ID: 324342
Sample Name: Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim
Cookbook: defaultwindowspdfcookbook.jbs
Time: 09:50:48
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

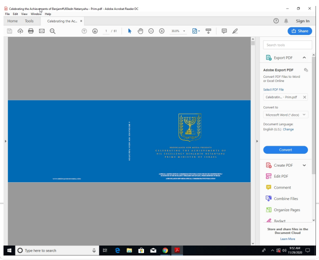
Analysis Report Celebrating the Achievements of Benja…

Overview

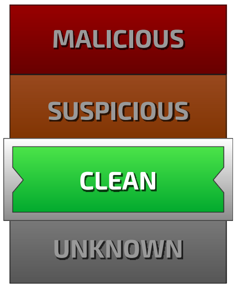
General Information

Sample Name:	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim (renamed file extension from none to pdf)
Analysis ID:	324342
MD5:	fb9dca5d3e122ca..
SHA1:	76ed2e8f2c876cd..
SHA256:	c679efb245b1ce9..

Most interesting Screenshot:



Detection

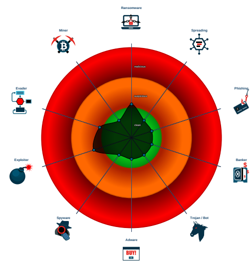


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to access load…
- High memory usage for Adobe Read…
- IP address seen in connection with o…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 6116 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6128 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 3492 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5524 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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15540169491933176135 --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=15540169491933176135 --renderer-client-id=2 --mojo-platform-channel-handle=1660 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6152 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1684,2245332663126947271,2796270942385178651,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5895458359813356849 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6196 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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2668593196950910738 --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=2668593196950910738 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6352 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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5586481229821336722 --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=5586481229821336722 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6444 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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13996197876522443299 --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=13996197876522443299 --renderer-client-id=6 --mojo-platform-channel-handle=2144 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

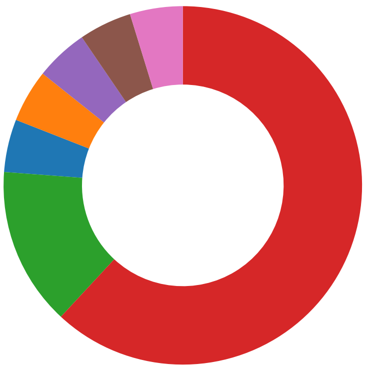
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Exploits
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

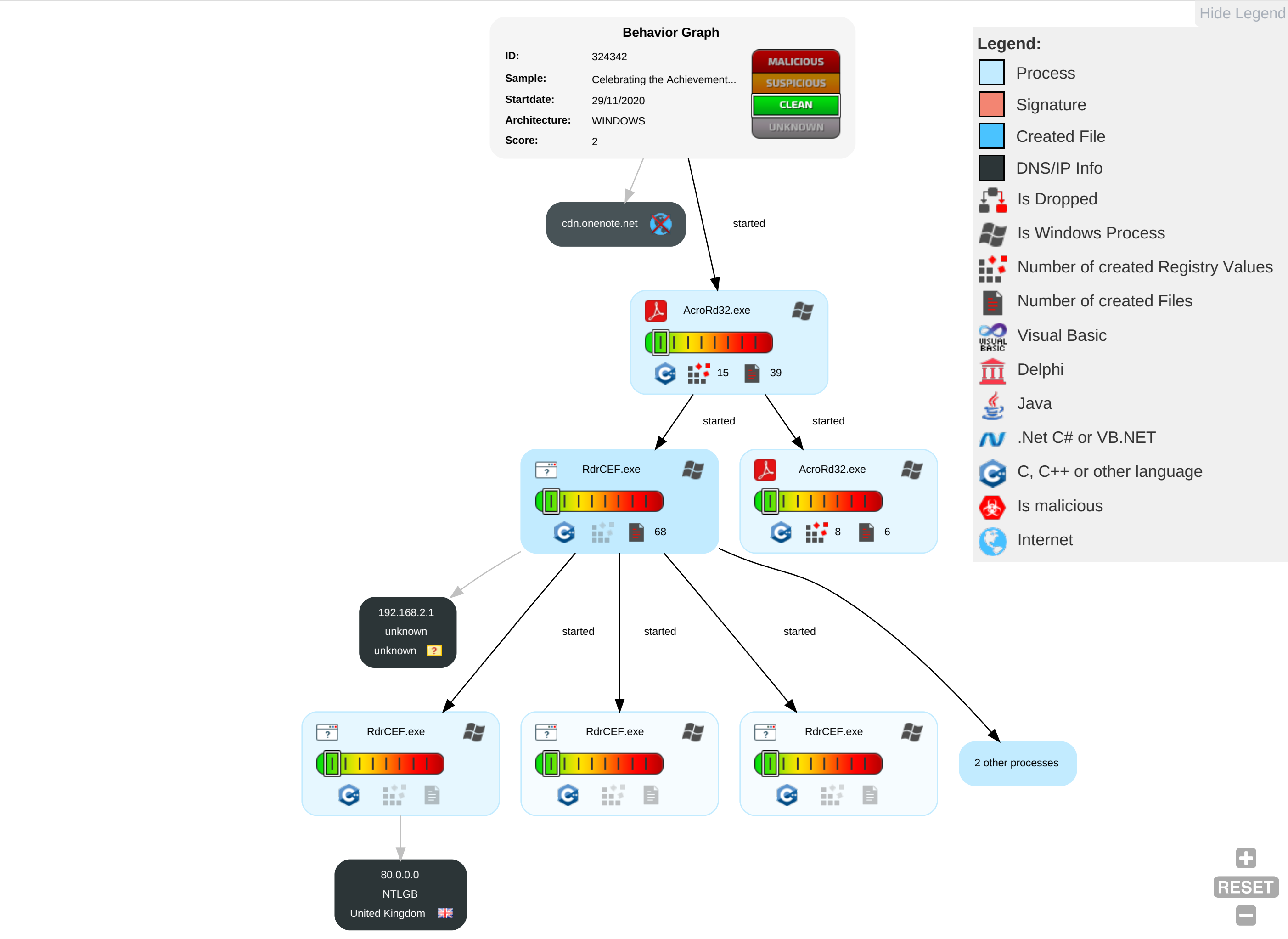
Click to jump to signature section

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	Impa
Drive-by Compromise 1	Exploitation for Client Execution 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock

