ID: 358593
Sample Name: Official Winning Notification.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 22:01:47
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

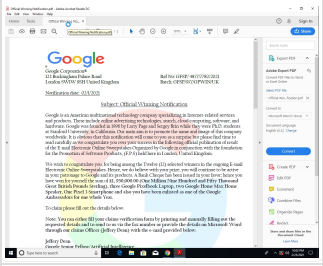
Analysis Report Official Winning Notification.pdf

Overview

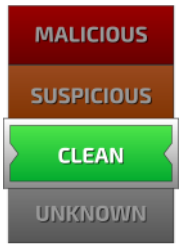
General Information

Sample Name:	Official Winning Notification.pdf
Analysis ID:	358593
MD5:	3653519eb05f612.
SHA1:	a7519a45b1a03c..
SHA256:	fb016c07a07157f..
Infos:	

Most interesting Screenshot:



Detection



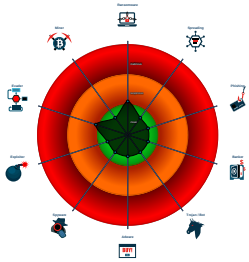
Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Contains functionality to access load…

IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 7100 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Official Winning Notification.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 1740 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Official Winning Notification.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5824 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6832 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=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13763115675501202353 --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=13763115675501202353 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6872 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1696,2716905115287683301,2737728514390977682,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=11125268993836637515 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6604 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=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6719864216122095185 --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=6719864216122095185 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4420 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=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6939263152797598052 --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=6939263152797598052 --renderer-client-id=5 --mojo-platform-channel-handle=2128 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

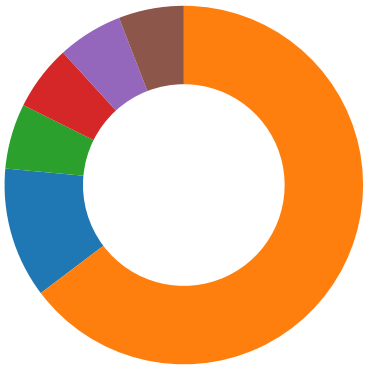
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

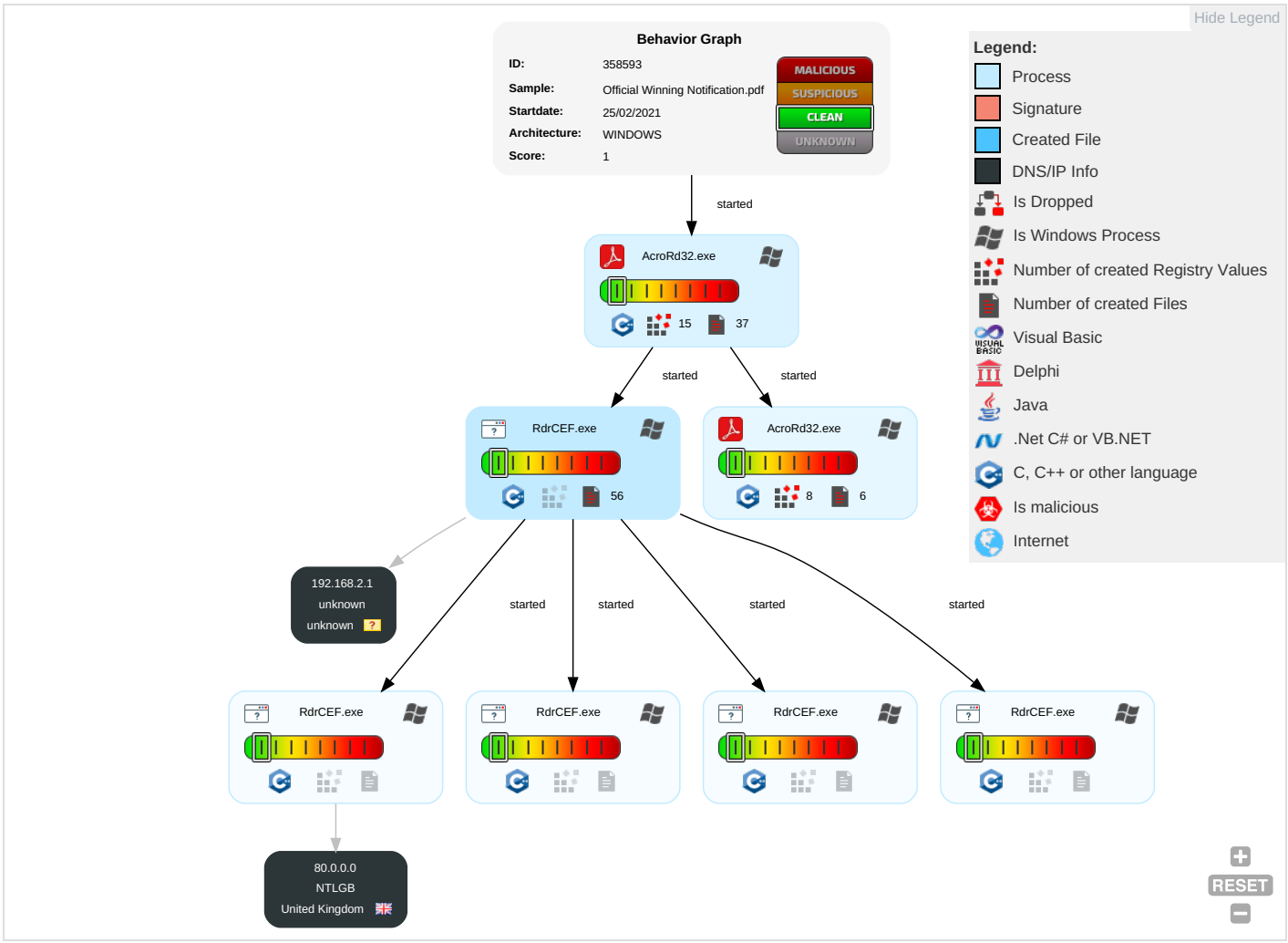
Click to jump to signature section

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

Mitre Att&ck Matrix

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

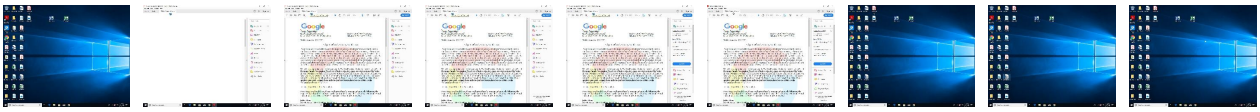
Behavior Graph

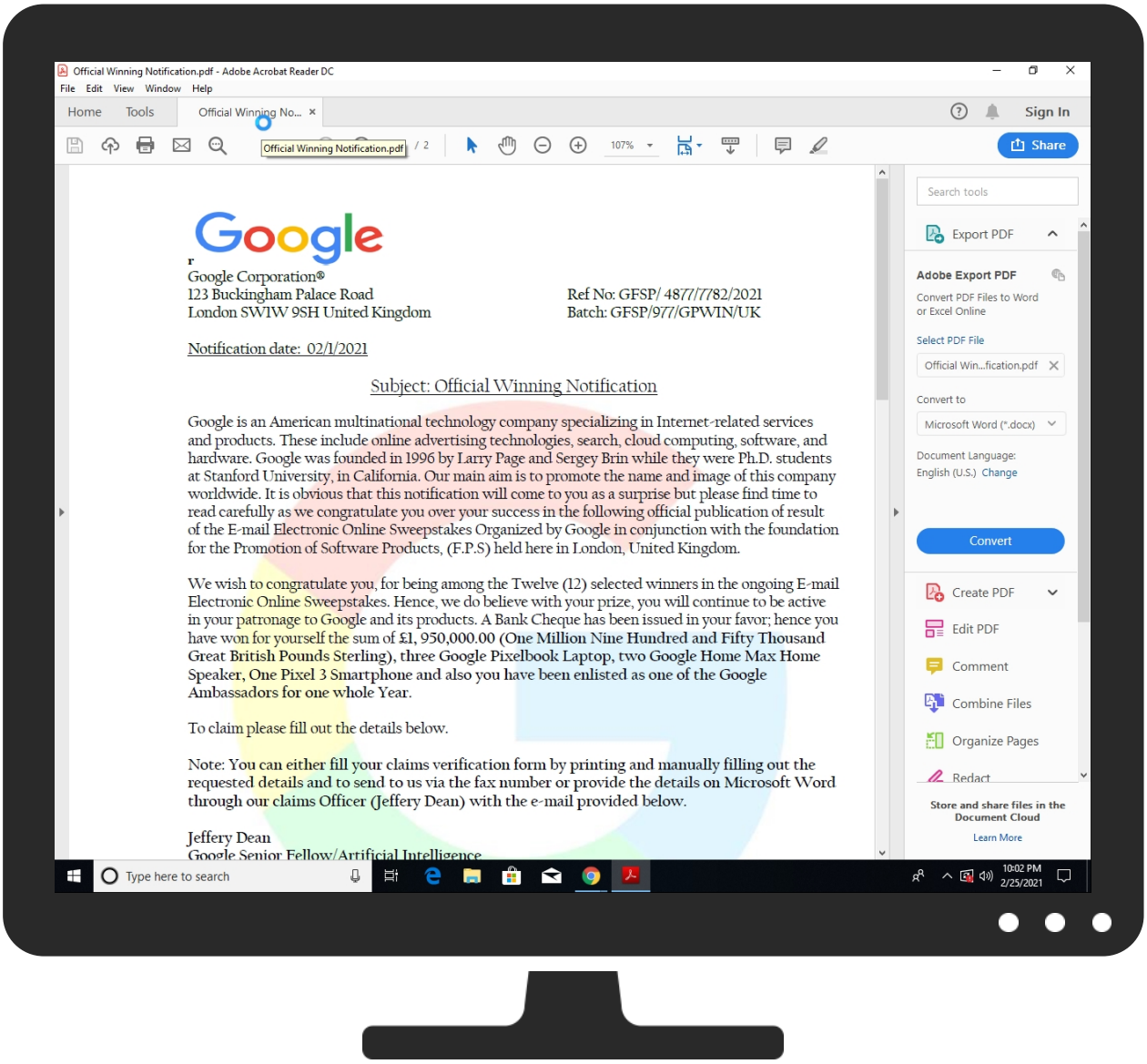


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Official Winning Notification.pdf	0%	Virustotal		Browse
Official Winning Notification.pdf	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/6z	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.fontbureau.comhttp://www.fontbureau.com/designersNormaaliNorm	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/E	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/%	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/8	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/8	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync//.	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/z	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

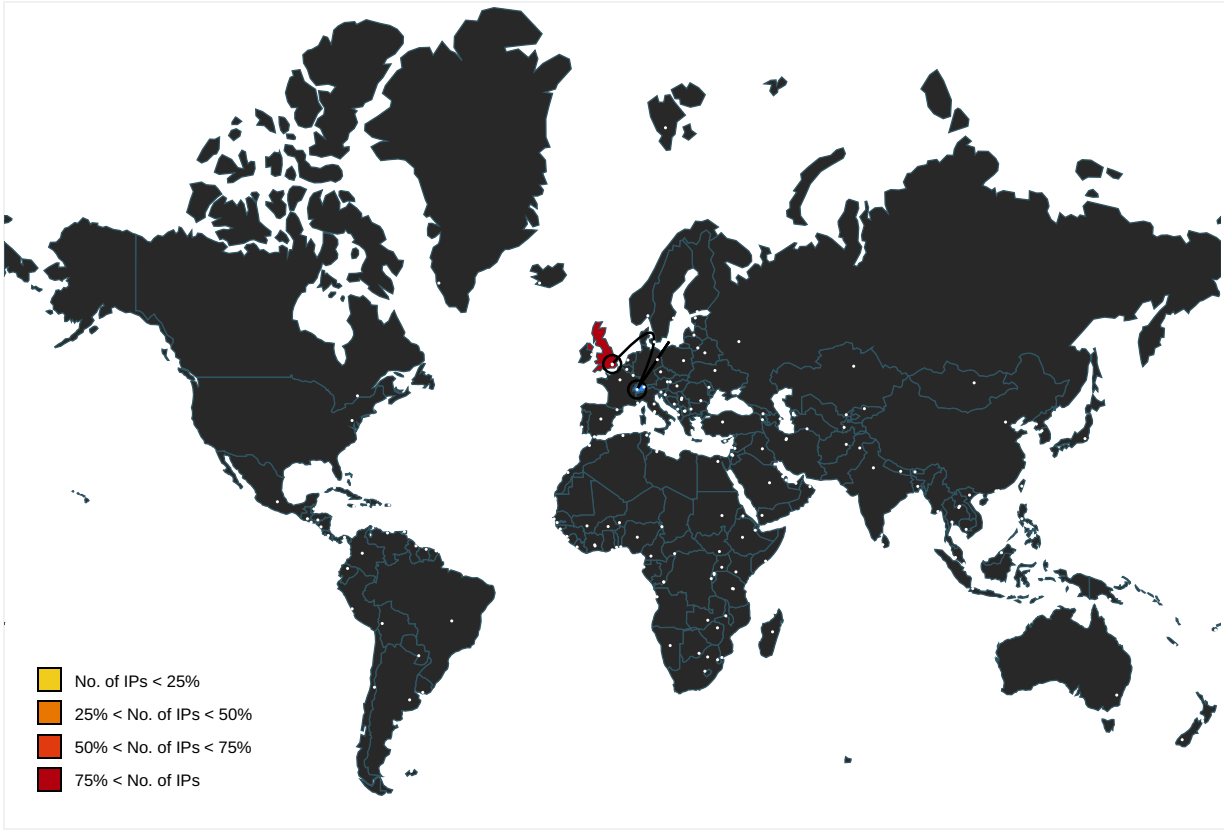
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/6z	AcroRd32.exe, 00000003.00000002.826279918.000000000B704000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/property#u	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000003.00000002.813762738.0000000007FA0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comhttp://www.fontbureau.com/designersNormaaliNorm	AcroRd32.exe, 00000003.00000003.810767977.000000000B8EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000003.00000002.813762738.0000000007FA0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000003.00000002.813762738.0000000007FA0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/type#u	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false		high
http://www.npes.org/pdfx/ns/id/E	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cipa.jp/exif/1.0/%	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfe/ns/id/?	AcroRd32.exe, 00000003.00000002.823948430.000000000AA80000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/8	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/8	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000003.00000002.818578961.0000000009753000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/schema#(	AcroRd32.exe, 00000003.0000000 2.818578961.0000000009753000.0 0000004.00000001.sdmp	false		high
http:// https://upload.wikimedia.org/wikipedia/commons/thumb/2/2f/Google_2015_logo.svg/2000px-Google_2015_lo	AcroRd32.exe, 00000003.0000000 3.811143314.000000000BB1F000.0 0000004.00000001.sdmp	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000003.0000000 2.828029853.000000000D420000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000003.0000000 2.826279918.000000000B704000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000003.0000000 2.823948430.000000000AA80000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000003.0000000 2.818578961.0000000009753000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000003.0000000 2.813762738.0000000007FA0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000003.0000000 2.813762738.0000000007FA0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comRL	AcroRd32.exe, 00000003.0000000 2.828029853.000000000D420000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000003.0000000 2.813762738.0000000007FA0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000003.0000000 2.818578961.0000000009753000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000003.0000000 2.827572000.000000000D313000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000003.0000000 2.813762738.0000000007FA0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	AcroRd32.exe, 00000003.0000000 2.826279918.000000000B704000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000003.0000000 2.818444864.0000000009670000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync//.	AcroRd32.exe, 00000003.0000000 2.827572000.000000000D313000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersCalifornian	AcroRd32.exe, 00000003.0000000 2.826239517.000000000B6DA000.0 0000004.00000001.sdmp	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000003.0000000 2.813762738.0000000007FA0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://ci4.googleusercontent.com/proxy/WCeJ4rENmPZcAQey2hEeQlAVe9VA6nj4D7cjyL8rZDV91xnMngYsueY4QXU3	AcroRd32.exe, 00000003.0000000 2.826729348.000000000B8FE000.0 0000004.00000001.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/z	AcroRd32.exe, 00000003.0000000 2.826279918.000000000B704000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/8	AcroRd32.exe, 00000003.0000000 2.818578961.0000000009753000.0 0000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/id/t	AcroRd32.exe, 00000003.0000000 2.823948430.000000000AA80000.0 0000004.00000001.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 Emerald
Analysis ID:	358593
Start date:	25.02.2021
Start time:	22:01:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Official Winning Notification.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@13/46@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 204.79.197.200, 13.107.21.200, 13.88.21.125, 23.54.113.53, 40.88.32.150, 104.43.193.48, 52.255.188.83, 23.54.113.182, 23.32.238.123, 23.32.238.129, 51.104.144.132, 205.185.216.42, 205.185.216.10, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:02:41	API Interceptor	10x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
80.0.0.0	vUp5vjYOoL.exe	Get hash	malicious	Browse	
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSljf0v9YP9XHTo1mHg1DdlnrlGltn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	vUp5vjYOoL.exe	Get hash	malicious	Browse	• 80.0.0.0
	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	• 80.0.0.0
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 80.0.0.0
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 82.12.157.95
	wEcncyxrEe	Get hash	malicious	Browse	• 213.48.143.199
	Swift.pdf.jar	Get hash	malicious	Browse	• 80.0.0.0
	0001.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495.jar	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 80.0.0.0
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	2EB0.tmp.exe	Get hash	malicious	Browse	• 80.0.0.0
	muddydoc.exe	Get hash	malicious	Browse	• 80.0.0.0
	RQMofd68Ad.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 80.0.0.0

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.657062052067343
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Q6S6bmi7Z+P41TK6tOlMen9YOFLvEWdM9QgC1bpm/i7Z+P41T6:vDRM9giZiEolhDRM9onZiEQ
MD5:	B3398944F2DBDBB3E8BCB6DF7E59D290
SHA1:	A9C6931641993D10FB3F094060BA99EEBDD2A1E0
SHA-256:	FFAC5925E7B671B4C0DA4731CDB26D867A428EB2B95DA47D1208094CCB4D3EA7
SHA-512:	5535B32A48D987040CA875F5C4F7F45DF30492E44B5A97EDD0D1A4007FB985BDA9D99B6B9E56F14726530F0E09F1B38E88AA2E2F76702EDD92094797487AB2A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..?%.../....."#.D..c....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....F.w.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..lJ.../....."#.D... ...A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....T.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.5942871639177705
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkXWtF8Be7Ywcr1TK6tbi9NqEYOFLvEkZFGjF8Be7Ywcr1TK6tm:V9zmtF9PQY9zXGjF9PQ
MD5:	28A2A46991BBEE244096E976D8421384
SHA1:	F5EA7A74A04672D1D44759D2F82266207AC084D5
SHA-256:	2F2DBAA4FDC41807B6AE6676F69CE80861E7C1B59AD29B8E736D4A5D698912C7
SHA-512:	4E824E93533B82C1BBBC53C6A8836C3B0256931F9D271FC7F702A5FFE7DD9EE75B1BEC0BCD74603FB3A088ACE00ED517A9813D3111C214AB3F27B54326D3EAA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .}Q..../....."#.D:;.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....d.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..w8.../....."#.D.....A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....a.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.575962191388063
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFc6hlUo6jsdbyeRVFAFjVFAFplUo6jE:tB4v4FSBsdlB4v4pSBE
MD5:	4253869511C40B48FEBB9FC759637668
SHA1:	7737FD82BBC3B9A293B97BD8965ABA5B3C7695FC
SHA-256:	A968129E3E3666C20A0C033D3AE16D8BCD365D64FA0260FA3B40D986B06AAD2D
SHA-512:	931763C5492622D4A917F229C84A18AF66B6EE0F7A64264D257D20B206DF0E27738CC408F9D108D912F5D5C5A107A72D773134EEBEDA346F9FF43F1FDD355967
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ..<%.../....."#.D3.c....A..hvDO.N.t@...n.*..... ....A..Eo.....A..Eo....."t.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...H.../....."#.D.o. ...A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.642912678449115
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rs02iWulHyA1TK6tB3:IbRkiD/WussX3
MD5:	E1940EC35E4627CD3EFFED002AE3689A
SHA1:	36847EB13C15499EE8B8733C7ECA202727906501
SHA-256:	7C253678B09D101DC4CFAA1BEAF3D12B6C7A0146EA151EBC2425B17EE8A29393
SHA-512:	B7925A218686D755B54C6B90DD602207715EBF8300DE4C0CD88C1DC29AEC7CCAC774C65F7C29CD4BB1FFD4DE0E09E74C8F5674CCB98B0A1D0AA19547B3025 2F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .K.*.../....."#.Do.u....A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo....._.L.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.521071286389481
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuJCPVyh9PT41TK6tc:pyixRuvCPV41TEa
MD5:	C88437C843BA51A7498B5DF20EFB56E8
SHA1:	19F7917BCFC9AB4093AC5BACB750F102E79D3D51
SHA-256:	070ED2872DD7712E7D295D64BC7B882B34295668F5CAFC2AFCE902337A51DC50
SHA-512:	2A46D5199D410EEE379B07DF6CBDBECEA5201FEE15C0BE14C0846908032BF63F3732A5365970E1767991A1CDF9FE0DF73DD436E5D0B5C0F428DF56E7478FFE/ 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .].I.../....."#.D>.. ...Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....1.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.603129386164243
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVNjgWJ6Nco2sZI8xeGvP5m1TK5ku:mvYOFLvEWdhwjQ46NLZIl6P41TK6t
MD5:	D824426679BE97B472124BE227151108
SHA1:	C577E5F606C6D2A2B651524FF6779E965C127ACF
SHA-256:	0531ABD2332A9786CFAC036CBD6E6810FE5C566CEA67A78565EB45F99F240411
SHA-512:	3D39EE780836F2B8B3DA66292D8F23D4A9053388BDB54E7139DCACFC9E0A028BA3FC96A74785E5E304AF257E55EEAA480B4AF9892EA729361D619A4C0C14347 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .m.F.../....."#.D.....A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.562047830482464
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVznJl7ocyxMtv9EWm1TK5ktWX:mJYOFLvEWdGQRQOdQ4386g1TK6t
MD5:	B2DF46382CC42FBCDF8BE240DAB06E58
SHA1:	FD44E0741A349E42D6D4E8F818DD7923660C1B39
SHA-256:	4B0D956A7148B6515A2CE6DEDC03F4AE15C616993F9D1109C17A4A1926497555

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
SHA-512:	30570556DAC9F894B930A9CC47BF3CC503804A2E5AA37C15122E9076BEF478D4DCE48A27CCC084D8B1E1084CE66B7D1300FC98B6E02A140329F4452E5F51F01
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .{9J.../....."#.DV). ...A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.600377203176676
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLl6KA0KtUMuR/41TK6tn2OYOFLvECMLrhtwIMuR/41TK6t:Z5MB6KA0iUMuR/EH5MPbMuR/E
MD5:	B4350547E85036A7882F3B5695660E47
SHA1:	4B3E419A79EECB0DDD8AE7D9CC027683057E5F0D
SHA-256:	9923CA1F4D39357E14336D2E22602085237426C13AB866F802A01490B7ACB8AC
SHA-512:	741DC8EAE8ECB4364587F2AEE169FCC99CE345FC6F026FB4F8C3D8F1B7A4680684D0F6AB06AE1E07B40037AE666504A64F4DC9482C1486CF13CE5244921FE71
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..v..../....."#.D.Q.....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 ...8.../....."#.D#.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.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):	214
Entropy (8bit):	5.545314354711959
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuUAAMby0zBUKSAA1TK6ty9//:pRxAfbeoF/
MD5:	DA620FB1698BCEAAD26909637F017B45
SHA1:	BE5861C84A88EFC5B94C98F5E6547D3C550DD4CD
SHA-256:	E40B6F2F05C05FD7C187B4347C0D1A8891CC66B9F83CC9F101A5F5F8764F563C
SHA-512:	696B1F073C9EA13413CF2273BF8DDFE8A14797F66711D9E1223DB831FF43B3126A6B7A7EC7409217285612C3C8A679579ABCC9537DBFDDFED48C9B0803F874F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...J.../....."#.D.T. ...AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A. .Eo.....C..#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.563255864108861
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFvV+iMcvtUdyP41TK6tued4HXXYOFLvEjMSWFvn6KaZcvtUd:KkXxKMSCvV+iMcvtUloCkXxKMSCvha+I
MD5:	6E5F7F80DFEC293E4C38C8978085DA4D
SHA1:	587A429D83F4A7352F08DF7318A5B085BA444906
SHA-256:	17C58BA5E526955CE202699544E69AC1BF3B1E17AB9628D88573AC78476D4A19
SHA-512:	AE2760DE39A4AE4B9A703C573CDF6002B9AFDD2B61167056A15CAE696ABB413B9F0E569C525A20503BD250A24E6A1A93E20FC1128075BC505CE84521A9CAE5 5
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..s..../....."#.D.J.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....7q.....0\r..m.....1.....5... ._keyhttps://rna-resource.acrobat.com/plugins.js ..z8.../....."#.Dx.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....C_./.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.574009474426953

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLDpIqyM+VY1TK6tZXekl9YOFLvEWsfOLEpGQyM+VY1TK6t:5h6OLDMkvxh6OLEpG5k
MD5:	8D5263C8FFC610424A767F8B77A01A9E
SHA1:	AFCF0D36BA4C82DBF87CAC45421E9226D287CCD7
SHA-256:	E0FD6F9A11E20A935A2080DA37EB2DD240BF26FE177F131FEA4C20F56BC73E33
SHA-512:	40A49EDBA0F10B4A9FBB944F518273392637CB0F5935E15E37FC303ECAE7F020550E1E00A2D50C0639A5804547AB2D18D773A0FE3D142659F3A383C469F80CA4
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..k..../....."#.D..L....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....u.....0\r..m.....;... I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...B.../....."#.DZ.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....R.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.651346801055482
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFhfrwSeKaTLnkSRVFAFjVFAFJx991wSeKaTLnWS:UB4v4JwzXLnkSB4v4Jr91wzXLnD
MD5:	CB59243A12B3A73B0D255BBADD860453
SHA1:	A78353994EBF0BB68AC53749036F0485FE6B41EF
SHA-256:	CE071EED6F331DBDC2868A0818A0BAA34365F23ACDB1AD82F1E45712FE6B9FA0
SHA-512:	5BDE9695E5ECF6B413C02C93CC7000FE44F2F9B56926783185EB9B9FB6C0125534E188FC6D3A835B1B9079801923EAFC6FD17CE608210DB409E0B8C78DF9AA4
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..i....A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....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 .&.I.../....."#.D.. ...A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....f.K.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.478781377606746
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuC66yR11TK6ty9/l:BsR2Ese1fyPQt
MD5:	D4CC20680177E7C0FE0A782F9ED88C84
SHA1:	751300C9BDC8B48304633F299F58D317F5FA2490
SHA-256:	AC4AB425C5A516CED53026AF9655BABDD1FA7C76F068181F75B84433CE9530E1
SHA-512:	377F7FAECA5AFD58C12960983EA707B17D1F2E7474F450F36DDD411205F4E4F5CDC075CA7B8FA97F38E4E3DD803C6844B583305534145792D373099EDDA054B
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .A#l.../....."#.Db.. ...A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.653530766355002
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQVL4B7OhKlvA1TK6t:RbR16y4BJk
MD5:	F4BDD9D7603854E53345EB9D4C045632
SHA1:	3FDA8543B609E551FE27ADC392DD0365C18E8FDB
SHA-256:	E246B507E3A18EAF42BB95F1499B7AB6BCC93AEBD5833F0A58A239CC28D45D9A
SHA-512:	420DB647A6C454A6D260A29F00A069470FF4D862058454B7E2AFDABA91E5556BA62BB8241F5B13C40AEC8F249E853C3399A2635296E9157D90F102034D79C3E9
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...F.../....."#.Dl?.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... az@.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Size (bytes):	211
Entropy (8bit):	5.558552303606603
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuaqSQdFt1TK6txQ:B2geRHRQ0S0/Q
MD5:	9F9F9DA2C6C8FDAD97AC10A430654952
SHA1:	6363F410191351EFDBE0DA831C8CCA7FAB5F37DA
SHA-256:	C21E26B568956E165C80E209CB0FF89C61102C20046E1B75B02576B196EFA062
SHA-512:	E3C48EB63C8962B8E69290564C78F49737A51DCD8BEB25001F4E666ACAD4D580BF15C1BD8896CB5F20523D8F345EC6D202124A1D6B3356D5624A2F4442A26CF
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .v I.../....."#.D... ...A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....3.w.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.627339545766115
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQNYyfFyt1S/1TK6txnzyEYOFLvEWdrIOQDkAt1S/1TK6tWt:WyeRle7Fyt1wnzyeRlsrt1w
MD5:	08560CA0D8B9D99B2EA13372270E0D64
SHA1:	CB3E70ADEF2C7130A3DB024A2B8C22E4507EC458
SHA-256:	03B993218EC8E68E1A5E889FB84C31A5101CEBA749219120C5F1CF69925A1D77
SHA-512:	B2356D142B69773B3D129C73F817DE4798AEDAE65F042609FE00D52AED411C11F307D02F263113947CA2034F448F59F548000DE4FC40F497CFF55F624C31C7B8
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .E."..../....."#.D..V....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..O.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...C.../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....8G.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.5690234630556645
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFv6nr8LhpkNJNqww6U+5m1TK5kt//:mnYOFLvEWdhwyu/LMNrqwK+41TK6t//
MD5:	C27577A531484BC15330071AD1173AC6
SHA1:	23CEF8A1A4AFE1A00DACDC94E2E317E36A55693B
SHA-256:	A2BC136F6EFF9042AC3AED47C9507AF1122B7CF1C2EF4EC53715671524DC8A6A
SHA-512:	377EB093D3CFC2AA5CC60D70D3522EF8C3FA3AEF0349DDD9923D19F6F1EF655A6584CEEFBE53FA80DFC2E74DE267B185D4AD377B78A83CB7D87EC7F15DA08 B54
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...E.../....."#.D.....A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....&.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.614973124999022
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbufghfO441TK6tR+s/EYXYOFLvEWdrROk/RJbueGqfO44A:/RrROk/rfLEHRrROk/trfLEVm
MD5:	A39F2DA6116C15AA458DA2A64A37E5C5
SHA1:	7252D3D7A30F909A5183CC0CE3F69B69935A3CF6
SHA-256:	A700D6CBF2DD89C5F53762E6B83EB32296623BEC17E639795E674C4A3C96715B
SHA-512:	183DDCA7EFDBD67A9630FC440DDE5A32B701B5B920909F8360A740E7613AC3B2F1AE251259432526E657528384B1FDAE2A95F25473F94E89791683BC8D2688D8
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...!.../....."#.D..V....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....Y.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .].C.../....."#.D.i.....A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....Nr.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.598707733685904
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIACmhrbS1QPLr1TK6tQkMmDEYOFLvEWXI83IrbS1QPLr1TK6tX:xqTSm92CPLnpjqTLIr2CPLn
MD5:	0B7A15799CFAC568C563314DE2FDF0FB
SHA1:	D313DC90028450A5F8480E73859F125BE34877B8
SHA-256:	9AE05D6284E3561297E7F7AF8B64F7C294EC7326F109F5A719BD36908C8C62A7
SHA-512:	2F5CA9542EB1B4E0B042658AF34D605F8ADA3162FFC33C4083F999A27405911C87CF4CE8DBE0DC68F6581C5D99EF9E59E125DC605DA11226E637A123052D122
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..\..../....."#.D..L....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....R.....0\r..m.....:....f..... _keyhttps://rna-resource.acrobat.com/static/js/config.js ...B.../....."#.Dc.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.646718584033609
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuFsEJ41TK6t0+52YOFLvEWdMAuzhzDl2wlsEJ41TK6t:zRM7sDSbRMxlDlXIsD
MD5:	72A7E5096FC00A3B5C27FED4B55E3C8F
SHA1:	43A7631E6E3F19DBA16F50456B506967B2FBE6D8
SHA-256:	848D63A18CB57E7E98F4EF4361720D6C91CA97113DCDF353F5F7A5081D18F762
SHA-512:	082558AB59768805B41FC6AF6EA9719D6655F9AB197167E9720A028456B9155A03BCBCBEDFDF2F5136E774AC612614D2D00DCF7F3670D9298AA1DCD62F8176D
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..$.../....."#.D..b....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.... ..W.z.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .<MI.../....."#.D7.. ...A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....~.H.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.59989734861437
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuBGTFong1TK6txf2YilPYOFLvEWd8CAdAuIn7Fong1TK6u:6lJRbFoMffqlJRVn7FoMC
MD5:	2216A8436736BF5FA143A662B7EF33DD
SHA1:	99D29E9022F4748C49A1C5D3F6296B99E2680DBC
SHA-256:	E379570F00FB69045A2ADD93BD5189B5FC33FFA0F394B68465289EC554F93DF4
SHA-512:	BBCCDB5962E920AFCD4F1C2E3802E12F040D05D0C8DF63EA7798CAA32B0F47D8A5B3CA64BF87A04731EA983E511A8689523482683ECF0D225088133048F186B
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...$.../....."#.D..b....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..E o.....F{;.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..OI.../....."#.D".. ...Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.... .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.643382795976206
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuCmQfKJAPOe16wG1TK6tuY8nYOFLvEWdrROk/IuccAPOec:F8hRrROk/YGJA2e2j8hRrROk/CcA2e2
MD5:	E415E3F5DD82067375A4A5E013B9CB65
SHA1:	E9ADDEE641029F0DDCE3B8DEA2B946264A95AA44
SHA-256:	60F123A8CC8D3AE161BE883AFBA2355F3E7D04C731676EC260ED46ACE811495C
SHA-512:	1D44542AA078CB6332708D7CACC2BD31D5086F31EB9099376FBF22986F5C9BECA149C799CF7242531C475E125A13BE341EB33A330F10F32BB9FBD808550B5A4
Malicious:	false

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.698488422086994
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQwP9irNJIi1TK6tULrnYOFLvEWdrIoJUQNsFrNJIi1TK6tf:ehRcvPYrNJICGhRcJrNJIC1
MD5:	B0BC0457D2248CA6DB92DAD3397E2636
SHA1:	1BFD1D3AA0C4B0AAEC42C0159B63A044C092A6A3
SHA-256:	33667DB883BD5FC8F523F4E4DC867B03626D90CC02050B6B6719633B4B001884
SHA-512:	72578CCE1EF131B7F39C3BE81A3F74952B0DAD0579B30F71E87656D2DC8508AADA9FF8C1942D8E53F1AA27E5D4E6DF4F70E57DC7A75A73DB599BAF313FA3FF01
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .(5".../....."#.D..W....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....(.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .+.C.../....."#.D.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....,.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.611966147914558
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuui2ZLzgm2d/1TK6tmeOEYOFLvEWdrIhuuQzS2ZLzgm2d/1TKm:0REiiRejR3GiRe/
MD5:	4E1F8D001556F3496D0AA4EEF6D139F9
SHA1:	E67C6B7126C75334E11EC85FF5CDA8DA804F902C
SHA-256:	3EEEE192114B606018594D86AD69A9C30DB4F802A092EE3F542E86AA2089F5CB
SHA-512:	02F3E6F89CFD87F97A97204C0A79CAAD6FF66AA2CAEAC58F4BFCB15E4F936A938323312CC50303BA16DBA9E02096F6E985FC0507F18C632CB6C5859DA44D0DC
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...!.../....."#.D.V....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....I2.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .P.C.../....."#.DX.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....9#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.674499839776606
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1K4kys2kx56uvp1TK6taeAElVYOFLvEW1KA5ys2kx56uvp1TK6ta:6JJKfhJJKog
MD5:	8B19C9CC94123D44CA58D188A5734F1C
SHA1:	42070EF36F6BFE49C2EAB45DD5592EE0CB39A536
SHA-256:	41590A5935159FA3EFB374D000BAF04A2FDC95440F7A33CCFD4A91BF3E2915F7
SHA-512:	F6D33E3707FFA329AE726883AB40794ED3C7009BA41AD0C6F3383F5C8700D766063EFCBB5FFF5FBA852B2BCC02DA7D106D713790FAF0862A271B22BE3CE7564B
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...../....."#.DU.$....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....+.q.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...:.../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.635070437998171
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
SSDEEP:	6:mWYOFLvEWdBJvvuLchKehUDLYtmOZn1TK6tO:xRBJIcErDcFZL4
MD5:	843AA501F489D35F44FF1908D4BA6BC5
SHA1:	D5EA6D05D56FCB4BBCC88C6343F21F9188AEA8F4
SHA-256:	EC39D7BE899884C873EE94C0D842C863A9ED216843AC66008EA4C99DC14E697B
SHA-512:	7F0B96A072FCF7FC53C56A52857EEFFDDE8553D4275D6EE68A5459D7983C02D943D13EEFA31D615AFD4E7C6642C856C90C7BBF28194C2F15E26575138568ABE
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...I.../....."#.D... ...A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....h].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.638447046018663
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7ryaVPu1TK6t7+sRPYOFLvEWIa7zp70fyaVPu1TK6tLj:BPH4acfPHVach
MD5:	FF64215D316D35F841D3BB35AC65EB3B
SHA1:	DDF72A99E539D70D6CF8B5D88CEC79EF07444DBE
SHA-256:	C9E88EFD5F2FED33110377416ED8812838F33B50C61B1C985986073D3F242A54
SHA-512:	0E24B7DD04CCFB81087C68BA8BAC48B973794030603203B5E48E82DD279BFEFC70B19F1767E6BDC897921FB40F0DB3A6DABA3FFB28E58D395DA2492E42B524 8
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..y.../....."#.D9.....A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...8.../....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.596436272538276
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVVSiF4XVAZ+8cV3vRm1TK5kt0l:mKPYOFLvEWdENU9Q2wiM3Y1TK6tc
MD5:	6DE3799CA1EC198EE6437D299AB64C78
SHA1:	31E19FCE1877AC5868B6B37CE2554E93CDDFA66F
SHA-256:	D7BD6863ACA03D39230EDAC6C89997E26FA86C80C4FA1A201A5646E4BC324F81
SHA-512:	D66F3D72A378C581FE93C2D687C00DA927F4EDA2CFE0636EFA6E6089328A3032421634C20CAD6DDB888DE1F3DEEEAE40893A8A3FACA9B7D77168E111EE3A2/ 47
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...F.../....."#.D.p.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.604655051117828
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQYQjBRCh/41TK6tR/:XRc96Di/E3/
MD5:	5B0A514227FC6D5FE8B3DBC62C7A1054
SHA1:	E9B1B0CA9C77FF2D05F8CB9A74BD6C922A21A734
SHA-256:	DD93F009AD05E333A72DBE828EC4687CAFB5CB18E9F9B60CFBADA8D7D9E0BD6B
SHA-512:	F7F302D1C98E308F241D34816381EE5D4236041C6F1CF12E2D15DEE2C97C7EDD638085875D01DFD4059510F74CFAC1C52D99F74E255CCC3F15194C26C431CBI
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..3J.../....."#.D.?. ...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo. .....r.W.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Size (bytes):	231
Entropy (8bit):	5.585461595442176
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuZtVULlF4r1TK6ta9tl:bs6xRkiR2LlF4nY9
MD5:	B389183393C6CD13CB0847E6B6AF025E
SHA1:	645DBA60888635BF54CFB20B92817B649FAECF97
SHA-256:	A6DAF8188C8DDC0545A208C5722CE44C7F9E5D21B6DDD5D465BC486607E1C423
SHA-512:	99A264681BACA408D050B8A4D94CECCE0D21D6CA375BEE7520824094F624188BD5D37B48E60898AE8369D942F042EFFC0AC8DAEB75AB934EEBD5D9ED7EB6A6C8
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..."../....."#.D;.X....A.P...#4..l....5...5..).w.. .h.~..A..Eo. .....A..Eo.....j_.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.483981595981914
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvI6vg/K/lFrV/Ccu1isLK5m1TK5+:mhYOFLvEWd/aFufdN941TK6tL
MD5:	C305F75822E0DAAD5D65C0004AA5E83D
SHA1:	E54A902524FD3A8F60705F23ED2AFFEB902DEF37
SHA-256:	F3166F2EE846DCC1D6B2AB1121D7E101FC1B2E7EBB04433842582FDD76007A2F
SHA-512:	03A15B2D35921DB72ED78070F867C3AA3D0CDA485ECB6A92052332A45CA8D650DB25DE931B5178E67F919362A99816AE70ECF37B339D57647CC6ADE651F42DAD
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .-.J.../....."#.D-.. ...A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....A.=.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.527398008465665
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ3oBMqVd3G4K41TK6tF:2DRuRhB9Vd2kn
MD5:	F2195BFBC3CCA0E6A8D826B7D8C29020
SHA1:	0FDDF241972E7F143DE5123C67BB43FD4F9E58D5
SHA-256:	F8E2DF46DB7770150C517378FAB74002B7DB06DCBF13644C40B16CE08BF05AB8
SHA-512:	6E8FF1290FD959AA7EDE00EAA6D2483DE3CD89CCD818C29F3E243695737B0868656B25546B789A2CCA3993FD1008BFE9689B8D34BF564A15380B3B3ECC32E69A
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...J.../....."#.D.7. ...A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. ....ov.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.64668376134707
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QtWyyOuA424r1TK6tCkqYOFLvEWd8CAd9QUNOuA424r1TK6t:+RQt5BrnoRQtBrn
MD5:	E6C53625564C40F9360BA05F7A6CAF27
SHA1:	9D964C6E20E869F05CAA1991896F046FCB62213A
SHA-256:	749DFD462EF5E5F7CD4DB48E4C3901DC4FDE303279CF2A631ED101DEDC980FF2
SHA-512:	D551A27AE789914211E64D49023E4804FA10C38DB17C2D762FCD031E0C5B89BE33B49765CFE577F7613E349F6B16B3D6280D69C36C787BDE4EE63E616C8D470
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .ZB%.../....."#.D.f....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 ...J.../....."#.D... ...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....=-&.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.567215520233991
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvBKggCtNbg2iHio/Mm1TK5kts:moXXYOFLvEWdENUAurKgZbyC8n1TK6t
MD5:	FED5130F96DFDA69A847A02F8809233B
SHA1:	F992485D4A98633089F60D4AD7854A9FFC23C2D9
SHA-256:	0B1F82534FE2C5F878A18C1958C4FB187AC3DFA0F1EF2EBC0080B5309A59A391
SHA-512:	79F65F67AF5CDF9D4F94FEEF106F541EF2995E208C6FD8551D82DD7B418A95D2C08AA14B534589AA723D9630BAB69DB1BD1C3E059267E779AFCC63A8A6D107F
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .$.E.../....."#.D.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....G.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.633573309749434
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQTyKsLmB41TK6t1tMQZYOFLvEWdrROk/VQdeKsLmB41TK6t:nRrROk/VFKNmLfRrROk/VseKNm
MD5:	7E8687C9A3B98663B2E805F86B665C2E
SHA1:	C389A323E35C309F4E1B1C930CFA8DA0400A6CA4
SHA-256:	8AB5DEDAAA1FBB4D308E2E89895C97CB027343B48C5D7742DC9A440CD5A328DA
SHA-512:	4A73C5919495FB0D0B61D15F31B42E5A9BCA88CF46FD708A1DE26AD61E519BA328D9FB849BF253D93F62CF0451CCEDE8B9FE298471B37609A40C6CFE617965E
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..<"...../....."#.D..X....A ./.ev.....N~..6.b.....$.j.:C...A..Eo.....A..Eo.....}PN'.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .d.C.../....."#.D@.....A ./.ev.....N~..6.b.....$.j.:C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.559111075890443
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuutnNfAdm9741TK6t:qxRcQnNfAdu7E
MD5:	0705542EA6670A5C4638D32CF638A988
SHA1:	9DDBA383F609C271242B2B1B8B5879725992D1AF
SHA-256:	A5082A8EB57653D503514094A8DCB4C6B35E81BC21F73C764D2CC15C8DB528D6
SHA-512:	FEC0CFD16DCD0C948964E618A0995008E912C084A270BAD83DDE50F234F9B10B061E775128F90429A608AECB51F891D4B7DDAA7B5012A4C47E6917C4F750D44
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...H.../....."#.D".. ...A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....U.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.585532088229944
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvMJDm/wA9xp6shoq+Nem1TK5ktRel:mMOYOFLvEWdwAPVu+DmIYiJn1TK6tM
MD5:	8BDAAE1029CF299121777EDB5323AE40
SHA1:	7FFD1301DF23D270263CCEF65685112B11B5F2AA
SHA-256:	6817427C2634DE602F2261E57666A9A1AC7C6BBA781E54B174AC8640738BE982
SHA-512:	0D6B9EA7B56BDD6DFE16EFC3C4C3AC58E6CAC8B291C9E69222F821ECC23635102266BE312F38BECF73F4C88D42A17C898DD0C10C0E2B39F1AD9E048C4C3B5B7F
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 .).E.../....."#.D.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ..+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.641613555516609
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQe3GSzhcsBXIh1TK6tP:mxRBJQt3GSDB0
MD5:	67D5B3C7BAA4A63B8FAE9A60CA9105FD
SHA1:	C076826BBE3F0BE0C18EA96288FCBE44BED360F4
SHA-256:	92676D7F3F21BFB2BA1FEBB9D3BDC6ADE3F36F3DAF6C4BB1DA3434E7568FC1CC
SHA-512:	468B72570664E6051558FA5CEBE0792E50388108144FCB0C2177A85EACBDC10ECC47CDD120EFC64A26FD4107E1BFF7DF209C3031DF43FB2542F655CED21B73E 2
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .w;J.../....."#.D.z. ...A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....M.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.594906653540444
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQJR9kDc3Me/1TK6t49XMsPYOFLvEWdrROk/RJUQM60c3x:3RrROk/swoc+VRrROk/sdFct
MD5:	54962196A20C68B88450D7AB3BE6E2DE
SHA1:	09523137432DC3889B21D44EE17CFB251279CF07
SHA-256:	A2BC59D24D0DF5893A05E62E6B59D7F315605E93EA7513A1C5AEA8BED42A20C6
SHA-512:	C6F037BDE77C0B78B765035C72F0287A55E74537D05F368DAB83D5D8D16FBE3BC54F4CC0073DB748D70FA280F895552BCB13A5A2EF60DC0F8C3AB5513002A9
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..r".../....."#.D.fX....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 ...D.../....."#.D.....A..... 9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....d'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.08314588261182
Encrypted:	false
SSDEEP:	24:B1jmvTzHEgM+8DixWAzYeVmi1mZstvtrwXupSqvxgL:zmvnEgRzs8i1T
MD5:	68BB77A1BF75F86B055787264B8ADCC7
SHA1:	5499C994008C85269C41F663D9FE590FBDEB6231
SHA-256:	000E324722D20C4C26F01EA51E98F1275E0C1ED4EC616EA05DAE4B9CFA5702E4
SHA-512:	7CF8D1F244601659EF103894D72F0515606EF832CDC68FCFD9E8D005D33E8303228423498E895041AE5E878DBE5E693782E608671910E050DE078CCEE4111815
Malicious:	false
Preview:	.....6..oy retne....).....T.....3.....<.../.....v...q....<.../.....C..M.....k.....#...(...k.....]...I.@...../.....@...../.....6<|...../.....<...W..J.../..... ..oB*..,../.....a.....,../.....;.y~A...<.../.....P....V..<.../.....F..=z;...<.../.....o...<.../.....*....<.../.....2q.....<.../.....Gy.'.h...<.../.....k7A...<.../.....: ..N.A....<.../.....;/....<.../.....<.../.....P[. q..<.../.....,+..._.#..<.../.....J..j.....<.../.....o..k...`K.../.....^.~..z..`K.../.....[.i..%..`K.../.....@..x..`K.../.....*)....J: .`K.../.....A?.2:...`K.../.....&.S.....`K.../.....q..`K.../.....u\]..q.`K.../.....!...0.o.`K.../.....*.....`K.../.....+.{..'.`K.../.....MV3...`K.../.....=....m...`K.../..... D.4..`K.../.....+.U.!..V.`K.../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.142635644367693
Encrypted:	false
SSDEEP:	6:mNdoMPQL+q2Pwkn2nKuAl9OmbnIFUtpedoM0G1ZmwPedoMaSQLVkwOwkn2nKuAlz:s/PVvYfHAahFUtpc/0G1/Pc/tl5JfHAR

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
MD5:	C141120D565C64BE1735AC49DE6C0AB3
SHA1:	1E1A312CDEBBF173068CB9E39CF68AF2CFAE30FE
SHA-256:	0BEBB1FF739A9FA7D9BA0D50A22251E201C38F4A82725E2178BC4FC7AB9B4224
SHA-512:	C9DBD9D7BC68AC86ADBC43AD74B1E17E809695064919C41833F7E72FBB17592082DF00F6DF154D142FA36E90B9F1C283E9833A2E71EC0AFBFD498109C1613D5
Malicious:	false
Preview:	2021/02/25-22:02:53.306 16c8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/25-22:02:53.312 16c8 Recovering log #3.2021/02/25-22:02:53.313 16c8 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.008050090959268128
Encrypted:	false
SSDEEP:	12:I+mmTsx+mmTsxlNTpyxHHyTpyxHHyTpyxHHyTpy:TmbsmbPXytHwytHwytHwy
MD5:	03B3B4BB0F979E273B32ECC52C9B0E01
SHA1:	D307CEFF6AC7E7D3E424C1A855C56168596AEF69
SHA-256:	299FDCED8539A4D45595DBB33856A5A4045215BFECDD3EB7206996390C48C643
SHA-512:	4927E9663FD9AB3DB4449C765F0A55D33DFB51029B3F129E8FD1625C0C5F5593F52E59F180A5A0D1FE49D13C16D84EF3875FAB580375CADB6C5A4CF7439EDA1
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210225210242Z-279.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	2.834315990641938
Encrypted:	false
SSDEEP:	768:Q2NSqddBRR1fZ1/6HHQz/9cBuWnCoLO2aa0AgmSB9+ErtwA7hsXFcZ:qgfZ1/6HHQjaPCoLOa4
MD5:	5BB99AA3CCCA274B9B013BF11699F8C6
SHA1:	90FCBA0DAD9186BA80A88D30F4B106D539957782
SHA-256:	0A0DE95326878718F8B21A3B95B263D13A7F32FB0B064E3C379EAD8287EDFA57
SHA-512:	E92099A241F8007CFB180CEEABDEEE7A7A5D3D10B8FD950132CB23E1DBC0FB1985E2BE25F5C44555D2B96AB7753C1BF3CA37BA0529E4205426F6E331A6CEB7F1
Malicious:	false
Preview:	BM.....6...(...u...h.... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4471834910856085
Encrypted:	false
SSDEEP:	96:k49lVXEBodRBkWCgOOh1CKKN49lVXEBodRBkWCg3POh1CKK949lVXEBodRBkWCgx:HedRBTedRB6edRBdedRBa
MD5:	23A4C93BD38D4A3200A10FC3C0803C22
SHA1:	53D70865609B19B39C2AC1EEF58A7706A35E1DA2
SHA-256:	E208A54004884263B53C39526124C29E836C2A3ADA017E180FEE6F7AA2180954
SHA-512:	CCD35A67876E8925CB5E8C091B72AC646AE7477F5A29E717125BF1355C3D616F4820FB024B9B1E70B6FD717F41B6CF6E8099BE229FB59BBB04A887126FCC5242
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
File Type:	data
Category:	modified
Size (bytes):	34928
Entropy (8bit):	3.3118364003939083
Encrypted:	false
SSDEEP:	96:fCgOOhZCPj949lVXEBodRBkqCgOOh1CKKKt49lVXEBodRBkzCg3POh1CKKod49lJ:uiedRBXSedRBzCedRB7yedRBSs
MD5:	09DEE2C0EBEC3B79F5C304D43C525FDB
SHA1:	8FE7EA23C6EC75D104DB4C7C2642DCB8774438FD
SHA-256:	FCC9EDEDF3578C1A4BE3640E248FFFCCA5657F497B20A1AF53ECA053F4F7906A
SHA-512:	060D06D5372C34BED33C587E5E57603D92DE6A2587A9CC74FE2A20543A52918163E58FE592984677D8559BF6C58A738F0D8C46FD19AC411CDCE7E0A90939F45
Malicious:	false
Preview:	.....Mr..... .....W....X.W .L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZjNt/rK8Qedx5NjDdE4+RDHuNYyu:J0GpiyVFihjNtDK8QIE4gDHMK
MD5:	FC3F157E9303BEE51E821A0B3069AAB9
SHA1:	C199F788C6A931BDC22E4975B1865B7DEBE31C7C
SHA-256:	ECD2E4D5D245D7F31B487506FD89BFB6EBDFD6883D34283A7C4ADE132A56E5FF
SHA-512:	C65F1AB088BA499F89DFE55A03D1B42BE11BE88A230DF9AC47445BD0793BF8FA978059DF1DC6D5CDF88F1F0CE46E2613AB1B50835FD7A76FD1B995F11EECCE 45
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.880769101080503
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Official Winning Notification.pdf
File size:	170599
MD5:	3653519eb05f61261b207e18f6f601bc
SHA1:	a7519a45b1a03c8a215a7c674e6b9da29d101258
SHA256:	fb016c07a07157f5142d2d9043405a57ed20b700e981e62 7993c25bda3a7f29f
SHA512:	83f51d54045f1a30407d15a0051c16824180aa19ad9943 2c4c041d02fbc6b12b2f79dd7446f6482f5e24f2047c3a73 8a258bfb7a909a6b852f8f8453146092b
SSDEEP:	3072:wHjikLQeCnnJn+dn3SnBkLQeRDT4ZXNR1IxYflE 8kRSUuvBOqsPQRoogakVSE:wHWMZmF+FSBMZRD 0INRm+E8kRgOqyl5/
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/ Lang(en-US) /StructTreeRoot 39 0 R/MarkInfo<</Marke d true>>/Metadata 131 0 R/ViewerPreferences 132 0 R >>..endobj..2 0 obj..<</Type/Pages/Count 2/Kids[3 0 R 27 0 R] >>..endobj..3 0 obj..<</Type/Page/Pa

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.880769
Total Bytes:	170599
Stream Entropy:	7.916386
Stream Bytes:	157887
Entropy outside Streams:	5.125573
Bytes outside Streams:	12712
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	55
endobj	55
stream	22
endstream	22
xref	2
trailer	2
startxref	2
/Page	2
/Encrypt	0
/ObjStm	1
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-22:02:54.030638	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:23.664422989 CET	53	65298	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:23.674280882 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:24.641752005 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:24.695194960 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:25.344346046 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:25.396380901 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:26.032032013 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:26.083062887 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:26.803152084 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:26.851845026 CET	53	53097	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:27.810815096 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:27.859807014 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:28.958487988 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:29.010201931 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:30.095297098 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:30.147074938 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:31.699485064 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:31.751653910 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:32.635889053 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:32.684662104 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:33.996156931 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:34.049319029 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:35.399241924 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:35.448291063 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:36.244119883 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:36.295717001 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:37.074841976 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:37.123358965 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:37.983422995 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:38.051429987 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:40.148794889 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:40.197463989 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:40.994075060 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:41.050947905 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:43.628490925 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:43.677493095 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:49.303414106 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:49.305427074 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:49.358099937 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:49.365708113 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:49.842349052 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:49.894088984 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:50.329478025 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:50.329531908 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:50.388112068 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:50.391488075 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:51.376187086 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:51.376261950 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:51.435715914 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:51.439488888 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:52.170486927 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:52.224694014 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:53.421044111 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:53.421092987 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:53.474565983 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:53.480160952 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:53.970343113 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:54.030504942 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:57.430309057 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:57.437062025 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:57.437114000 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:02:57.481828928 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:57.485754013 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 22:02:57.497246027 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:18.896866083 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:18.956072092 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:23.591521978 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:23.671525002 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:24.324191093 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:24.382937908 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:24.945622921 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:24.995794058 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:25.459985971 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:25.539179087 CET	53	49285	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:03:25.805119038 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:25.880992889 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:25.961034060 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:26.010102987 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:26.575431108 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:26.658967972 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:27.203182936 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:27.260799885 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:28.076802969 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:28.136774063 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:29.217950106 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:29.266968012 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:29.730870008 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:29.780277014 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 22:03:39.011672020 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:03:39.067054987 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 22:04:05.354461908 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:04:05.402940035 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 22:04:07.404717922 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 22:04:07.470834017 CET	53	59794	8.8.8.8	192.168.2.4

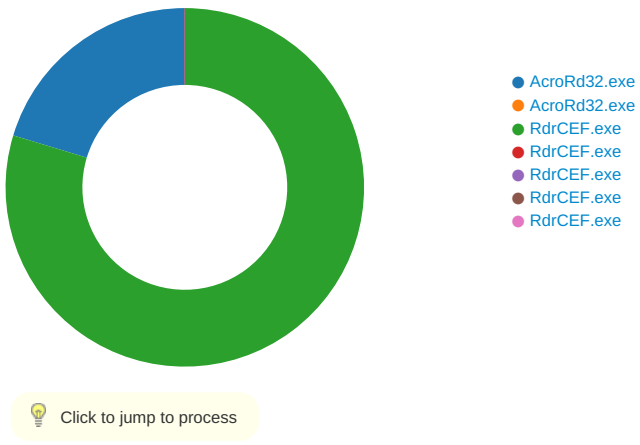
ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 25, 2021 22:02:54.030637980 CET	192.168.2.4	8.8.8.8	d078	(Port unreachable)	Destination Unreachable

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 7100 Parent PID: 5860

General

Start time:	22:02:31
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Official Winning Notification.pdf'
Imagebase:	0xc00000
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	C365C3	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	C5AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	C4EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210225210242Z-279.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	C4EA85	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	CC83C8	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	CC83C8	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	CC83C8	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	CC83C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	CC83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	CC83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rci97ug_zoz13j_1cc.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	C4EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	C4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rzn57z8_zoz13k_1cc.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	C4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1r2qrcn_zoz13l_1cc.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	C4EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1658qel_zoz13m_1cc.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	C4EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1j76qd7_zoz13n_1cc.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	C4EA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	C4CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	C4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	C4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	C4D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	C0EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	C0EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	C0EA55	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	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Official Winning Notification.pdf	success or wait	1	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Official Winning Notification.pdf	success or wait	1	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	C5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 4F 66 66 69 63 69 61 6C 20 57 69 6E 6E 69 6E 67 20 4E 6F 74 69 66 69 63 61 74 69 6F 6E 2E 70 64 66 00	success or wait	1	C5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 35 32 32 30 32 34 31 2B 30 31 27 30 30 27 00	success or wait	1	C5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	170599	success or wait	1	C5DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	2	success or wait	1	C5DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	C5DF47	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	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	C5DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	C5DF69	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	C5DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	C5DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 1740 Parent PID: 7100

General

Start time:	22:02:32
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Official Winning Notification.pdf'
Imagebase:	0xc00000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 5824 Parent PID: 7100

General

Start time:	22:02:40
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0xaf0000
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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	2	BE59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	1	BF83E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	38	BF8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	109	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	12	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1085	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	29	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	5	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	2	BE59E2	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	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	BE59E2	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	2	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	1	BE59E2	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	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	12	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	12	BE59E2	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	2	BE59E2	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	26	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	26	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	28	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	BE59E2	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	10	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	10	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	144	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	BE59E2	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	134	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	BE59E2	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	97	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	BE59E2	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	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	3	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	BE59E2	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	84	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	1	BE59E2	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	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	BE59E2	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	8	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	BE59E2	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	162	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	1	BE59E2	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	74	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	BE59E2	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	4	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	16	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	5	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	2	BE59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	1	BE59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	BF83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6832 Parent PID: 5824

General

Start time:	22:02:43
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13763115675501202353 --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=13763115675501202353 --renderer-client-id=2 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
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: 6872 Parent PID: 5824

General

Start time:	22:02:45
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1696,2716905115287683301,2737728514390977682,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=11125268993836637515 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xaf0000
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: 6604 Parent PID: 5824

General

Start time:	22:02:49
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6719864216122095185 --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=6719864216122095185 --renderer-client-id=4 --mojo-platform-channel-handle=1852 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
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: 4420 Parent PID: 5824

General

Start time:	22:02:51
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1696,2716905115287683301,2737728514390977682,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6939263152797598052 --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=6939263152797598052 --renderer-client-id=5 --mojo-platform-channel-handle=2128 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xaf0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis