA35345F6C5B3DF17B4BE9244B361E952BD0434A0D29184748D972818952EAB83AE7B4DBC3B8A397071C2E5466BD1CCA88A
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129180347Z-189.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	1.8860963472929324
Encrypted:	false
SSDEEP:	96:E3hNtouS8u27Q40JN1hNaw5pIPEwb3G94d0zFqv7ZKIZPZHv35ZMzUP7PJum2zl4:yz7ZaX7FGxR4lXbXXdWW+R
MD5:	11FAC24280131BDB9F5B3A68F18CECBF
SHA1:	BB6D156299CE74E6043D6F2AD6C84572F964637A
SHA-256:	14722BAD22E332CDA1B6D4FB7067FD489725E491EC4238DB53102EB25B1AFEE7
SHA-512:	384F7BF137ED78791AD1AFCAC4AC8460191A54F20A42D046318BFC3A9243B7492BFBB97D909C6ECD16272FC16D2DD7068AD2FEC2042FD7C77C88ABE6DCC840A
Malicious:	false
Preview:	BM.....6...(...u...h.... .....DDD.UUU..... .....www.fff.....___.....DDD..... ....

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

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Size (bytes):	32768
Entropy (8bit):	3.386460540436001
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQGOhFVCsL49IVXEBodRBkRGGOhAVCs749IVXEBodRBklGGOhe0:iGedRBaedRBbedRBXedRBw
MD5:	FE1D012A2CFB575F52BBF326333C5A46
SHA1:	E247628C4C4A5804F20E784DD6EA8E5940872C8E
SHA-256:	AE781CD951B7A01A780A6572BD73102A3C467EF88A1F4E87BDA2E1D4E1115DC4
SHA-512:	96ABA9F739D6799D940E917581BAEE6A7B49ED7B1A035244B29C7A22E9E5EA93422B0E10784E2CB0321E675F3EBA33E57ED642F55D947E07B6D0422D293C2D3C
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):	3.199323246039711
Encrypted:	false
SSDEEP:	96:47OhFVCPj949IVXEBodRBkDGOhFVCsmLR49IVXEBodRBk2GGOhAVCsZd49IVXEBM:4niedRBFLGedRBlCedRBoyedRB0
MD5:	9C5376FAC4DF02009821090BF16482C5
SHA1:	D08841379B803D1A1342F417CB5C300D4DDAA381
SHA-256:	631333ACF0867F24FF796A4455A6AFA6B97C701D076E571F21EB44A4907EDCCA
SHA-512:	0533A9182D9A1C4CD984F5B0C172AFE91952FFD9550035A6A3CDD6391BF01DD4163213916552B1E3C2DDED750B347FABD3B451A9D908427EC92A83CCC73E43
Malicious:	false
Preview:	.....|.....X.. .h...y.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5620	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

Static File Info

General	
File type:	PDF document, version 1.4
Entropy (8bit):	7.941002651961782
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Invitation - Prime Minister of Israel.pdf
File size:	118780

General

MD5:	e3f4a57d14090a2866c16e4f2321bb30
SHA1:	0163a63054fd5da40c44e685cb7601decb8a2cd0
SHA256:	63f3f7706c4d6ca347ec95beb3e9401fcc3d8d263e8da4cf809d663f837757d0
SHA512:	919c3ee1141c8eeaa7fc219da8fecdc713477bdaf99b230c5ce2a622fd97737ab26c5b2d0ec968286efc5abad397518b121ffa9b298a8fd45e1a727b53c50d84
SSDEEP:	3072:MpK3dmmACoS0/MHEOFsYZjqO3iUaiJFs3YR:MpWdm5LjysViJF/R
File Content Preview:	%PDF-1.4.%.....2 0 obj.<</Length 3 0 R/Filter/FlateDecode>>.stream.x..[[....~._.....%0.[.@..0....$....=/...[wWKj.wC.agm./u.....\..?o.N.~.u.4...../.....Nq..w.q<M..q...]NV.;.....a....5.>..nJr.F5.....e./..?..t../.K..v..|.....X+S.;.=..|1...2

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.941003
Total Bytes:	118780
Stream Entropy:	7.943462
Stream Bytes:	115699
Entropy outside Streams:	5.116033
Bytes outside Streams:	3081
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	19
endobj	19
stream	6
endstream	6
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	1
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:03:34.130160093 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:34.157315969 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:34.832859993 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:34.859812975 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:35.664891958 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:35.691919088 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:36.425170898 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:36.452666044 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:37.401889086 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:37.429193020 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:38.130481958 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:38.166038036 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:38.858625889 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:38.885691881 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:39.710414886 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:39.737613916 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:40.691587925 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:40.729583979 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:41.570544004 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:41.597865105 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:56.765604973 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:56.804966927 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:56.828418970 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:56.865086079 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:57.781502962 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:57.818540096 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:57.831324100 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:57.868246078 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:58.831419945 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:58.867275000 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 10:03:58.881423950 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:03:58.916858912 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:00.881629944 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:00.917054892 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:00.931595087 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:00.958722115 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:04.884841919 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:04.911957026 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:04.994299889 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:05.029895067 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:06.199347973 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:06.226443052 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:07.254822969 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:07.292273998 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:26.009946108 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:26.053996086 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:42.546519995 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:42.573595047 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 10:04:46.614689112 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:04:46.651823044 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 10:05:17.310476065 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:05:17.337735891 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 10:05:18.564110041 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:05:18.599894047 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:27.846013069 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:27.897073984 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:28.430617094 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:28.466237068 CET	53	63619	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:29.079998970 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:29.141158104 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:29.479746103 CET	61946	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:29.515274048 CET	53	61946	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:29.938205957 CET	64910	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:29.973834991 CET	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 10:06:30.406352043 CET	52123	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:30.441871881 CET	53	52123	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:30.880930901 CET	56130	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:30.918898106 CET	53	56130	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:32.129892111 CET	56338	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:32.165807962 CET	53	56338	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:33.041809082 CET	59420	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:33.077933073 CET	53	59420	8.8.8.8	192.168.2.3
Nov 29, 2020 10:06:33.422455072 CET	58784	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:06:33.458372116 CET	53	58784	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:23.916672945 CET	63978	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:23.958337069 CET	53	63978	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:24.171423912 CET	62938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:24.198596001 CET	53	62938	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:24.612324953 CET	55708	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:24.656814098 CET	53	55708	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:28.196592093 CET	56803	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:28.240256071 CET	53	56803	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:31.149012089 CET	57145	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:31.184487104 CET	53	57145	8.8.8.8	192.168.2.3
Nov 29, 2020 10:08:31.435102940 CET	55359	53	192.168.2.3	8.8.8.8
Nov 29, 2020 10:08:31.470801115 CET	53	55359	8.8.8.8	192.168.2.3

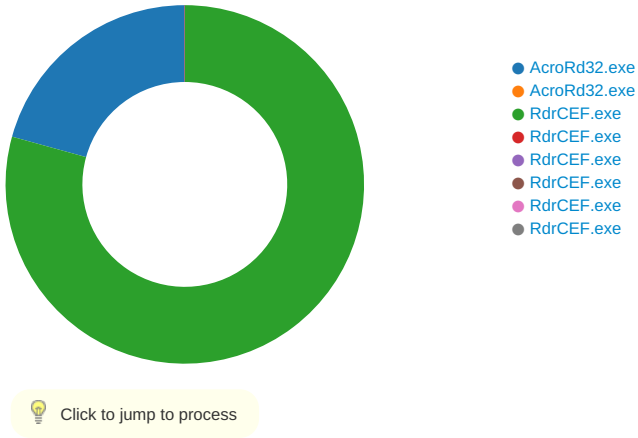
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 10:08:23.958337069 CET	8.8.8.8	192.168.2.3	0xa375	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 3016 Parent PID: 5560

General

Start time:	10:03:39
Start date:	29/11/2020
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\Invitation - Prime Minister of Israel.pdf'
Imagebase:	0x10c0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10F65C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	111AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129180347Z-189.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5620	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock3016.1.2436489975.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	1142657	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rn6khmu_zafkb2_4c4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R10ed2x4_zafkb3_4c4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R2qwawl_zafkb4_4c4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rg26kl4_zafkb5_4c4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11883C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ry1awbi_zafkb6_4c4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	110EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5620	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	114D405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	110CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	110D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	10CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	10CEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	10CEA55	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Invitation - Prime Minister of Israel.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Invitation - Prime Minister of Israel.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	111DF69	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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 6E 76 69 74 61 74 69 6F 6E 20 2D 20 50 72 69 6D 65 20 4D 69 6E 69 73 74 65 72 20 6F 66 20 49 73 72 61 65 6C 2E 70 64 66 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 30 31 31 32 39 31 30 30 33 34 36 2D 30 38 27 30 30 27 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	118780	success or wait	1	111DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	111DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	111DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	111DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	111DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 5620 Parent PID: 3016

General

Start time:	10:03:40
Start date:	29/11/2020
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\Invitation - Prime Minister of Israel.pdf'
Imagebase:	0x10c0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 5072 Parent PID: 3016

General

Start time:	10:03:46
Start date:	29/11/2020
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:	0xff0000
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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	10E59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	10	10F83E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	83	10F8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	219	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	10E59E2	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	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2172	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	10E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	8	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	24	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	24	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	56	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	60	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	4	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	10E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	8	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	6	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	12	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	10E59E2	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	255	10E59E2	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	3	10E59E2	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	12	10E59E2	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	3	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	10E59E2	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	87	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	4	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	20	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	4	10E59E2	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	23	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	3	10E59E2	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	486	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	55	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	60	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	20	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	4	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	10E59E2	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	6	10E59E2	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	3	10E59E2	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	268	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	4	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	225	10E59E2	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	3	10E59E2	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	18	10E59E2	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	3	10E59E2	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	48	10E59E2	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	3	10E59E2	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	3	10E59E2	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	3	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	234	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	10E59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	216	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	2	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	24	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	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	10E59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	10E59E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	10F83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6240 Parent PID: 5072

General

Start time:	10:03:48
Start date:	29/11/2020
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=1692,565714168120498593 5,18091407090887986711,131072 --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=18388359474767092242 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xff0000
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: 6368 Parent PID: 5072

General

Start time:	10:03:50
Start date:	29/11/2020
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=1692,5657141681204985935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11592911304768251189 --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=11592911304768251189 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xff0000
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: 6452 Parent PID: 5072

General

Start time:	10:03:52
Start date:	29/11/2020
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=1692,565714168120498 5935,1809140709088798671 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10775127221883232441 --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=10775127221883232441 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xff0000
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: 6496 Parent PID: 5072

General

Start time:	10:03:55
Start date:	29/11/2020
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=1692,565714168120498 5935,1809140709088798671 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8896761926437382365 --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=8896761926437382365 --renderer-client-id=5 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xff0000
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: 6704 Parent PID: 5072

General

Start time:	10:03:58
Start date:	29/11/2020
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=1692,565714168120498 5935,18091407090887986711,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2426508304687755912 --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=2426508304687755912 --renderer-client-id=6 --mojo-platform-channel-handle=2132 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xff0000
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