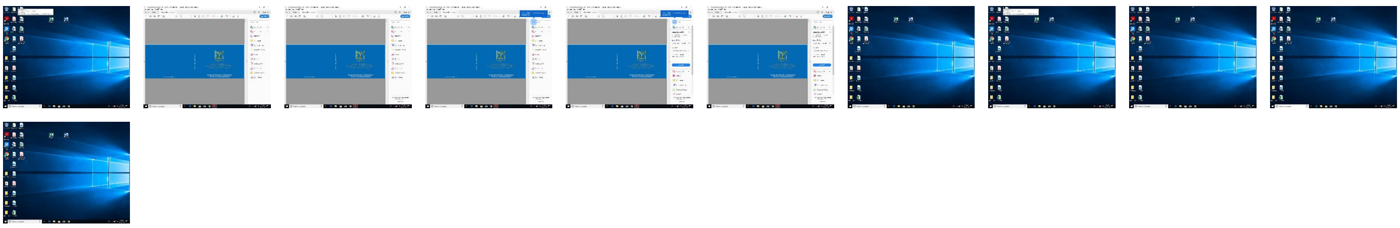
Behavior Graph

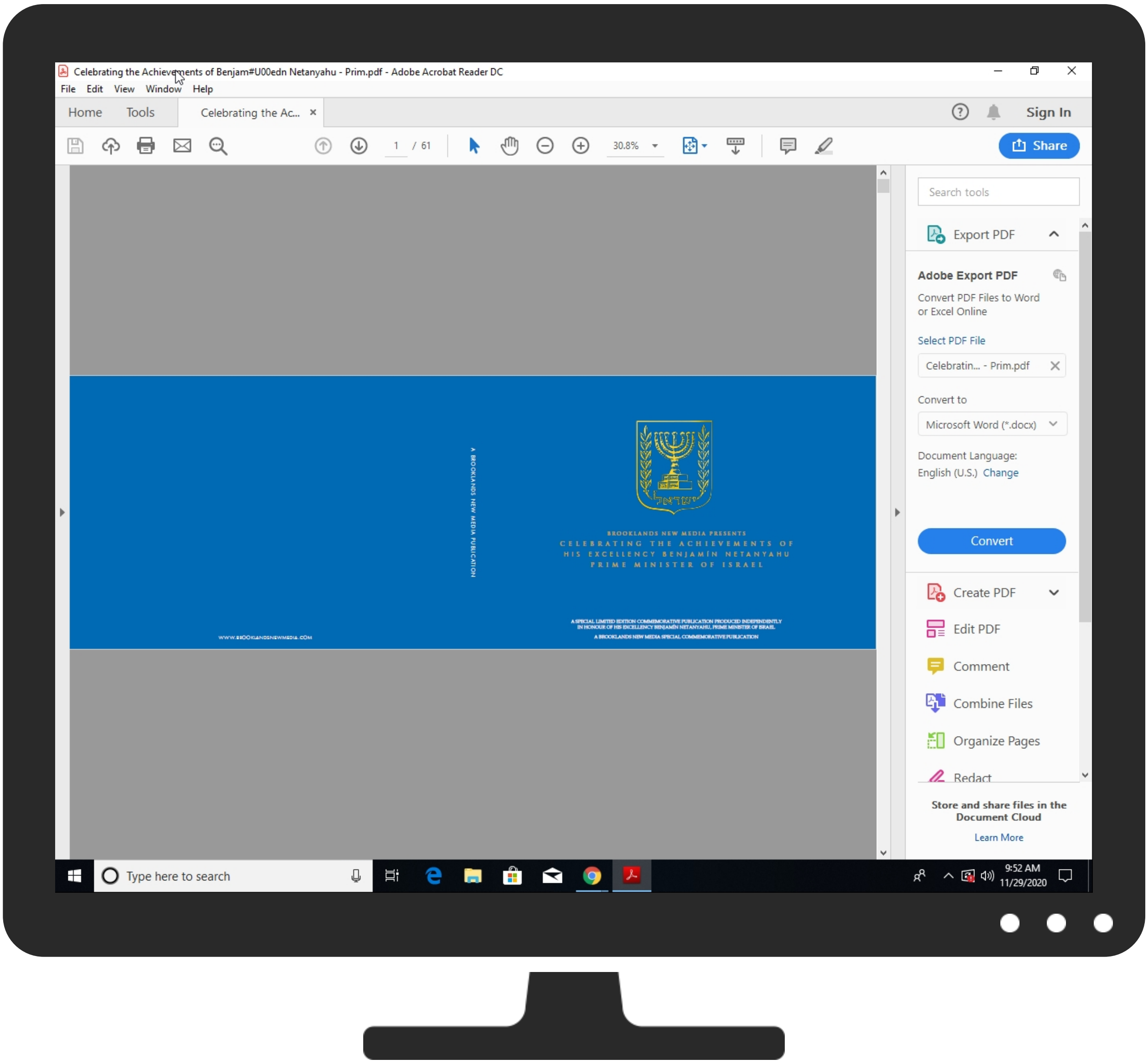


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	0%	Virustotal		Browse
Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cdn.onenote.net	1%	Virustotal		Browse

URLs

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

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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/E	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C-	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	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://https://api.echosign.comRL8	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/ER)	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://ims-na1.adobelogin.comQ	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/c	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/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://cipa.jp/exif/1.0/)5)	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s	0%	Avira URL Cloud	safe	
http://www.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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.onenote.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.useplus.org/ldf/xmp/1.0/	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/detail/1041876728?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/E	AcroRd32.exe, 00000001.00000003.422898356.0000000013203000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/C-	AcroRd32.exe, 00000001.00000003.422898356.0000000013203000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/detail/1213863567?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false		high
http://https://api.echosign.comRL8	AcroRd32.exe, 00000001.00000002.440603712.000000000D390000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cipa.jp/exif/1.0/ER)	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.gettyimages.com/detail/1041876744?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://www.gettyimages.com/detail/1191103531?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/:	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false		high
http://https://ims-na1.adobelogin.comQ	AcroRd32.exe, 00000001.00000002.431108735.0000000009593000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.gettyimages.com	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	AcroRd32.exe, 00000001.00000003.422898356.0000000013203000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/c	AcroRd32.exe, 00000001.00000003.422898356.0000000013203000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.gettyimages.com	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.440603712.000000000D390000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000003.422898356.0000000013203000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/detail/635460660?utm_medium=organic&utm_source=google&utm_campai	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/eula?utm_medium=organic&utm_source=google&utm_campaign=iptcurl	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://cipa.jp/exif/1.0/)5)	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://xmp.gettyimages.com/gift/1.0/	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://www.gettyimages.com/detail/1201459640?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/detail/655527090?utm_medium=organic&utm_source=google&utm_campai	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.441850255.000000000D7DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.431108735.0000000009593000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s	AcroRd32.exe, 00000001.00000002.441850255.000000000D7DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.426758262.0000000007D30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gettyimages.com/detail/1204352280?utm_medium=organic&utm_source=google&utm_campa	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	false		high
http://www.aiim.org/pdfa/ns/id/s	AcroRd32.exe, 00000001.00000002.443897570.000000000DE8D000.00000004.00000001.sdmp	false		high

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:	324342
Start date:	29.11.2020
Start time:	09:50:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim (renamed file extension from none to 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:	28
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:	clean2.winPDF@15/48@1/2
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 PDF document • Find and activate links • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 204.79.197.200, 13.107.21.200, 2.20.142.203, 2.20.143.130, 92.122.146.26, 51.104.146.109, 92.122.144.200, 52.147.198.201, 104.42.151.234, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.11.168.160, 92.122.213.247, 92.122.213.194, 104.123.31.226, 104.83.127.80 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, acroipm2.adobe.com, arc.msn.com, cdn.onenote.net.edgekey.net, skypedataprdcoleus15.cloudapp.net, wildcard.weather.microsoft.com.edgekey.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:51:44	API Interceptor	12x 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	
	sldiW.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
	sldiW.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):	820
Entropy (8bit):	5.711271816821708
Encrypted:	false
SSDEEP:	12:vDRM96alL3ZiEhDRM9I3ZiE+DRM9vZiEKhDRM9DZiEj:7/uLAE10EU5EK1FEj
MD5:	B5AE2AC994F18305C33BAE4C13129F4F
SHA1:	4F167CDA07E09B7223A19160932F40FE798DC5D5
SHA-256:	8E497D345F46D0D89A91616F343FAEC1B6ADC24935B5F5220B3B348B1B809393
SHA-512:	DE40321203ECD6138748FEECCD26B5470539DE426C358BABB3A363C61187CCA69538CF51B14319553F7F5491186FB2FC1A8BB1D69154D007BB7CC37D7820A06
Malicious:	false
Preview:	0\r..m......M..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .g6..../....."#.D..J....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 .g.(.../....."#.D.Z.....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 .F|@.../....."#.D8.M....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 ...f.../....."#.D.E.....A....d.{v.^.G...d.W.:...P..k%..A..Eo...... ....A..Eo......,./^........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	696
Entropy (8bit):	5.660134726822664
Encrypted:	false
SSDEEP:	12:V9zf3i9PQe9zQkTE9PQWl9zOz9PQA9zxdS9PQ:Xzf3i9PQizTE9PQqzOz9PQYzxs9PQ
MD5:	8A79018FE72FC215E5197B4D9759D48A
SHA1:	D0F94EA107E5143E89047544D5131640326A0800
SHA-256:	026EFDD7C36D43394A88FDD73D39EBA6D18E09A6D440DD6031CC5942B0CE3ED1
SHA-512:	F00F283AA78FFD3E1FB878B860991E904F05F0B8E152DC6528723D4D604645998FC46B6FBD60411FB64D4D1BC157C76A7184FE3439CD8936FF338CDC98CFD61
Malicious:	false
Preview:	0\r..m...........,....._keyhttps://rna-resource.acrobat.com/init.js ..7..../....."#.D.d.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo..................A..Eo........\.........0\r..m...........,....._keyhttps://rna-resource.acrobat.com/init.js ..../....."#.DNC.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo..................A..Eo.......=;.........0\r..m...........,....._keyhttps://rna-resource.acrobat.com/init.js ..y1.../....."#.Dl%.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo..................A..Eo......s..........0\r..m...........,....._keyhttps://rna-resource.acrobat.com/init.js .5.X.../....."#.D......A.1.x.'.vI..*|Z. .o...+.4....0..A..Eo..................A..Eo......d:.f........

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):	5.636343604671505
Encrypted:	false
SSDEEP:	24:tB4v4QfSBZB4v42SB2B4v4Xvx6SB6B4v4TSBO:nMxSBjMFSBGM0p6SBaMISB
MD5:	D8E3F64636F669D4C28C82A9AB0E639A
SHA1:	89BB9C276D287B850E717A25FE9471767D659F77
SHA-256:	A512F92E4ACF12036B1C9222F9E4DE3BD7593940128D38D4C5F4E68D81563B8E
SHA-512:	CE3A98FF53718AD87FE8FF313660843935A161929C4580F13BE0FB5C3CD5C01C8C78D520185105DABEF8710220599B506FFA5B8E53F38B3347A78ABA7A47C0F4
Malicious:	false
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..I....A..hvDO.N.t@.... .n.*...... ....A..Eo..................A..Eo......z]..........0\r..m......v...n......._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view /selector.js ...#.../....."#.D8......A..hvDO.N.t@.....n.*...... ....A..Eo..................A..Eo.......kw.........0\r..m......v...n......._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracke d-send/js/plugins/tracked-send/js/home-view/selector.js ...?.../....."#.D..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 ...e.../....."#.D.......A..hvDO.N.t@.....n.*...... ....A..Eo..................A. .Eo......",d.........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	464
Entropy (8bit):	5.697370006216664
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0

SSDEEP:	6:mNtVYOFLvEWdFCi5RsTNulQiWulHyA1TK6tlNtVYOFLvEWdFCi5Rs93+/lA9CZiM:IbRkiDyNunWussbbRkiD3W9zWuss+
MD5:	8BD4B725BE5A882C3452035D44AE7FCB
SHA1:	320E706947C863DF2A9FD4CA3B2FB99AF5DF0FDC
SHA-256:	8775BE498085DB49579EE502ADDE24605213BDEB99E4E218D3CFC15A2CC699AF
SHA-512:	ECD26CCA3092E820907EE323B77731508E72790729F285E34F633020DB1AA0B5E35DC31792112B78B94788DC15B7BC5A99982534B4005E406395D23454AEE51B
Malicious:	false
Preview:	0\r..m......h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..../....."#.D..[....A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo..................A..Eo.......-..........0\r..m......h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...D../....." #.D.lV....A..8 P..a...R..Y....7.@..2Dm{..A..Eo..................A..Eo......Q.7.........

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):	5.600467648166394
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVus/lUVyh9PT41TK6tY++yiXYOFLvEWd7VIGXVuQcvlLLT:pyixRutV41TEmyixRuqcFRVV41TE
MD5:	226ACB456F660B47A717355EA142065D
SHA1:	5C2EF11CCB3B6CBCA8CB5B27D2816D4325AD48A6
SHA-256:	7B200DA5D82BE7557B9B2CA498DDDEBA0F03EB72781127AC8432CC5A1E480D0D
SHA-512:	130460268ED96ED384DABAFFE6881D3225A877FC9BE0BCC7414CF167B25154F79933E243F8CC9F4D83FD24E2321BEC2CA14F871C1CFF71D56F70472343B2CF7
Malicious:	false
Preview:	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. ......_.........0\r..m......R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...f.../....."#.D.......Ak.Q.....-_..y.....O...>..1....A..Eo................. .A..Eo......G..a........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.646666694814673
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQvEqlJsqhLZIl6P41TK6t1vYOFLvEWdhwjQPwRlpVZhLZIl6P45:0RhkqsSLZCRRhkygLZC
MD5:	5F4B2FD6AD9CC0F72C37B4A9BEF64C93
SHA1:	DAAA7AC9DA5336095712788A3340D3BB27CAE73D
SHA-256:	675B35E7021E87C82E44F48B8D42F19D72A166546CE9FCCEFF8DF716A060A2F7
SHA-512:	26C93CC169FC04DD2B9770595C9D628449E067445BA5229EB978F2E51E579C7D39E84B28FAD52B346AA0EFE2AF40E6036CB6CA6527DF4264C0F89CB20070BCE B
Malicious:	false
Preview:	0\r..m......X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...!.../....."#.D.X.....A.].>....uUf..N...k......c..l.A..Eo..................A ..Eo......r.z.........0\r..m......X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .7Uc.../....."#.DM......A.].>....uUf..N...k......c..l.A.. Eo..................A..Eo......Y_8.........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.558055166099032
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQmvlO0uF6g1TK6tVAStlMJYOFLvEWdGQRQOdQYttlRF6g1TD:2RHRQCkF1oStlIRHRQCbBF1
MD5:	EBED28894FD8A1489EE5FB658A923723
SHA1:	32F3ABD45CE52CBF9110B7C8F0493B91828D2E5F
SHA-256:	735BC4B0A1FF8C9B6A4A81CC71A9A0704711A65BCE5E6FC52ACEEDE39FCAF49B
SHA-512:	F44C2401BB064008F1C287D0FC3509E348ED8596B5B6E8FED0213B59F15D095BC32EA1855C8243D04217C6BBC2D7FE5BFA0F8DBD06989DD3281B124B0A89A70 B
Malicious:	false
Preview:	0\r..m......Q..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .qh(.../....."#.D.......A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..................A..Eo ....e+........0\r..m......Q..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...f.../....."#.D8......A..c..y/L....|y.n..C/I.....X7-ne.A..Eo...... ....A..Eo......nW..........

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):	5.655589460606377
Encrypted:	false
SSDEEP:	12:Z5MwasMuR/Ex5MJNQMuR/ER5MmKQMuR/EX5MZMuR/Ed:ZSwaFuR/ExSJPuR/ERSmSuR/EXSeuR/k
MD5:	E247BBEB135760FCBBEA2FD06E329E42
SHA1:	95DB58A49342C9D4FEA4B93028698F3054438E7D
SHA-256:	808447C180BBB4ED05E3187C6AF8607B66348B20C7BA0E58CC2E1832E0CE58BC
SHA-512:	4EC64F5C14B83FB5BB7D59B51F1E8DC7767B5B7B6A9CE6A2BF9AFDEA8BB2CF9A3D4F047A70E508AB918A5649B17D88ABBC54A91E193F9824BD51EE2630578DAB
Malicious:	false
Preview:	0\r..m......3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .R{..../....."#.D.......A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo..................A..Eo......^...........0\r..m......3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .{...../....."#.D._.....A.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 ..1.../....."#.D.A.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo..................A..Eo......O...........0\r..m......3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...X.../....."#.D......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):	5.594386307988863
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuIlMNiSm0bbsIDMGH41TK6tH:XfRM94KsIZE5
MD5:	C7748EAE35C4EBB965CCB401F4D97247
SHA1:	12A44CEBC564F6E77C312A559F685221A2618F35
SHA-256:	7C447E175643A0C6A895F780550B1EE74103B85B3BEBED6952E40CACE2C4FABC
SHA-512:	30C556DC61E6F7D776A8F7619881D30CC36AB0B8F89FFC36DEF0B5429E1F7555A491940E762E17CB71E343D34ADDABB4C92C9EED95C83CB01A3FEE661F3C89CB
Malicious:	false
Preview:	0\r..m......T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .}.0.../....."#.D.j.....A..`.....^....L>..Xa./......C.y.A..Eo..................A..Eo.........q........

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):	5.559822226616038
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtugl1+by0zBUKSAA1TK6tq4fPYOFLvEWdtu9Lqlvk0sby0zBUKSh:pRabenRlk0sbe
MD5:	1517252D66548BB370EB6A85791102A3
SHA1:	8C168FB15F9E38C6C7DF5ED79DFA58C4F956A9C2
SHA-256:	82643A596235254DE1CAD724102D172191E06C69ED4937853325597F9D161C32
SHA-512:	BF756E1E11EA4B82A9DA26E4B852A04C3530B578FA3B21525C47F61B70CE64FA5DEB1BC8BA036917B21393ED6E370D86F145FB2642AE274BD07D45F8B5AF8C50
Malicious:	false
Preview:	0\r..m......V..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..G).../....."#.D.......AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..................A..Eo.........r........0\r..m......V..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..Ag.../....."#.D.......AQ..E.=....=h`t..t..3%A.F$ ..w..A..Eo..................A..Eo.......D.3........

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):	5.62567789051962
Encrypted:	false
SSDEEP:	12:KkXxKMSCvewRtUlEkXxKMSCviSY3tUlikXxKMSCv7gtUlBkXxKMSCvjjlRtUl:KkXxiCmyWEkXxiC5Y3WikXxiC8WBkXxG
MD5:	9292C0DA9C8CFD1D78F8B04434BC4EAC
SHA1:	0368F7B5FEAC1062BDDB4A484CB1E302E62B9A68
SHA-256:	457918AA171D768713030DC0689005C86481161E446E19DA2EB383EBC3DADE8B

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
SHA-512:	F547DDC40852AA87A77B5CF286317EB1CBA5768DB9B490C02577BE3EE4CB6FE9A98D38162D9B6971CEBBCB057BECAAA189865DC52D600A28119EC29BF4A8CE91
Malicious:	false
Preview:	0\r..m......1......5...._keyhttps://rna-resource.acrobat.com/plugins.js .fy..../....."#.D$......A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo..................A..Eo.................0\r..m......1......5... ._keyhttps://rna-resource.acrobat.com/plugins.js .Y...../....."#.D.X.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo..................A..Eo........wM........0\r..m......1......5...._keyhttps://rna-resource.acrobat.com/plugins.js .).1.../....."#.D.7.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo..................A..Eo......V.$.........0\r..m......1......5...._keyhttps://rna-resource.acrobat.com/plugins.js ...X.../....."#.DM......A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo..................A..Eo.................

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	748
Entropy (8bit):	5.619600620581292
Encrypted:	false
SSDEEP:	12:5h6OLFTik8jh6OL6Rwaknh6OLsk/h6OL+ok:5h6K38jh61wvnh6k/h6B
MD5:	363143A3DA799368A54B792377E52CF1
SHA1:	89172024DAF5CEC939C26C10631F33ED0A0B5852
SHA-256:	8E23F23D79B11B7C5A03ABE7D7F5648EBAAFE822A8100AB840BF3C8F15E1EAE9
SHA-512:	C3C99D76C84106E17BDD0F835D715DE9EFBBCFDDB77F98463DD005933D29B29080653161A3E6C0EF1F46697784AC3C1387082F4D46341E7DEB389FB252BC55D
Malicious:	false
Preview:	0\r..m......;...l......._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..../....."#.D..6....A..q.O...j....._y..L^z...?..@N..A..Eo..................A..Eo......4%..........0\r..m......;.. .l......._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..../....."#.D.\.....A..q.O...j....._y..L^z...?..@N..A..Eo..................A..Eo......M@u.........0\r..m......;...l......._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .Q.;.../....."#.DoE2....A..q.O...j....._y..L^z...?..@N..A..Eo..................A..Eo.......bV.........0\r..m......;...l......._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .A-a.../....."#.D.......A..q.O...j....._y..L^z...?..@N..A..Eo..................A..Eo......9...........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.686175224408189
Encrypted:	false
SSDEEP:	24:UB4v422CwzXLngB4v4S+wzXLnKB4v42wzXLnIB4v4LwzXLn:8MkbnIM9bnKMCbngM1bn
MD5:	748808B1DD2873063C6299A02DE037A2
SHA1:	C4CA10B5B7511F25662852F5863F9E811A688E76
SHA-256:	4E1FEFD442B8434695B03AC4AB6EB036BDD758407978273DFE6BA6CEB46C13D4
SHA-512:	35292ABCBDD81968D6B19A92A4CB6C2D4951263E3EF9491791BBFD14DE8FE0B09090250C103A03ACCB79F8A802EB5540D5DAB556139A6D07077FCAFEE69A4D7
Malicious:	false
Preview:	0\r..m......t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..../....."#.D..N....A......H...{...2. ./.k`..r4.C. .A..Eo..................A..Eo.......".z........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(.../....."#.D.......A......H...{...2../.k`..r4.C. .A..Eo..................A..Eo......M..s........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 ..@.../....."#.D4.J....A......H...{...2../.k`..r4.C. .A..Eo..................A..Eo.......Kg.........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 ...f.../....."#.D.......A......H...{...2../.k`..r4.C. .A..Eo..................A..Eo.......P.........

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):	5.540706722778198
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQeUulTl5GFCaa+41TK6th:NRMHdZl5Gda+En
MD5:	9D8129E5F5076A83CFB45FB152C509C4
SHA1:	B6EE196D032E217B8C932027EB99199054F9A8A0
SHA-256:	EE721EAA1329F9F61E5D1246C31549BDD3DAC4FE22B34E19B61DA6EBA32E0627
SHA-512:	E478C70D601B6EAF71CC3D86A4C94231240C2156CA0AFEDFFC0825EB8F754A5499EBAED6E6A40470D9DDE1D6BD579C6CFED7163B6B2A3533480E18B610746E60
Malicious:	false
Preview:	0\r..m......R....L......_keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ...1.../....."#.D.......A...G.3D.....Q.g0...._.Q.........A..Eo..................A..Eo........h.........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.549919496365361
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuQlkP11TK6tDMs2VYOFLvEWdvBIEGdeXuclc11TK6tdt:BsR2Ese4VVsR2EseS
MD5:	097B27E0FFF19D2A1446921BA432247A
SHA1:	1185E05F57B58D77D01BB901EADCE31B1875E8B6
SHA-256:	11C1B31E30B7CE2680C2CB19204FB56A69C780B5E09F466A7939160B098334F6
SHA-512:	26383E97E02D632FF43CCA097EDB7B90D46C76C95829E0409635B42EA82D8950CF3F80E6ABA7AC93AFE8110A94DCFD8B2529A4CE55ADE6B9DD570F9381B1942
Malicious:	false
Preview:	0\r..m......S...]......._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..S$.../....."#.D.[.....A.A.o]@r..Q.....<w.....].n\....A..Eo..................A..Eo ....1..........0\r..m......S...]......._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .R.e.../....."#.D.,.....A.A.o]@r..Q.....<w.....].n\....A..Eo...... ....A..Eo.......K.`........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.648186030298204
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQPl8SPB7OhKlvA1TK6tmMaVYOFLvEWdwAPCQfLulcFkcTB7OP:RbR16nSpJkYbR16UjDVJk
MD5:	A7AF7EDC0F96829575B8823FCBA09856
SHA1:	9649ACA39B021F895EE26F75BE501BA71D36115B
SHA-256:	F42DFE862D12C76D5E98FFA80DC36152CE621C226DF1E6357EADB4BA4AE24154
SHA-512:	8AB4FD0ED9708FC762DDB9316B2DBDA3C953CE28601A4B9C6EE7C83E683FB60369AF342D1B4A81F39D379A59FB33B15A4398E961323F73FD22017FC3D68D834B
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......O.......... .0\r..m......J......{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .aSc.../....."#.D&......A..4T].....Tw.....(..b...EO....9.A..Eo..................A..Eo...... _DWH........

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):	5.629545704626591
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuYqlHSrgrjQdFt1TK6t5b2s2gEYOFLvEWdGQRQVuqulBy+:B2geRHRQ66gn0TbR2geRHRQNayR0
MD5:	D9B32122F6337011C1BB6C1F7E6D61F9
SHA1:	8EE265CA8D9182DDFCA375BDB9EDED671B5E907F
SHA-256:	EEC7BE90014CDB90AE274195E511254472EC033D93F2AE06CF88B8195424DAC7
SHA-512:	BC8BFD7BE7760D38D48948D94D5645E802474723D7D3136950D64C6B796F9E5A34CAA1DD3C3CC5BEFEF7A5DA9F817BA056C1F154A069B9DF9BE4DBDE82F3E3F
Malicious:	false
Preview:	0\r..m......S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .. $.../....."#.DC<.....A@..{o]...9o|..qY....T....{..u.b..A..Eo..................A. .Eo........1.........0\r..m......S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .k.e.../....."#.D.......A@..{o]...9o|..qY....T....{..u.b..A..Eo ....A..Eo......3..J........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	824
Entropy (8bit):	5.696639792183308
Encrypted:	false
SSDEEP:	12:WyeRlFRDt1wL3MyeRl3t1wdyeRl6/OMyt1whm9yeRlLt1wC:WJ9RDfw4JvfwdJiWMyfwhqJDfw
MD5:	35224B025216D721243E432ED8F1CF79
SHA1:	E4C9B4C5D0E2A1062B6615F92F45DD94C36817B4
SHA-256:	4445E171A8134DC219C4BBF535063C3356D4E70C5CBA337926DC91623273B0F8
SHA-512:	07DA04D94F609A6A45A61277A37E5BE227E6E9286B98C13E2BEFD4ECAAADFFE213DFD4C227EEA7F38F4C44091DDC196CC08F79243DE1A8417D7AA35D2EA76AC

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Malicious:	false
Preview:	0\r..m......N..../......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ....../....."#.D.Y=....A.t\a......x5.'OuE.C..@......x..A..Eo..................A..Eo..... ...02........0\r..m......N..../......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .b...../....."#.D1......A.t\a......x5.'OuE.C..@......x..A..Eo.............. ....A..Eo................0\r..m......N..../......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...>.../....."#.D.L:....A.t\a......x5.'OuE.C..@......x..A..Eo........... ....A..Eo......J.CI........0\r..m......N..../......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .}.a.../....."#.D.Y.....A.t\a......x5.'OuE.C..@......x..A.. Eo..................A..Eo........8B........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	436
Entropy (8bit):	5.61352818477239
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu7O0/lIYsqwK+41TK6tK8nYOFLvEWdhwyu1lupqwK+41TK6tMl:wRhMYkwK+EESRhDkwK+E
MD5:	F52B0B2A4EDA2465EA7A360C7884DB2F
SHA1:	C70DA31CA5C546FB8632A6FA743E6FC4E5C706CB
SHA-256:	7BE137C7C6E7AD9276DA4CC583BDD67F32639910BE950A628EC6BC50B1054652
SHA-512:	6A1E901146D26370D428528C8E13BDF14EB323E2616D24014631C34B76A1C63B05E20A6125981DF0ABE2ADBAE8FF956222F6D8D9215EC42D8019659FA3DC43F
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.$G.A..Eo................ ...A..Eo........2\|........0\r..m......Z.........._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .N.c.../....."#.DN......A.......7...o..a=.98I......(3.$G.A..Eo..................A..Eo.......v..........

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):	5.652015486517911
Encrypted:	false
SSDEEP:	24:/PJ/BKps4rtVPJ/H0bs4mPJ/rs4+PJ/1s4:XJ4u4rfJv0I4aJw4iJq4
MD5:	1B40024B6A3BC34AA5391449491FD24C
SHA1:	7D868AD8AAB1C4DDA9153199341C8D0DC295E62B
SHA-256:	F996F62DC78649953480A8BB6E89714A8D782973719E51ED9A70D39F96BFDDD8
SHA-512:	5DDF115ABE1ACCB89AC579059F04126644C3EE0493A29988FCECCD00D9AE3AED4A5F3B0507BFF545458E8757A6B575BCEFF6B102238157A2A1FB42BDA6CD6 1B
Malicious:	false
Preview:	0\r..m......f...F......._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .fe..../....."#.D.'=....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... ....A..Eo................0\r..m......f...F......._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..../....."#.D.^.....A..~..rw.+[.... !.)?..f.U..(=.=.A..Eo..................A..Eo......~..@........0\r..m......f...F......._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .. .=.../....."#.D6::....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..................A..Eo........H.........0\r..m......f...F......._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector- files-select/js/selector.js .w.a.../....."#.D.G.....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):	5.669668837726127
Encrypted:	false
SSDEEP:	12:xqT8CtF/rcNCPLnD9qTv6NCPLn0qTm3zNCPLn4rqTKzNCPLnG:A4CnSMnDMYMnrC35Mn4uG5MnG
MD5:	4C57CDF158204A587FCFC385755FB866
SHA1:	40EA32DE80142243ADCD0DA8B8B002BC5BB5684D
SHA-256:	9238F1D20534958A4C3C8843ADD1527A35E67A14719DF69A446FAA03A3C17778
SHA-512:	D7291B7F4194E23940F2F5EB77C847EBE554F69E0077A4BEDE3EA418543066235BDB83719209FFEC94871A11D83DEEBFC1C1F68A482B591F9680DBE31194BB5
Malicious:	false
Preview:	0\r..m......:....f......_keyhttps://rna-resource.acrobat.com/static/js/config.js ..../....."#.D.6....A..~]...%s..<...n.f..<.....1#..U..A..Eo..................A..Eo.......W..........0\r..m......:.. ..f......_keyhttps://rna-resource.acrobat.com/static/js/config.js ..../....."#.D.......A..~]...%s..<...n.f..<.....1#..U..A..Eo..................A..Eo.......n..........0\r..m......:....f......_keyh ttps://rna-resource.acrobat.com/static/js/config.js ...;.../....."#.D.<2....A..~]...%s..<...n.f..<.....1#..U..A..Eo..................A..Eo......y.m........0\r..m......:....f......_keyhttps://rna-reso urce.acrobat.com/static/js/config.js ._.`.../....."#.Dk......A..~]...%s..<...n.f..<.....1#..U..A..Eo..................A..Eo.......+5x........

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Size (bytes):	828
Entropy (8bit):	5.674510098895626
Encrypted:	false
SSDEEP:	12:zRM6mmzsDbRMU2JzsDl/llZRM7zsDWRM9zsD:ztYDb7DtllZJDWXD
MD5:	498553A7BEE03C2288899651915F90F6
SHA1:	74EDD4CEB23FB92413F81AD5119F2B871C05490F
SHA-256:	47CB54DD3B3500CFDD0DE2D7693939ADD34A577C35BD924E616B7B71685F9EC6
SHA-512:	E5618B7DB7A94E70AC78FC0B218A6392A91B3EA6D78C0AE410C70D68274A15CDB3A41C557B9D5821794341CF893CBF8DE9DE88E58E20535CCFC23C7E0FCCA80
Malicious:	false
Preview:	0\r..m......O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....../....."#.D..I....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 .wc$.../....."#.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 .o.?.../....."#.D..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 ...e.../....."#.D0G.....A..z._a...'.v.......4p3..1.']...A..Eo..................A..Eo.......?..........

<table>
<tr><th colspan="2">C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>840</td></tr>
<tr><td>Entropy (8bit):</td><td>5.654908814746241</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:6lJRkleLoMtlUlJRToMVclJRUzvoM7QClJRTRoMj:Y6KoMtlyVoMo+boMEwZRoMj</td></tr>
<tr><td>MD5:</td><td>EE4B97EB4FE1DE37DC8C225885B5E6ED</td></tr>
<tr><td>SHA1:</td><td>C6DCEFFEC203AD12D7F5F81F05E6F4BF86F8BF2B</td></tr>
<tr><td>SHA-256:</td><td>345CC187DEE0132BBFA39C1F73B007C3AECC73A055469253062B4EAB88F1C5BB</td></tr>
<tr><td>SHA-512:</td><td>28D173BE95D95B47D54C44A35E1254EB38B64552FE4D24D5A93164B5BDD526A7CA5F4E1BD850D24FFB1D0248A5D2BBB270483FB3CEE67B8EF3E0605C880C2A8</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>0\r..m......R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .(...../....."#.D..I....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..................A..Eo......6_..........0\r..m......R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...'.../....."#.D.......Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..................A..Eo................0\r..m......R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .v.?.../....."#.D.D....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..................A..Eo......G1h]........0\r..m......R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...f.../....."#.DGZ.....Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..................A..Eo......sOAi........</td></tr>
</table>

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):	5.6582630781989804
Encrypted:	false
SSDEEP:	12:F8hRrROk/yhxRqw25N8hRrROk/Z2kv8hRrROk/B2+8hRrROk/A2:UPJ/yhTB2GPJ/Z2kaPJ/B2zPJ/A2
MD5:	BBCCA2D7FBCD4A97FE5603B2062AC3FA
SHA1:	8F0B1A3F5A6DAEFF05D1FB40326D3DF6361CF3BD
SHA-256:	63A9D977147D5330F43A912C0B02CB71646AA37FD5229043864DBB4A2F18ACF3
SHA-512:	15A7FFEA2179BF5D23B79721D13C623A3FF49F03EDA49FB21205EF774EFF169BC86408DF284FE6D9098C7D0BD6A8B285AE1B42A1AC9639A6C3031FE7C7492D1
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.H.....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 ...=.../....."#.Di.9....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 .2.a.../....."#.D2=.....A..%.k.SZ..~W.....:)'B..ad......A..Eo..................A..Eo........yj........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	5.739218539138368
Encrypted:	false
SSDEEP:	12:ehRcEnNJIC6hRckr7NJIC8k/QhRcUY7NJICrhRc2ZYbm37NJICR:ehfNJIC6hDrZJICYhKZJICrhPYbMJIC
MD5:	B52CB9CC4E600CFE00F9717245883E9F
SHA1:	6A724772E8BC7304AF2DD5A66DCD1DA005C1FA80
SHA-256:	1424EB0C189DD590A5968BFA4ABFF631EEB75451168AB5445527796DC2E0B8E9

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
SHA-512:	33F107E6DFE190EE6801346333906B1E550D41F788F1F9ACE69050BF369811B9085667E453799B268AA9F74182343D9CDEA5D3315EE7B9320F54F0B732C20A4E
Malicious:	false
Preview:	0\r..m......U..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .W...../....."#.DB|=....A.;"./N_.,.:C..2....9L.H...3:...A..Eo..................A. .Eo......^G.L........0\r..m......U..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .Y?..../....."#.Dq......A.;"./N_.,.:C..2....9L.H...3:...A..Eo ....A..Eo......&..1........0\r..m......U..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...>.../....."#.Dip:....A.;"./N_.,.:C..2....9L.H.. .3:...A..Eo..................A..Eo.......:6.........0\r..m......U..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...a.../....."#.D......A.;"./N_.,.:C..2 ....9L.H...3:...A..Eo..................A..Eo.......7.]........

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):	5.632938723023893
Encrypted:	false
SSDEEP:	12:0ROp/oiReCRs/RedRG73Re3mcR696K4Re:0m8C5dik2cUl
MD5:	5D553FD0FA05E022E4D586D6E4D88F79
SHA1:	39BC4D851584011E053F9844A2BD2F9AFA2B2B3A
SHA-256:	FFB1F9C611BDB65729ABC7F52397A638E4DF80DE1FAE4B50A7BD5C79D49D2C67
SHA-512:	EAC288278A679008A8199453A86BD0CBB9BD515CC5A696C278F7482EE569DFF34346B1C2D91C1D902E0907AD29D760E8AEAF9D9C96B8502586C8AE1CB144F5 D
Malicious:	false
Preview:	0\r..m......P....r......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..../....."#.D|.9....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 ..../....."#.D.......AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo..................A ..Eo......BW.^........0\r..m......P....r......_keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..K=.../....."#.D..6....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 ...a.../....."#.D.......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):	5.656468234718681
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KUll/i8hkx56uvp1TK6tAeAElVYOFLvEW1Krtl0kx56uvp1TK6t:6JJK8rIWiJJKQIYJJK8UqIrwJJKG1I
MD5:	C5F94AE11F0B70300B023A56EA95B18F
SHA1:	6FF9291260C65254ADE9B30A6A3C948FF6AE19A1
SHA-256:	A89A0F70BC57B749DB63E45F017246E5A2BED6D6376FCA934E3716B1D0CEB6A6
SHA-512:	615B72579DF56BBF5715BEF931C84516E68F6E21D2D9BB45CF7708530C01F017D97CC0FB03DD27B26F076A180D66F75CBF733C411F98BBD13C01CD7973CD24E
Malicious:	false
Preview:	0\r..m......<...)6......_keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .f..../....."#.DVe.....Az?...SwC...^..y.....V..7R-O.....A..Eo..................A..Eo......VO._........0\r..m...... <...)6......_keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .O...../....."#.D.......Az?...SwC...^..y.....V..7R-O.....A..Eo..................A..Eo.......5..........0\r..m......<...) 6......_keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...3.../....."#.D.......Az?...SwC...^..y.....V..7R-O.....A..Eo..................A..Eo........w........0\r..m......<...)6... ..._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...Z.../....."#.D.>.....Az?...SwC...^..y.....V..7R-O.....A..Eo..................A..Eo........W.........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.623710336336768
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuqlyehUDLYtmOZn1TK6tg2WYOFLvEWdBJvvuXvllhUDLYtmOZ7:xRBJErDcFZLuBRBJM2DcFZLl3
MD5:	35FCAE91CA71E55359490672CD212CDB
SHA1:	68B5808FC09FA546AA27D1FED19FB2373970E75B
SHA-256:	252E4530CE827CC95EA2DB023B4D77CA469D756430537BE4B76BF5F647DEF891
SHA-512:	B0726E9A20D5D646AFE3E61583B8D52282A2D2D53C20C00F43FB69DC140FCB0BE6632EECA50582E65EE4E3DF7AAB62C60CEE1D67C69D565437C1E43F64651D B4
Malicious:	false
Preview:	0\r..m......V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..W$.../....."#.Dmo.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo..................A ..Eo......dcOe........0\r..m......V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..e.../....."#.D.......A....t.q..W.EZ....1...[.zC.7mD..A..E o..................A..Eo.................

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
File Type:	data
Category:	dropped
Size (bytes):	844
Entropy (8bit):	5.637206015348115
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7G9X/lkCj7VPu1TK6tjK/EsRPYOFLvEWIa7zp75Els4VPu1t:BPH4vK4chaTPHrT4cFPH8Uc5rPH8XGc
MD5:	737EA1EDF56375AB86CDCA4179E5AA10
SHA1:	940E91D0BCC8AD5E812107CF453C01D25E90A4BC
SHA-256:	8EFF7CD96B3C3FCDDAD04ABB51D11756904B2471D8E669A54ACBCC4C00017861
SHA-512:	D3600F21D50A6EBDC44EDEF5A9F10E88053C32E994A220083A657EFD952AC2D15C56FDDBA6D26C74E892255849582DB2F92A904E293B15752EB7FDCCB2B9F41
Malicious:	false
Preview:	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 .<...../....."#.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 ...1.../....."#.Dur.....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 .3.X.../....."#.Ds0.....A...L...Im.@.........E.nW...IP..A..Eo..................A..Eo......B...........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.628655418060546
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QjUulL0lPiM3Y1TK6tZAeKPYOFLvEWdENU9Q1tlDPiM3Y1TK6:bJRT9gn0Nr0kzJRT9gLr0t
MD5:	01935B0BD4C153A078F50E4224C32F49
SHA1:	A50E103DFE958A8AA30BE039BE78CCFCFFBF7500
SHA-256:	7B258DD82281DCD516A1E779FC260F753B4B34F54B5588332A2B80E23BAF50DD
SHA-512:	4D91F3522A0020E44E0B8F3DF0D51583631FF25D523F0219E4BBA5A47B02F297F33BF2F21B1FF98482668513DCE6EAC68575D09248209343F208F24D831FB31E
Malicious:	false
Preview:	0\r..m......P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...!.../....."#.DQ......A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..................A..Eo.......|]`........0\r..m......P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .cTc.../....."#.D~n.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..................A..Eo........sB........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.628817702795534
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQcIvlJSYhjBRCh/41TK6tjQt6EYOFLvEWdccAHQH/lqjBRC:XRc9yvSYhDi/E0Rc9UQDi/E6l
MD5:	5DFCBF8806441C6C8559C41F429CCD38
SHA1:	EE8F11347B61339ACD28DCF20563748C6870ACC2
SHA-256:	ADE3F73529A202CC737BFCBC8B38EA72F19D05305F7398128A2359DFE7FF89B6
SHA-512:	E22110A289B57BC92A1DC027E0E870FAF5D337E36C48DAC54C1F76D0B1C7655FA13C41A2908CC820FDCAABD45006C67EAE771EB6593A3C6D54BACA23FD7F9D7
Malicious:	false
Preview:	0\r..m......P...W3......_keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..f(.../....."#.D;:.....APJm...0x.x..RD...BB!@5..<..]....A..Eo..................A..Eo.......y.<........0\r..m......P...W3......_keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...f.../....."#.DB......APJm...0x.x..RD...BB!@5..<..]....A..Eo..................A..Eo.......].........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.617279290363936
Encrypted:	false
SSDEEP:	12:bs6xRkiy/DoLlF4nShs6xRkiGw0oLlF4n:brxpy/soOrxpn0oo
MD5:	6F7CBA4DF11724A45EA13097EC8863A7
SHA1:	A248153C13F0235005FB7DA6479ACDEB313C8858
SHA-256:	4595A8B1E96A2E5DF14D42E18D2FE4654F3FFEDC2BECA7056750C7997ADFEC59
SHA-512:	E416948693FCB69919D019CDFC3474AF2D5E8F6C21D6D3E7F2AF2A4F9D8581568D8925233F3D50DF29305E507CA8762DFBDFAE06E895616B8EF38A0A2182B3C

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Malicious:	false
Preview:	0\r..m......g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .}...../....."#.Dn4>....A.P...#4..l....5...5..).w.. .h.~..A..Eo. ....A..Eo......KE..........0\r..m......g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..R>.../....."#.D..<... .A.P...#4..l....5...5..).w.. .h.~..A..Eo..................A..Eo..................

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.5928488261965805
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuWTtlQ0Q941TK6tREhYOFLvEWd/aFuZlL941TK6ty:WRGA0Q9EMRZ9E
MD5:	47D6B05E9E2B04E1FCAB8490F72643C2
SHA1:	F5E4418667D3F26952B6A2A6D0B48A33C64B64D6
SHA-256:	0C9B4F2A1CBF6DAA05600DE455232E9200A4233FA6B80954E9DA79E16B68AE24
SHA-512:	EBEAF6A0FEFBBA7866D1AFE73BC907FB7B1089533B8F903C486EB60CEC8E4E61060B3138D42F91CAE9558C2DD7DBC9F9659B46EB40FE4BF1CD75C222D79C0 34F
Malicious:	false
Preview:	0\r..m......W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..X).../....."#.D.......A...a.f.m.i.o.p..3U5.....^...I.A..Eo..................A ..Eo......=...........0\r..m......W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..Pg.../....."#.D.......A...a.f.m.i.o.p..3U5.....^...I.A.. Eo..................A..Eo.......v..........

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):	5.5711479109373965
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQb7ttlbg2oBMqVd3G4K41TK6tNR9YOFLvEWd7VIGXOdQNj:2DRuRD2oB9Vd2kdDRuROeYoB9Vd2ke
MD5:	6092A114A096C0D53E065AC9B5797E8F
SHA1:	552117F60E2C352567AA2A4110EAC449AB0C7627
SHA-256:	335288F4DC15ABFBE0E45034C24C76113378B1A786EAACE190BCD99E6322C76F
SHA-512:	4521D315FA25528D27D81D2539B4237BBBD9B34D8C1B6BF24F7CF6A6BD21D0BE8AB3021D3EE09B4BD7336DA43CFDBF12A8E75268ABF233E2644473FE8EC2D0 29
Malicious:	false
Preview:	0\r..m......P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..2).../....."#.D.......A..y.$..$.v5j...T...z.]..._S....A..Eo..................A..Eo.. .....L.D........0\r..m......P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ../g.../....."#.D`......A..y.$..$.v5j...T...z.]..._S....A..Eo..................A ..Eo......8f..........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	832
Entropy (8bit):	5.618628654468633
Encrypted:	false
SSDEEP:	12:+RQulPzrnO8RQUzrnxRQJUXzrn0URQFYizrn:+lP/nbT/nxy8/n0UIYi/n
MD5:	8965EE82114796F295FA896D3C266740
SHA1:	C4500AB0181AC4D569CB00686DFB78647D69E073
SHA-256:	56A11400C63907F059932D235E7029E15B70CC7EE0943123E29F027D222877A9
SHA-512:	02E8F9775CA47CB064D027F86AB69518E75745FF4EF9F4A4957396F2651B878016B5207720E70083EC148EE70F121209977403244C6D22BC28E2D9D0EC63527F
Malicious:	false
Preview:	0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .m9..../....."#.DX.M....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..................A..Eo... ....-..........0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...).../....."#.D`......A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..................A.. Eo........t........0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..}@.../....."#.D.0G....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo........ ....A..Eo........A.........0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .p"g.../....."#.D@......A#..@..k(v.8g..5.~_....]Pj.*.. 6.A..Eo..................A..Eo......kt(.........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Entropy (8bit):	5.59273182188937
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAubO2uloyC8n1TK6tmoXXYOFLvEWdENUAutUulSgmlyC8n1To:xhRTZOO7QvhRTPUtl7Q
MD5:	8600C4C4EF6630106E31C6CDED88ED17
SHA1:	FE5AEE6513E54A672405F526670FA409448596C6
SHA-256:	B881BCFA6AB0802CF8E497D449EE8ECD23CA542C5C4523097F49E8C00B5AB2A9
SHA-512:	25478754EEFBBBC6F32F389BECC8F516F6CE00A4AE4E555E6D8D599493D529C2B329F7803932809984A21B3C1B5509E11D515BF6C4FF6A38A4BFEB17BC419F8
Malicious:	false
Preview:	0\r..m......R..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ... .../....."#.D5......A8.../...;.\\o....1..........+..A..Eo..................A..Eo........j. ....0\r..m......R..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...c.../....."#.D.......A8.../...;.\\o....1..........+..A..Eo..................A..Eo.. .....Zo)........

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):	5.675824365158671
Encrypted:	false
SSDEEP:	12:nRrROk/VS/com41RrROk/VmmLTmb/RrROk/V1xmERrROk/VYtcmT:nPJ/QcdoPJ/Ijb/PJ/QEPJ/WrT
MD5:	94AAE51E96F4F2C6D9CD0DBE9CD4D1BC
SHA1:	FC47121DEAA213A36A5FCCA2E7545947A2292C52
SHA-256:	5E8EBA92D571D9ED9E9FDD37B22E563EA9D480F6FBBB5E9C617A8B13F6A3368E
SHA-512:	B534FA413F95F027D6A5BCC3C56A14F6A522B1E3204B3834496A2FF47AEB7AB0E7689E94EC849027C6021997751C5E176DA8CCFBF48CD42BEB73B26BCB3176 E
Malicious:	false
Preview:	0\r..m......]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ._...../....."#.D..=....A ./.ev......N~..6.b.....$.j;:C...A..Eo........... ....A..Eo.......HYo........0\r..m......]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..B..../....."#.D.j.....A ./.ev......N~..6. b.....$.j;:C...A..Eo..................A..Eo...............0\r..m......]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .M.>.../....."#.D..:.... A ./.ev......N~..6.b.....$.j;:C...A..Eo..................A..Eo.......e..........0\r..m......]......,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .o.a.../....."#.DZ+.....A ./.ev......N~..6.b.....$.j;:C...A..Eo..................A..Eo....../.wX........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.5934984454836725
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWutNlEYGAdm9741TK6t0eZ/lXYOFLvEWdccAWuIwUulOJ/Gw:qxRc8Yrdu7ELxRc2/rdu7EZ
MD5:	A4D4B11F11A55CA1BE4C54779C4E796A
SHA1:	4107112FCD8187ED03B0AA21D66518A2544B05EE
SHA-256:	C23FD814E050441BDD4E382A61664C52D2976E5B27C8B8B416DC51391F976A7D
SHA-512:	A98ED04E3DFF18869DE6024266C8CB0E2522EF93F626FEBB621B894DDC93301E6A8F1C0A4D3C858FCCDF7AF543EFA310F5118FBECAF9017D52A4A123156B5C BF
Malicious:	false
Preview:	0\r..m......R...F......._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...#.../....."#.D8......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 .!.e.../....."#.D.......A...U...I.>P...X...x..0U.~;m.x.k.A..Eo............. .....A..Eo......gs.,........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	5.5771482914905235
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVugulV9kJn1TK6tz/HeMOYOFLvEWdwAPVuUulwp3HJn1TK6tgg:2R1y9qLFveR1rFVpLyg
MD5:	29F0FA8BC467BDF48C12DA2FB3FDBEF2
SHA1:	3AE85E77AC8ED43C704D91F0C761A4723ABB5197
SHA-256:	4C7D31E73C9457A46F0902240596FE1083E38CB94EB6BA41675D61C2D8A9C0AC
SHA-512:	33E62846CA9B5912A98471DCB0FB6555FB8DA5DCAECF33DFA03C9961D8268251F36BE88F2EACE6FFEB5BD454ADF2ED9F746AE7C118294712B639115CBB29C4 73
Malicious:	false

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	424
Entropy (8bit):	5.700294179387455
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQjqlpiizhcsBXIh1TK6tF3PXYOFLvEWdBJvYQrU+/l/KSIz8:mxRBJQG0iiDB0fxRBJQAjKSIDB0
MD5:	643EDA76C7CCBD75A3E69604646F007A
SHA1:	6DADE3E34B5C271212984957E5031F904DCDA7C7
SHA-256:	D6F2C7EFD7026C3AC8F663314DEABBA64B6C9632E59018A0FF3A7F8053B309DE
SHA-512:	85A588E249CA4940DCF6350683DA6B6F6819A531246EB82DDC2FD8B39640A971716B8914120AF74874D1E8B160E494469E5AB0AD9F85D179DBEFCD64EB1E9CCC
Malicious:	false
Preview:	0\r..m......T......z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..(.../....."#.D.......A...k..`..N3.... ..d..$[.....{.A..Eo..................A..Eo......`...........0\r..m......T......z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .V.f.../....."#.D]......A...k..`..N3.... ..d..$[.....{.A..Eo..................A..Eo.......\ +........

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	912
Entropy (8bit):	5.66028508509186
Encrypted:	false
SSDEEP:	12:3RrROk/sm1tcblfRrROk/sBWnczRrROk/skZKucYFRrROk/srTcY:3PJ/D1mblfPJ/e9zPJ/DZKnoPJ/vY
MD5:	9C5837E57DF4F1A5B1B907F468527ECA
SHA1:	346206488984B91CD40E61AD2C2C45445D7B9CD5
SHA-256:	E2019789829DF28A851421028DB4232825F8A516693E722663FAC3C2FDAF7B45
SHA-512:	7012A4AE92391E548153565CE0607B8A0FB06EB7D47A62C908A401201C512317FD8C50016DE892F1E8C480740173E7D673B39B3589AE40B151C675B8F90868A2
Malicious:	false
Preview:	0\r..m......d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..../....."#.D1.=....A.....9Q].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/plugin.js .dD..../....."#.D.......A.....9Q].8O.z....=..:.N.{....N{.A..Eo..................A..Eo......P.~.........0\r..m......d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..P>.../....."#.D..:....A.....9Q].8O.z....=..:.N.{....N{.A..Eo..................A..Eo......V.f.........0\r..m......d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .A.a.../....."#.DUm.....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):	5.28034975800425
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QPO0n6x+nTMSGVOvwj5TjYHa:h1zZ4+dsp6b0n6skwKpua
MD5:	AF164EAEBD7F80B505DD80EB8F0E7F2D
SHA1:	38FB375F342889ED3E6A4D46C0F1608CD93B0BCF
SHA-256:	FEEF0FDC49CCD71A158A874CBD51AFE81E5B467F5AEF3144BFF386423FA07B26
SHA-512:	F40032E044E1F9BBA0A46CD4BCBA133B8C82D660C58BA8398BB3D8D8000B2F7BE78DEAD52E70B717CA7C495D70B26576DAB39E63EFD64BC7D12EBE7BAA48F98C
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...t..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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Entropy (8bit):	5.209940394879627
Encrypted:	false
SSDEEP:	6:cX4q2PWXp+N2nKuAl9OmbnIFUtwxf1JZmwyxf1DkwOWXp+N2nKuAl9OmbjLJ:cX4vaHAahFUtwxf1J/yxf1D5fHAaSJ
MD5:	4F80D22D6354A376B01362747D174D99
SHA1:	FB4F886F46CCF458703D767E86AFDD524EA73798
SHA-256:	72580E317B35477B5BE46247AC6C4C2EA890272471A7A090D903655F9B8AB0A2
SHA-512:	744905F544A49FEAB0B68A0BE0CAC2CE7F8D067974F60B9D0FFB64BC37017882D1BC13C53AC6B5D4AA67EA6FAA5982CFB8A3585708C869D284D0D5D210B7B8 B
Malicious:	false
Preview:	2020/11/29-09:51:49.172 18b0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2020/11/29-09:51:49.181 18 b0 Recovering log #3.2020/11/29-09:51:49.181 18b0 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	0.010371588441083619
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDdsmWiDdsmWiDOsmWhCDOsmWhCDTsmWhCDoDsmWhCDoDsmW2:tFVFVAnAnfnovnovnovnovnovno
MD5:	7992D0F5EDC35AC96CDED773CAEFBCEE
SHA1:	BC918CF4D77D516DD25CCEB974192DFDC147FF56
SHA-256:	99E8308BCBBC6C7EA91E369C6C8686344277CA206819362EAD3D6D778381E992
SHA-512:	6FC2977B88C6445CB52FF0067F0F926E9F14EC8B601567C4A4F1D06BEBB83A0061712074CB8B4581A8E2F2ED258E9521DE6E9B6105F6AF5C7EF129D5D4F0D8F
Malicious:	false
Preview:	VLnk.....?.......Tq.>..j.. ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129175144Z-225.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 164 x -55 x 32
Category:	dropped
Size (bytes):	36134
Entropy (8bit):	2.605022107769859
Encrypted:	false
SSDEEP:	96:DU1cz3CgLqGv5RUabD7C/H4ptLVu39oFxx5xxBOxxxxxxaap1xDxxHlxlx5vx5G:DKySgmGv5D2UtxUK
MD5:	4DE5BD6C29CB5D30F6B4089047218102
SHA1:	140B447010980C1DA8F61A8335E17F9C3F68530F
SHA-256:	76BE9C9D721374BB80A5F69DB97C7CE1B4319D41066A6FBFF99EDC2B423449CD
SHA-512:	EA94DB36D89734BCECCA38FB674766AA9474CB5775774098F0F81544C1E94B24F8784FE66FD1889C74D628E97CC51737ABA59D67F1B80DDDEF1653D8787373C
Malicious:	false
Preview:	BM&.......6...(............. ....j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j.. .j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j.. .j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j.. .j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j...j

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	32768
Entropy (8bit):	3.385949173928093
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQlLOhFVCsL49IVXEBodRBkRsnlLOhAVCs749IVXEBodRBklsnu:iGedRBjedRBcedRBnedRB1
MD5:	317C9CA9D3FB67AD53B85A24D083CD02
SHA1:	985EB403A77E18277F14877E4CBC495E2039150D
SHA-256:	F9780FC0BC47F90435FA3BE5072831EE8FA199CFCE5374B02C0A73F4775B5042
SHA-512:	9BCF82E53854D815F91A0575F3BE97228BE496C62FECEA7077866807F44EB69EF676F1631FCAC63E92874F4E0BD6526FC8D29772CFC649D10B04A715D4740334
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):	3.2004788532801536
Encrypted:	false
SSDEEP:	96:b7OhFVCPB949IVXEBodRBkXlLOhFVCsLLR49IVXEBodRBkhsnlLOhAVCsVJd49Io:bViedRBBLGedRBjCedRBdyedRBe
MD5:	5A10560EC96B0B6BB575CDFF30B65085
SHA1:	AF541F9ECA5CEE53A4AA9756C961F57DCCD16BAA
SHA-256:	44DA079F2F6AF9C2811809A52B2F25CCF4992132BE887E4D776C152DEE00AC35
SHA-512:	9111282E1C46A57CF0D901D74CF709EF3AC6E9FF38F47A03182BB121608C0AA3B39F7EA769BCFBDB110C2639B4A86963D517E5F1C7DA2F2C3E568ADA547457F
Malicious:	false
Preview:	....X... h...y... ....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6128	
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 1.7
Entropy (8bit):	7.890694414073813
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf
File size:	2973843
MD5:	fb9dca5d3e122cae28166f3e3be7bc43
SHA1:	76ed2e8f2c876cd8da438f19c8fe96d4a695918e
SHA256:	c679efb245b1ce95aeaad0cae3c4809a4e84b567bc0391 6c92b20a8adf07d71d
SHA512:	304cbfb5518dfdd59ed76b78d33595170bf3c2722b819d2 aed10adf08a3f75cc53d93a6a791731c38d75b4d1393a0b 5f03ee1f976e4a29276d9da73064ac3eb7
SSDEEP:	49152:MmXFFq67APabenR+TayeSKROhUsyZTBMI3YDhtOr4eTWljrbCw7:MugGbnayeSuenFtbeClXbd7
File Content Preview:	%PDF-1.7.%......566 0 obj.<</Filter/FlateDecode/First 6/Length 42/N 1/Type/ObjStm>>stream..h.214S0P...w./.+Q0...,H../-...K-....0..@....endstream.endobj.567 0 obj.<</Filter/FlateDecode/First 726/Length 3949/N 76/Type/ObjStm>>stream..h..[ko.....2.....>.*...

File Icon

	
Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General	
Header:	%PDF-1.7
Total Entropy:	7.890694
Total Bytes:	2973843
Stream Entropy:	7.896491
Stream Bytes:	2918250
Entropy outside Streams:	5.305661
Bytes outside Streams:	55593
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	451
endobj	451
stream	286
endstream	286
xref	0
trailer	0
startxref	1
/Page	0
/Encrypt	0
/ObjStm	3
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	1
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 09:51:32.378554106 CET	60152	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:32.414469004 CET	53	60152	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:32.789777040 CET	57544	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:32.816936016 CET	53	57544	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:33.572211981 CET	55984	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:33.607700109 CET	53	55984	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:52.331490993 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:52.332309008 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:52.368882895 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:52.369008064 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:53.334486008 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:53.334541082 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:53.370198011 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:53.370342970 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:54.383661985 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:54.383711100 CET	64185	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 09:51:54.419428110 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:54.420811892 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:56.427495956 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:56.427552938 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:51:56.463298082 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 09:51:56.466358900 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:00.443085909 CET	64185	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:00.443164110 CET	65110	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:00.478635073 CET	53	65110	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:00.480374098 CET	53	64185	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:03.111624956 CET	58361	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:03.139003992 CET	53	58361	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:05.386101007 CET	63492	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:05.423276901 CET	53	63492	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:07.613625050 CET	60831	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:07.651757002 CET	53	60831	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:08.403726101 CET	60100	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:08.439522982 CET	53	60100	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:19.273931980 CET	53195	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:19.317487955 CET	53	53195	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:20.913343906 CET	50141	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:20.953903913 CET	53	50141	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:37.780005932 CET	53023	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:37.807166100 CET	53	53023	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:39.603337049 CET	49563	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:39.630650043 CET	53	49563	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:40.334784031 CET	51352	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:40.365439892 CET	53	51352	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:40.644311905 CET	59349	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:40.681176901 CET	53	59349	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:40.997549057 CET	57084	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:41.024770975 CET	53	57084	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:41.698303938 CET	58823	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:41.725492954 CET	53	58823	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:42.446191072 CET	57568	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:42.473439932 CET	53	57568	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:43.454577923 CET	50540	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:43.490271091 CET	53	50540	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:44.592813969 CET	54366	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:44.619996071 CET	53	54366	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:45.339432955 CET	53034	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:45.375102997 CET	53	53034	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:46.439960003 CET	57762	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:46.467329979 CET	53	57762	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:47.107228041 CET	55435	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:47.134398937 CET	53	55435	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:47.751384020 CET	50713	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:47.778650045 CET	53	50713	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:51.743083954 CET	56132	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:51.770374060 CET	53	56132	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:52.472045898 CET	58987	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:52.509906054 CET	53	58987	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:53.177860022 CET	56579	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:53.213617086 CET	53	56579	8.8.8.8	192.168.2.3
Nov 29, 2020 09:52:54.165978909 CET	60633	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:52:54.203738928 CET	53	60633	8.8.8.8	192.168.2.3
Nov 29, 2020 09:53:10.828963041 CET	61292	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:53:10.829500914 CET	63619	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:53:10.867938995 CET	53	63619	8.8.8.8	192.168.2.3
Nov 29, 2020 09:53:10.877278090 CET	53	61292	8.8.8.8	192.168.2.3
Nov 29, 2020 09:53:12.712122917 CET	64938	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:53:12.739357948 CET	53	64938	8.8.8.8	192.168.2.3
Nov 29, 2020 09:53:13.825695992 CET	61946	53	192.168.2.3	8.8.8.8
Nov 29, 2020 09:53:13.861166000 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 09:53:10.828963041 CET	192.168.2.3	8.8.8.8	0xf6a2	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

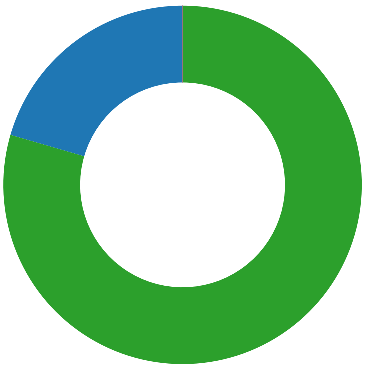
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 09:53:10.877278090 CET	8.8.8.8	192.168.2.3	0xf6a2	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- AcroRd32.exe
- AcroRd32.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe
- RdrCEF.exe

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 6116 Parent PID: 5580

General

Start time:	09:51:35
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\Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf'
Imagebase:	0x1150000
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	11865C3	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	11AAE05	CreateDirectoryW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6128	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	119EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock6116.1.3030462071.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	11D2657	CreateFileW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	119EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129175144Z-225.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	119EA85	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	12183C8	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	12183C8	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	12183C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	12183C8	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	12183C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	12183C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rmv474c_105ehxy_4q8.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	119EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	119EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R12lmuhd_105ehxz_4q8.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	119EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ramecxd_105ehy0_4q8.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	119EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ra6lzc3_105ehy1_4q8.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	119EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rdw23zs_105ehy2_4q8.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	119EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6128	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	11DD405	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	119CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	119D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	119D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	119D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	115EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	115EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	115EA55	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	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	success or wait	1	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Celebrating the Achievements of Benjam#U00edn Netanyahu - Prim.pdf	success or wait	1	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	11ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 43 65 6C 65 62 72 61 74 69 6E 67 20 74 68 65 20 41 63 68 69 65 76 65 6D 65 6E 74 73 20 6F 66 20 42 65 6E 6A 61 6D 23 55 30 30 65 64 6E 20 4E 65 74 61 6E 79 61 68 75 20 2D 20 50 72 69 6D 2E 70 64 66 00	success or wait	1	11ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 30 31 31 32 39 30 39 35 31 34 34 2D 30 38 27 30 30 27 00	success or wait	1	11ADF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	2973843	success or wait	1	11ADF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	61	success or wait	1	11ADF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	11ADF47	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	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	11ADF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	11ADF69	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	11ADF69	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	11ADF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6128 Parent PID: 6116

General

Start time:	09:51:36
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\Celebrating the Achievements of Benjam#U00edn Net anyahu - Prim.pdf'
Imagebase:	0x1150000
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: 3492 Parent PID: 6116

General

Start time:	09:51:43
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' --bac kgroundcolor=16514043
Imagebase:	0x870000
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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	9659E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	13	9783E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	102	978447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	162	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	7	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	9659E2	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	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2180	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	7	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	86	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	56	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	239	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	287	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	9659E2	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	266	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	49	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	196	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	31	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	6	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	170	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	8	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	16	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	9659E2	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	309	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	149	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	32	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	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	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	5	9659E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	9659E2	ReadFile
unknown	unknown	4096	success or wait	55	9659E2	ReadFile
unknown	unknown	4096	end of file	1	9659E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	9783E5	ReadFile

Analysis Process: RdrCEF.exe PID: 5524 Parent PID: 3492

General

Start time:	09:51:45
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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15540169491933176135 --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=15540169491933176135 --renderer-client-id=2 --mojo-platform-channel-handle=1660 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
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: 6152 Parent PID: 3492

General

Start time:	09:51:47
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=1684,2245332663126947271,2796270942385178651,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5895458359813356849 --mojo-platform-channel-handle=1736 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x870000
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: 6196 Parent PID: 3492

General

Start time:	09:51:49
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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2668593196950910738 --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=2668593196950910738 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6352 Parent PID: 3492

General

Start time:	09:51:53
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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5586481229821336722 --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=5586481229821336722 --renderer-client-id=5 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6444 Parent PID: 3492

General

Start time:	09:51:54
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=1684,2245332663126947271,2796270942385178651,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13996197876522443299 --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=13996197876522443299 --renderer-client-id=6 --mojo-platform-channel-handle=2144 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis