ID: 338565
Sample Name: NORNIK COVID-19 NAMES.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 15:39:51
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

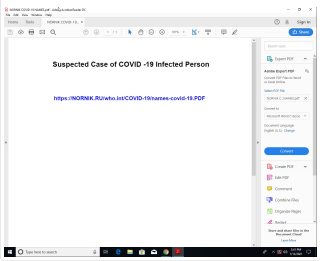
Analysis Report NORNIK COVID-19 NAMES.pdf

Overview

General Information

Sample Name:	NORNIK COVID-19 NAMES.pdf
Analysis ID:	338565
MD5:	9de37675ac573d..
SHA1:	3777f82c37f773e..
SHA256:	39325b29e92176..

Most interesting Screenshot:



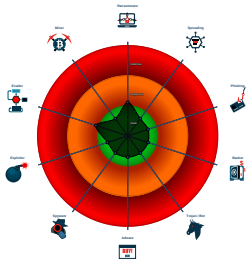
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Machine Learning detection for samp…
- Contains functionality to access load…
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 5872 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\NORNIK COVID-19 NAMES.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 1752 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\NORNIK COVID-19 NAMES.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6312 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6476 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=1636,5812136359608500254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1710734962896665663 --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=1710734962896665663 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6500 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1636,5812136359608500254,13138570058860233451,131072 --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=KAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAAOAAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=22617888244197332 70 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6540 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=1636,5812136359608500254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9399729911713544515 --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=9399729911713544515 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6956 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=1636,5812136359608500254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13560670023211164477 --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=13560670023211164477 --renderer-client-id=5 --mojo-platform-channel-handle=1792 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

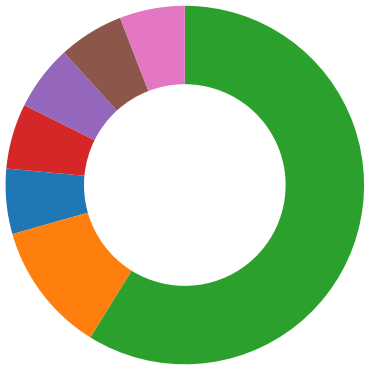
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

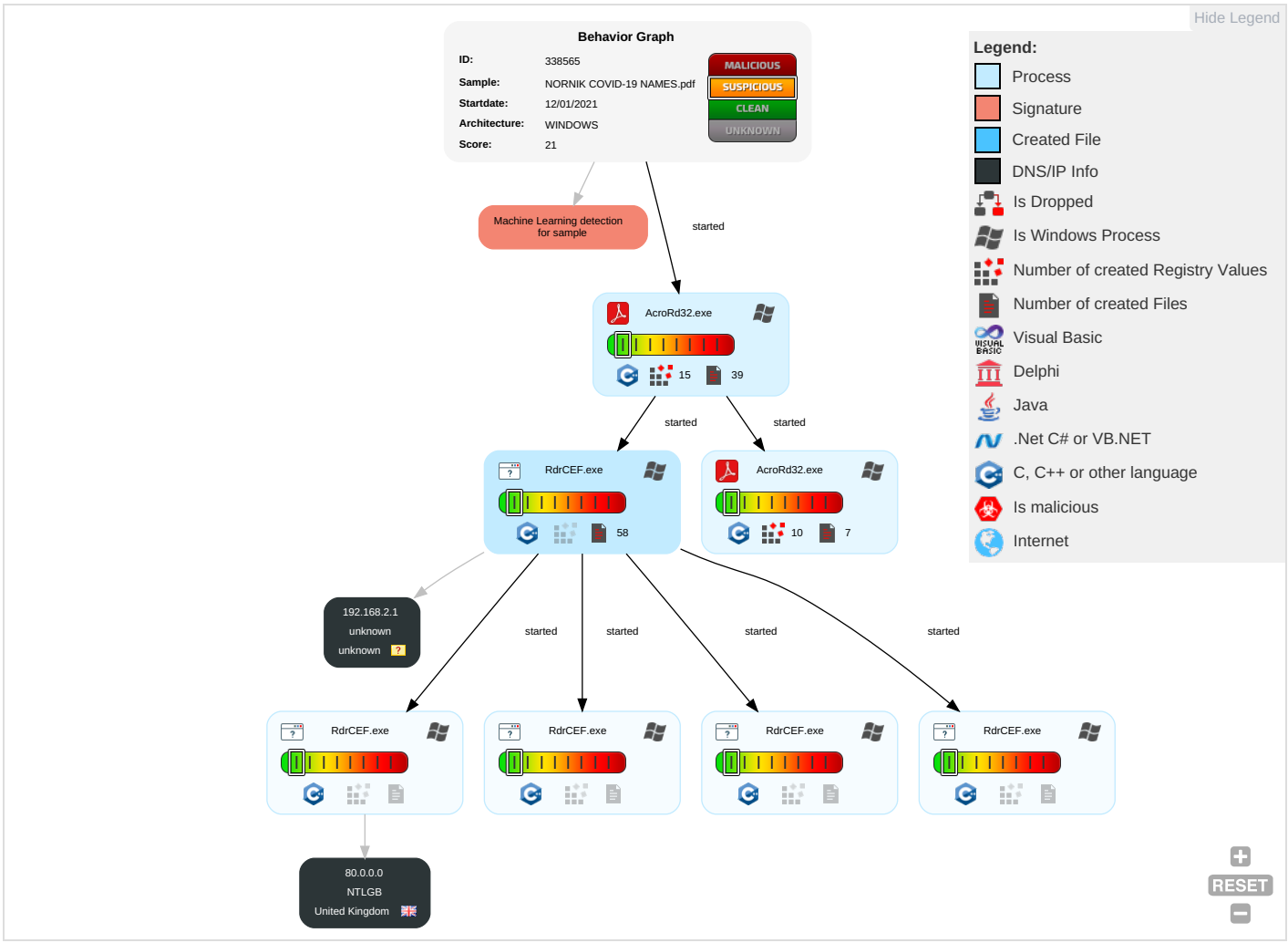
AV Detection:

Machine Learning detection for sample

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
Spearphishing Link 1	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 Devi Without Authorizati
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 Authorizati
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

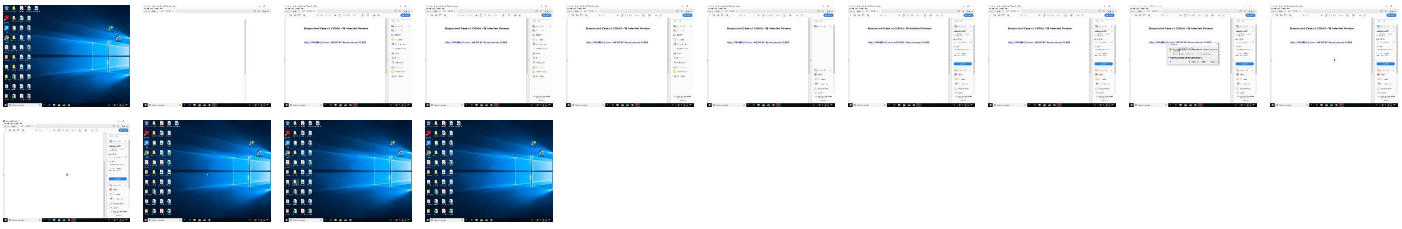
Behavior Graph

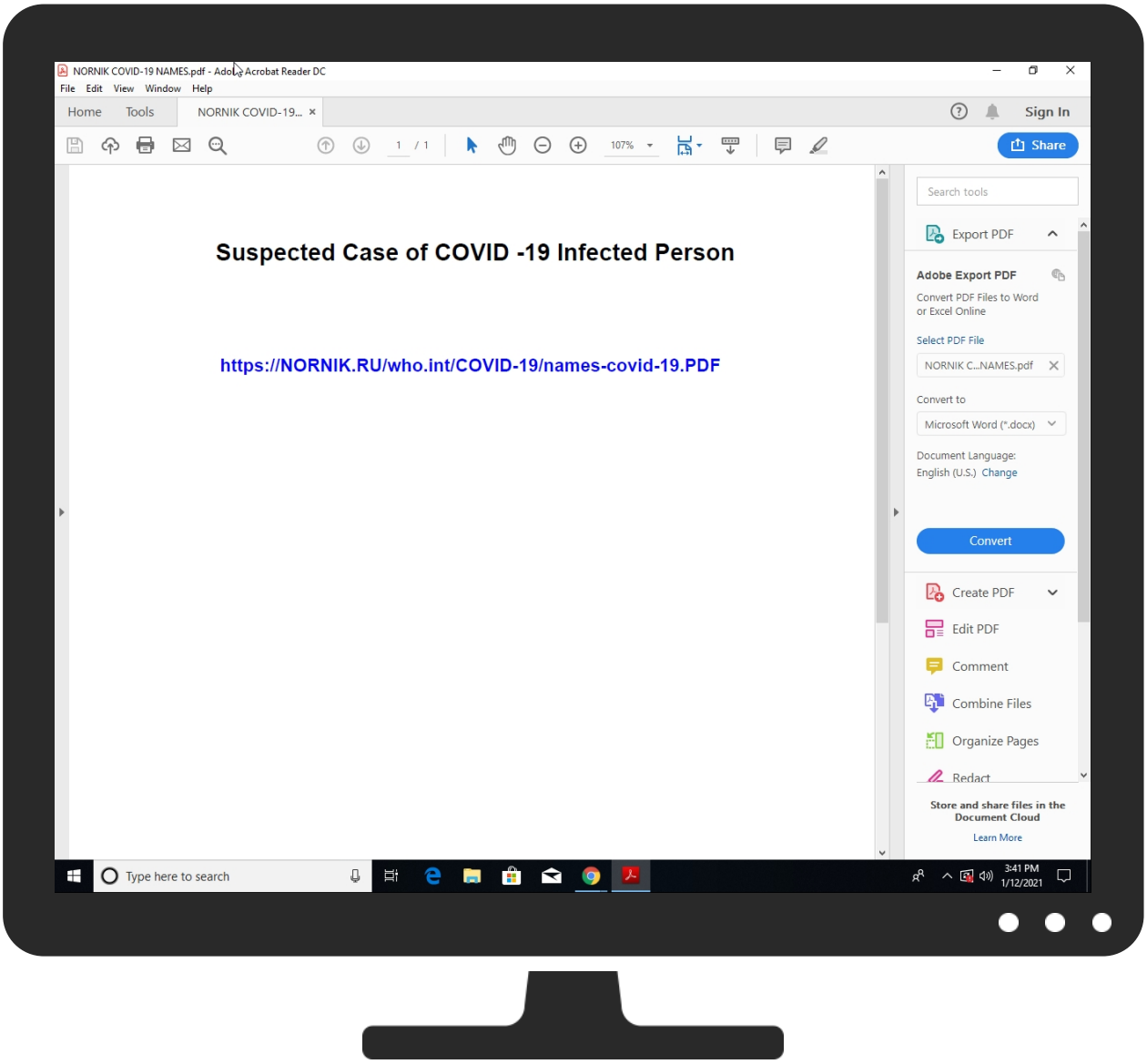


Screenshots

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
NORNIK COVID-19 NAMES.pdf	2%	ReversingLabs		
NORNIK COVID-19 NAMES.pdf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Z	0%	Avira URL Cloud	safe	
http://https://www.radpdf.com)/Creator(PDFescape	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/O	0%	Avira URL Cloud	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://www.dynaforms.com	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/.3/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/.3/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/.3/	0%	URL Reputation	safe	
http://https://api.echosign.comM	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/D	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/n	0%	Avira URL Cloud	safe	
http://https://www.pdfescape.com)/CreationDate(D:20210111111106Z)/ModDate(D:20210111112937Z)	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/1.0/e	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://https://www.radpdf.com	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

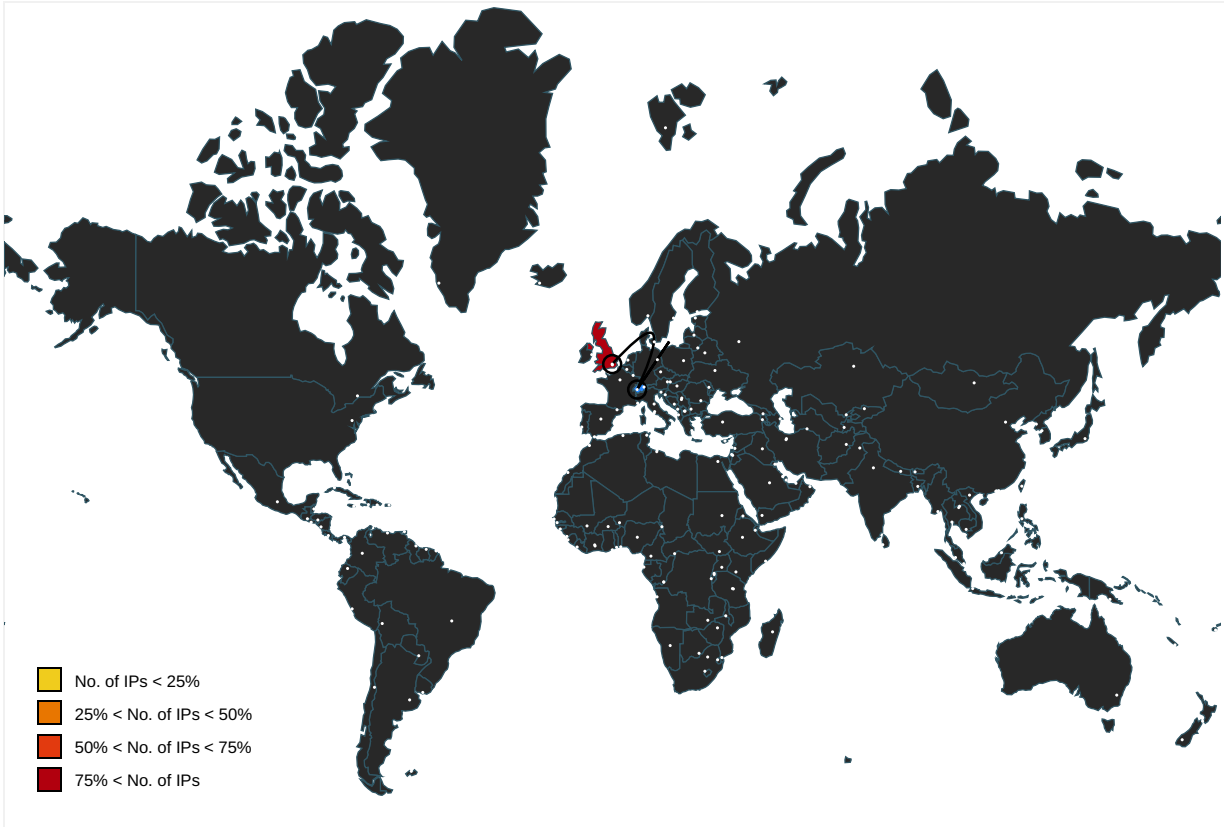
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pdfescape.com	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.413182050.000000000AE60000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false		high
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF_	AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDFkm	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF)	AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF:2ate	AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp	false		high
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDFcb	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Z	AcroRd32.exe, 00000001.00000002.413924308.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.radpdf.com)/Creator(PDFescape	AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false	• Avira URL Cloud: safe	low
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF7	AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/O	AcroRd32.exe, 00000001.00000002.413924308.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.dynaforms.com	AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF:	AcroRd32.exe, 00000001.00000002.413880541.000000000B101000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	AcroRd32.exe, 00000001.00000002.414019815.000000000B1B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/.3/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.echosign.comM	AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/D	AcroRd32.exe, 00000001.00000002.413924308.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/n	AcroRd32.exe, 00000001.00000002.414019815.000000000B1B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.pdfescape.com)/CreationDate(D:20210111111106Z)/ModDate(D:20210111112937Z)	AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false	• Avira URL Cloud: safe	low
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp	false		high
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDFF	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000002.414019815.000000000B1B2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://www.osmf.org/drm/default	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cipa.jp/exif/1.0/1.0/e	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/extension/2	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.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, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000002.413924308.000000000B132000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000002.414588980.000000000B442000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000002.403394594.0000000008EC0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://NORNIK.RU/who.int/COVID-19/names-covid-19.PDF	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.414413398.000000000B349000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.413794027.000000000B0CB000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.414490484.000000000B3BA000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.413924308.000000000B132000.00000004.00000001.sdmp	false		high
http://https://www.radpdf.com	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000003.396701314.000000000A2CE000.00000004.00000001.sdmp, NORNIK COVID-19 NAMES.pdf	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000001.00000002.399852276.00000000077F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/5	AcroRd32.exe, 00000001.00000002.414178292.000000000B274000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338565
Start date:	12.01.2021
Start time:	15:39:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NORNIK COVID-19 NAMES.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:	27
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:	SUS
Classification:	sus21.winPDF@13/47@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 • Security Warning found • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 92.122.146.26, 2.20.142.203, 2.20.143.130, 104.79.90.110, 52.147.198.201, 51.104.139.180, 51.103.5.186, 93.184.221.240, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, acroipm2.adobe.com, arc.msn.com, wu.azureedge.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/338565/sample/NORNIK COVID-19 NAMES.pdf

Simulations

Behavior and APIs

Time	Type	Description
15:40:51	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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	
	http://https://bouthilletteparizeau-my.sharepoint.com/:b:/g/personal/jproulx_bpa_ca/EYQbKRRM1_VEjGeslLjc5GwB075qH34FcIdpShYIw3DxFA?e=4%3abltg7p&at=9	Get hash	malicious	Browse	
	ds7002.lnk	Get hash	malicious	Browse	
	http://https://townemortgage-my.sharepoint.com/:b:/p/cislami/ETa8xXdrX-FKtlaSfOphTioBLICbx4muhejuoDN0jK0wqw?e=4%3aBnR24e&at=9	Get hash	malicious	Browse	
	iwqOx.pdf	Get hash	malicious	Browse	
	http://https://jcpconsulting-my.sharepoint.com/:b:/g/personal/maireads_jcpconsulting_co_uk/ERfHfSCzdwpCiQXDqtKNHKkBnVvlszs3rd1CSU_-rQLUlg?e=0TY6UC	Get hash	malicious	Browse	
	purchase.pdf.exe	Get hash	malicious	Browse	
	fOlUD.pdf	Get hash	malicious	Browse	
	aPJ75.pdf	Get hash	malicious	Browse	
	http://search.hdirectionsandmap.com	Get hash	malicious	Browse	
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHlfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHlfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	
	nyEdi.pdf	Get hash	malicious	Browse	
	CHoyU.pdf	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NTLGB	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
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 80.0.0.0
	utox.exe	Get hash	malicious	Browse	• 82.27.253.120
	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	• 80.0.0.0
	NormhjTcQb.exe	Get hash	malicious	Browse	• 82.1.160.234
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	• 80.0.0.0
	http://https://bouthilletteparizeau-my.sharepoint.com/:b:/g/personal/jproulx_bpa_ca/EYQbKRRM1_VEjGeslLjc5GwB075qH34FcIdpShYIw3DxFA?e=4%3abltg7p&at=9	Get hash	malicious	Browse	• 80.0.0.0
	ds7002.lnk	Get hash	malicious	Browse	• 80.0.0.0
	http://https://townemortgage-my.sharepoint.com/:b:/p/cislami/ETa8xXdrX-FKtlaSfOphTioBLICbx4muhejuoDN0jK0wqw?e=4%3aBnR24e&at=9	Get hash	malicious	Browse	• 80.0.0.0
	xJbFpiVs1l	Get hash	malicious	Browse	• 82.30.74.138
	SecuriteInfo.com.Variant.Razy.803156.13117.exe	Get hash	malicious	Browse	• 81.106.72.253

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sDSRBJGFaW.exe	Get hash	malicious	Browse	• 81.106.72.253
	Advice.xls	Get hash	malicious	Browse	• 81.106.72.253
	iwqOx.pdf	Get hash	malicious	Browse	• 80.0.0.0
	pty10	Get hash	malicious	Browse	• 217.137.225.123
	http://https://jcpconsulting-my.sharepoint.com/:b:/g/personal/maireads_jcpconsulting_co_uk/ERfHfSCzdwpCiQXDqtKNHKkBnVvlszs3rd1CSU_-rQLUlg?e=0TY6UC	Get hash	malicious	Browse	• 80.0.0.0
	purchase.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	615
Entropy (8bit):	5.723992291995027
Encrypted:	false
SSDEEP:	12:vDRM9l+53ZiERDRM9lo3ZiEGDRM9HstZiE:77EFloAEseE
MD5:	B726391586997DC41F86AD4C08DAAF09
SHA1:	AD31126B6EBACE9E714C5669EF74EFB51AA4301A
SHA-256:	278E4380CA115CEC13ADDC7055A0176E61252464AE1A543BBEA0775A6E55F52B
SHA-512:	D56FA8EA8B568F8F2B1B1A3127CBA0DA91B7D96EDD74E73433A04EDAC5A36F28C9B431242B5443D92582CD2A9BC5C8228D8BD752610BBE2FDD848B65A8A40A3F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..Hz.R./....."#.D.q....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....T4V.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .1$..R./....."#.D.6....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .\l..R./....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....e.....

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):	522
Entropy (8bit):	5.65831481632591
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkFl/anZ8Be7Ywcr1TK6tDQ2i9NqEYOFLvEkStE8Be7Ywcr1TK6tH:V9z/WZ9PQe9zF9PQk9zTNKpnmi9PQI
MD5:	915532513265D471759B77351952D790
SHA1:	253B23C2E678741820CB538577585DB08ED93774
SHA-256:	3A9FB4D0BA1B6F97482E71B9BA0E53E1657142679F172EF17E26AF65351AA7CC
SHA-512:	0CA9D252988372B276387EEF79A1A710B207DCA2F69B50AB72C0A1C23614F165EAE737C5B91E3B819AC701D0D9F15839A7324A0237593631A38D5E90A25A8153
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .A.Z.R./....."#.D.;....A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....].....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....R./....."#.D.....A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....".....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....R./....."#.DN.g...A.1.x.'.vl..*|Z..o...+.4....0..A..Eo.....A..Eo.....>2JS.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Size (bytes):	738
Entropy (8bit):	5.619886631009068
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFVAXBblUo6jiyeRVFAFjVFAFD+BblUo6japyeRVFAFjVFAF9iBb2:tB4v4S5SBCB4v40SBaHB4v4mSB
MD5:	87C6AB15033FDD7B2BB75D566ABFFC3E
SHA1:	B82A6FEB0D025BE113D14C16334930D5E981224D
SHA-256:	F9D9B72680CD171C72BFF96DF16D8243DCE93085AE8B09DDC21138F908C2EFEC
SHA-512:	5A23BFEF65C6A3B592946C74AC61C578D3A8D5B56CCC9F9C6066A2B52039B09D0A1340AA6DF1E5ED21D5C6E01F37DAB396FE0D7FB256E7BD9AA9071E0E393I 15
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 .REz.R./....."#.D.'....A..hvDO.N.t@.... .n.*..... ....A..Eo.....A..Eo.....N\.d.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view /selector.js .!R..R./....."#.D.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....j.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked -send/js/plugins/tracked-send/js/home-view/selector.js ..y..R./....."#.D.....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):	464
Entropy (8bit):	5.698190136405463
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsPP/+e/ciWulHyA1TK6t0XH/2NtVYOFLvEWdFCi5RsMT5RN:IbRkiDu+e/NWussGvYbRkiD9/NWuss
MD5:	ED060DA01494AF53DA85C20C7D16309C
SHA1:	27573AF7F25E03C7554B88D0A33D727A01BCBF5F
SHA-256:	D072291349DF24981677C0F2576EC5D21FA7E30D9EE45B83812CFBA07A89A133
SHA-512:	6928185846DFD08308029203E676F4BAC5625A58DE8B29464EF25F04EAEC10E91101FD14A896A1BAA059507C561D838B1A39A4795F5A6CF0996AB622B397A6B1
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 ..E..R./....."#.D.. ...A..8 P..a...R..Y....7.@..2Dm{. .A..Eo.....A..Eo.....2.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .....R./....."# .D'.....A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo..... .....

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):	5.568821862064165
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuPZXP3UVyh9PT41TK6tsD:pyixRuNZ/kV41TEaD
MD5:	6F2446EB92DF9D8EDA73A364E5F80D35
SHA1:	038BC5CD077C0728DBA63FA1509E15C887BBD6C6
SHA-256:	DF117EB2AA2142BB26BBA3B9875B63F071F260BBE65DDEA39BA5620077168FC9
SHA-512:	319754A8266F206A781C261D178A831AC21BFE9AEABF5FC25B21100D3C49D7071F840124EA18767BD85F191F073F8BBC7CBFD40CB7CE876E20400F07D09529F(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....R./....."#.D.....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.. ....TW.|.....

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):	5.637703140906653
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuV/YbyqR4co2sZI8xeGvP5m1TK5kq:mvYOFLvEWdhwjQjR4LZIl6P41TK6t8
MD5:	4BC3D4D0873FE4E09539F17D0BE23708
SHA1:	4D4344B035247902A045F228F66A03A6EF98087E
SHA-256:	5E52A4E15D75948BC60607C0E6E36227231A1E27C27FE9E567E2E2D640DD5920
SHA-512:	613EDAAA0C7F69C613ED398B2BF90C2D4BA77733611AD9D8695A5AC18AD076E42A22617854EC4CD1F481A9CAE982B3D9D154DFDD4782E2CCBC3286E799B3E 4B

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .r...R./....."#.Di.....A.].>....uUf..N...k.....c..I.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):	5.516546514672287
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuV5wtRvwcyxMtv9EWm1TK5ktH3:mJYOFLvEWdGQRQOdQBt26g1TK6tHN
MD5:	6E98AEE5818406EBDBAE58A0E231B6F9
SHA1:	01FFAA2E57E43195C206B4BEED22E73E185F24FC
SHA-256:	9F3E57BD5F101D392D4B9D33FBAA74D02C4272C32B6F82DA254F29213912293E
SHA-512:	95873C382CD334462BE6E2CEAD911F7BA5CF8A910B88ECA747D6358E7E533018D19FE765010E57978C8C69284690F5F60344CD39BFE107CFEA5F16778F4D51F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .x...R./....."#.D7.....A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo. .....`.l7.....

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):	537
Entropy (8bit):	5.654644636934228
Encrypted:	false
SSDEEP:	12:Z5MGzBU5MuR/Eq75Mxj5MuR/Evh5MD65MuR/E:ZSGzXuR/EgSxiuR/EvhS7uR/E
MD5:	2A2269FA326866AACC4E2812DD31A810
SHA1:	995C169156528879938AB82FE5E4EC2EB70870ED
SHA-256:	A7238ADE7EEEF1830BF2E53178D76368FA0317D10C04CC10C45CA5F613704DFD
SHA-512:	26BAEBCFEB234CD434E0D58ECFCB1D73F557E3F1C2DB8F6CC4614EBA37774BF23B599CF4E09956B99A8ADEF785DF233FAB8FF76DD8F059903761DB6E1EE01 54
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .p.Z.R./....."#.D.`....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....a.....0\r..m.....3.... <lb..._keyhttps://rna-resource.acrobat.com/base_uris.js .....R./....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb..._keyhttps:/ /rna-resource.acrobat.com/base_uris.js .....R./....."#.D..h...A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....)C.....

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):	5.5284468758594505
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu2q0/by0zBUKSAA1TK6t7lll:pR5hbelll
MD5:	49EDAD9795ECBFCAF6863F57BFEBD8CD
SHA1:	3C1E1E105F1860F4F67FCA2D86507EEA07948C95
SHA-256:	A2730DA19B5E1E49C73FF28E422171FA5E327154A8B0941295AE03E0FFAB52ED
SHA-512:	863D10CB56509CD2E42DB72091C2C049645A0E6AE94D3DEFE174EC786E9EBBF6966810F89BB438EF7EA59EB08E1ECEF0FA98D9B7DC4A139A8CA7E2FF1CDDC 9D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..Y..R./....."#.DSy....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....6m.....

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):	531

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Entropy (8bit):	5.624943177745693
Encrypted:	false
SSDEEP:	12:KkXxKMSCvgdtUl3kXxKMSCvuctUIlwkXxKMSCvKStUlP/:KkXxiCYW3kXxiCtW7kXxiC9W
MD5:	A3626425C497A3E1F744CE2CBAA93EF0
SHA1:	1FF0F7A420CB5258101CAE2841CDFE22C0D8CFA5
SHA-256:	E556CB800793EF8231612505EE1D85FD4A4E8047AA8D6D4CC0F797717BB49280
SHA-512:	1B8B13E6D9F1ABF4B3FA05E6315050980224DB1C0C1921A7F16A9B5F88D0CF378119FDF9377508EC6790C18B7E7556BC29552FD9758EF241DA426E2FD278F82A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...Z.R./....."#.D.X....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....S.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .....R./....."#.D,....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....K.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .G...R./....."#.D..g...A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	561
Entropy (8bit):	5.6474928121276164
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLkpzyM+VY1TK6trtMkl9YOFLvEWsfOL24gyM+VY1TK6tU2kl9b:5h6OLMCkHzh6OL9pk+Jh6OLAaik
MD5:	6DAA037C95299BB0FDD102F92445F696
SHA1:	A513711161E6298EB4266744D70EA6EAF395A1CE
SHA-256:	FDD5D9F98BA86724B7410FDAEEA5E3725BF0ACE42FF894DBCA4D3757ECDD11D5
SHA-512:	01AB58D48985DA67249AA2BF5C1CBE42BBC015A9C712824331C90CAF6229E6C64A8D32400F7AD18978D07D73C192F2EBE5FCD333C124C7975BC7F2B5D9E9B00
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .}.m.R./....."#.D{.q...A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....r.=.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .f...R./....."#.Dm.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....&.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..2..R./....."#.D.....A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....+.U.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	732
Entropy (8bit):	5.663997699276849
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFb7wSeKaTLn08RVFAFjVFAFIp2+wSeKaTLn8RVFAFjVFAF2+wSeKi:UB4v4b7wzXLn3B4v4IPwzXLn8B4v47wf
MD5:	FB34CE31C435DD5617995A78BEB90CD5
SHA1:	25969D75C4CC38AFD7599513FD50A1CAC40468CC
SHA-256:	CD17387D817E236355D446350EC6AE71C463DEDB3457C972BC261A81B321CC2C
SHA-512:	3CD39BBD363AAADDDB71FAA8792FEE82F33C1C62B526A3657E2F02E2E647C2D2F4F911EC28CD9FF0972406E406353AC30ACFF49FB3697B85E5EC1E9BECFBB07B
Malicious:	false
Reputation:	low
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 ...z.R./....."#.DH.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..'..R./....."#.D1`....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....5.....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 .....R./....."#.D.....A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....p.<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\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):	5.508945017306274
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuD89WV5WY11TK6t:BsR2EseA8c
MD5:	3E120CFA98E21CBC214AA40183A6699A
SHA1:	C72BB90DA33274C87B96DE0D0ECAB20E36B56473
SHA-256:	37FD4C4FEE44938B290668F5B75C4DF3AC01FB8A2C0F71C03B83AC397F0FE479
SHA-512:	2C4FBB687B22992E86C8C930E1874960A2E8E9BE4737942374F3E5A513AE69BCE415D4BEBD4F6B887CCBED0A6FC7D5E9DC1481119185E7B5E4785AE2E89F9DC3

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .....R./....."#.D.D....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....Q..x.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.645434370199555
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQZQJTB7OhKlvA1TK6t6:RbR16pJVJk
MD5:	5D3C579D4856A4A456C9B18A4A74A779
SHA1:	22D82AC5365ADD242FBAA02EB98A914D1ADDA340
SHA-256:	1F669F8A16049EDA7EF71BB4B293F8527602C74D7E067439593E31579A120301
SHA-512:	5B29A81B1DF6A7EE9DC8C974FB406324BD76BDF70EEAFA277A1ED6516D651669896703EB9B99185B22F3A0654EA025992159AFB45CE6A35538E66E4E8BCAF3B8
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .....R./....."#.Dn.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....F.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.610777659097853
Encrypted:	false
SSDEEP:	3:m+lx2gv8RzYOCGLvHkWBGKuKjXKX7KoQRA/KWEKPWFvBXt2brSQdF5YufMm1TK56:ms2gEYOFLvEWdGQRQVuJ0eQdFt1TK6t
MD5:	0DAB0B393A43903B41974DB85A7BE9B3
SHA1:	0639D9F63FEC1B3676D49E9190D8728F33E7D5E6
SHA-256:	DA2E95E41228293F8FF80D861D9C48E8843A9201559322302 53CB9B739237575
SHA-512:	C5393F27F285074CF3B24790BD86A878551E2050DE1E0122C013A4579E0CEE7515C29B08C8077AB84BEDF38A7176021FE19D4B4A9A7A86C704C6EEA7F1496520
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .H...R./....."#.D;4....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....!z.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.6697390981558184
Encrypted:	false
SSDEEP:	12:WyeRl2aRt1wa0yeRltlTBt1wMyeRl2rQTAt1w4u:WJ9fwfJbBfwMJ9Ufw4
MD5:	29D0F9E9057BF70B83D7777729E43C1A
SHA1:	1BBA3ED3529E5D7B976C3E8C91BF1E269CB02C7C
SHA-256:	AE50EBB80A3A6E569DA0FDD84E936164649B2CECF670FB6DA28D4E5A8DD8945E
SHA-512:	9E5E3A4DF2E28AB14BD938190DB5AF4F0C17999AE0465D3C25DA762629B6BC463A4803C25E5C8ECE73C48AD0440EF386CD04AFBA1320276CAF498C6FDFA967F
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .X.q.R./....."#.D..y...A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....32.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..6..R./....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....T.p.....0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .@...R./....."#.D.u....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....{T.....

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):	5.594297660323218
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu2ybBZqwK+41TK6tRl/:wRhCUwK+Ed/
MD5:	E9D29013DAA3A470CF5BCD0731716F46

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
SHA1:	D29F3CEE6AEA6F3162F87FE828C0545F709EBDF3
SHA-256:	72B33DB63E03A6D84FE424A0B3B93D5A386B80AD991F8427918590152F2835D1
SHA-512:	B97C76BC616A776D23CAE44276B1D8D771280FF772F05DF1E180AEB1D2040C88DE5E117BF38E1C301FA4B7BC6B06CFDCBD048E3FFB9E2FBEF6336AFCD5E7E60A
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .....R./....."#.D.B....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):	690
Entropy (8bit):	5.665995690268961
Encrypted:	false
SSDEEP:	12:/RrROk/+/ifLEdlRrROk/dSZifLEhRrROk/sifLE:/PJ/+/i4dlPJ/QZi4hPJ/si4
MD5:	42A476379BDA7CB7E3971A6BD84E03F9
SHA1:	712FE65A4EA3E318FC7F21E1A5930D9B02AA8ED2
SHA-256:	7AD3EEDE9C15FA2B08A0495F17BB9F0FA6CFC2D717743D46848FCA0C87E8FBC7
SHA-512:	1B0D5F83EA5A479A4A7D325D7DCF0D3E55F99CACC6A02FE1B483AE6A061FFD37E345EFD522774A34A701282A77DDAAC1624FC25B4846B71A6628B6B5D77AEC3F
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...p.R./....."#.D-.y...A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....JW.^.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..!..R./....."#.D".....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....#.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .N. ..R./....."#.D.a....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....&.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.654785616007239
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXI1/k1QPLr1TK6tU+mDEYOFLvEWXILbpyR5S1QPLr1TK6t6/EmDE1:xqTwkCPLn2qT8CPLn8TqTnvT35CPLn
MD5:	101FAD9AFD97169014E3576031987392
SHA1:	86B0B7A04CBA4B9764CA480583CABBFC28AF46B5
SHA-256:	A06B72A3C88110922C941DBB6A2FCF0F915291F3CD2380A39772E575DD6A3944
SHA-512:	EA1668483DF952A60B965A7651F4091581BEBF36F1F936FB7C686ECA9C38D6E543AC15884E08E82D72D8BFAFEC8DC0C8E0324A0434369B1950F550511C002E4E
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .o.m.R./....."#.D1{q...A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....vw.....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..}..R./....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....S.....0\r..m.....:....f....._keyhttp s://rna-resource.acrobat.com/static/js/config.js .l"..R./....."#.D.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....l+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	621
Entropy (8bit):	5.681227335613932
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAu/JXyw/sEJ41TK6tvM52YOFLvEWdMAuZYx/1LgZsEJ41TK6tZMy:zRMLnsDbRM6gZsDBRMl7rsD2
MD5:	ECE3FEEBF3DC4CE904FC80AD133C3F85
SHA1:	D5C38A6BE48463A5FA0EC154D4DD391847A70D2A
SHA-256:	A3BD9C547201E7DF3FE62E91A62BE5A3722462FA327CD2DE6A5545BC53FCA12F
SHA-512:	4706E55CBFB6DC9D4EF5E5768CAC919BFD244392320F4C5554C62B26DD5920858B70753B930D109559DA1C78DC8BA6DA709C3FF2CEF84DEF529713072B04052
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...y.R./....."#.D@.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.... ..`G.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....R./....."#.DI.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo. ....._.(.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .a...R./....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A. .Eo.....A.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.663682855896081
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuqrtKUJgFong1TK6tKHeYilPYOFLvEWd8CAdAu7a/shGYU:6lJRzFJqoMkClJR6hGYqoMrlJRBqoMg
MD5:	DA7E645D3D64EF1CE6E9512A768778D9
SHA1:	1AA5EE754994FCB4DD347F25B73057E60F61C1F8
SHA-256:	063B394F3FF4B4FBD33240D5CDE605DB7E382FB4B88984A7FA6966B19A78CC1E
SHA-512:	7538F5218D6D99D19307B7C52BDF488BD98240663AE558F54840C3BA8DD0774BAAF39A9F8353245006D7632E312175989DE27D5B6B30011EAFB4325C9C593FE9
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..Bz.R./....."#.D.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo .....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..E..R./....."#.D.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo..... .....A..Eo.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .Y...R./....."#.D.....Ac}.H7M=M..-....Ix..R.I... }Rl.$q.A..Eo.....A..Eo.....Y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.679866793147174
Encrypted:	false
SSDEEP:	12:F8hRrROk/zq258hRrROk/l82x8hRrROk/vE27:UPJ/zq2APJ/I82YPJ/c2
MD5:	5969CBCE5C468BCB2C90D550973FDA6C
SHA1:	CE7C2CAAA364C84C2327C9FE24E09C52B40CFB4D
SHA-256:	98B060B55F781777AF6DBA6D60D08E0DA54DE562873E31951AE4A9D6CBAD21FC
SHA-512:	88C61C4475758FE91F8DE3BDFBF28A8119FEB4059E341436AC4679EB6681A27BF3B95C13593ED1052D34259E3ADABBE4904A2940BB6E0EC5A32035CD8873F48
Malicious:	false
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...p.R./....."#.D..y...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 .....R./....."#.D.(....A..%.k.SZ..~W.....:)' B..ad.....A..Eo.....A..Eo.....*.$.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....R./....."# .D.F....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	639
Entropy (8bit):	5.683739545428913
Encrypted:	false
SSDEEP:	12:ehRcKzKNJIChnhRcT5NJIChRcSKSNJIC:eh9MJICnh0JIChBzJIC
MD5:	39C7FA117CF4F0EB01B918DAACE3E44C
SHA1:	BF269B8DAF986FE07572930D1E26F6C43E6913A7
SHA-256:	820A63CE272793AEAC56FDCD5D09C3FE4AB2848C928DCEF2DE07C2722A17FDA6
SHA-512:	93BB32FC2577A98C05F0E331CBF9407F459D4C90CD5085360823F5D6C31921AE430419E3F8C10A0E4DF69C0C8B764A11EE9B47AA2DB8107744FDC35B4C439A5
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..0q.R./....."#.D..z...A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A.. Eo.....-W|.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .....R./....."#.Dn.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.. .....A..Eo.....6.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .....R./....."#.D.....A.;"./N_.,.:C..2....9L.H...3:.. .A..Eo.....A..Eo.....W..@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.649476917007961
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu0rtYHQTLzgm2d/1TK6tmZ8OEYOFLvEWdrIhuwPEUbLzgm2d/x:0RKgGReIARW/RecRmawRe
MD5:	85F3D3E1E70516F1E3D6D2CD11933F72
SHA1:	9A108660895D4DE37501942D276D4B5F13555BF4
SHA-256:	8D94F71348C33BE29063D6D3BF090F20A439566276F5EA2DD41203F46C6EA395
SHA-512:	A400D00EEBA151FE0C0EBF5376A7C63D0E56916AC6B8F1C999DF0AD0B934B5A5434948F58ED031620CCFB1C452C6271FDE1E28558CE8070CCFD32CC8DF088(F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .?.p.R./....."#.D:.y...AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo...z.@~.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .^...R./....."#.D.X....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....0..b.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .{...R./....."#.D.....AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....s.....

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):	564
Entropy (8bit):	5.679658003809689
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KB7d0Bkx56uvp1TK6tz/EAElVYOFLvEW1Kf/sie0Bkx56uvp1TC:6JJKB7WIF/YJJKcWIcJJKSQI
MD5:	3428B6DD9977EA4F99207C56307914A3
SHA1:	27FC33667646104DC103F6B24146727684E1B045
SHA-256:	9BFEA64F40C3AE0FCE8CDC9CC74EB95972EC5763A87FBFD0888ABCE08F09D918
SHA-512:	D4991C090FBADCE27BD3437085955811840C26ADC3D316917CDDEAD4DEEC0963962614891418 78BB9AC9B72E635EA2D7696BD59A2FC1141D8C58EE5DF70866
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...^.R./....."#.D..2...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....%.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....R./....."#.D.G....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....#.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .O"..R./....."#.D.B{...Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....S.....

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):	5.653762026783216
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuaTZg7ghUDLYtmOZn1TK6t:xRBJe5DcFZL
MD5:	F36DD7CD73861D927E0DA739DB9CB3F0
SHA1:	9A975736D7BAEBC0B7EBEBD9A860FF42FDF0EB04
SHA-256:	8C4F7CBD6F1A936388C791FE58822EE0FE806D2782ADDDDC7F28E8D85FFE270A
SHA-512:	D00753197035858D9EA26E0EE49EBAB756D011A02969919F2FB67C03CAEC9593BC91B06358B5239C462AFB8FEAC0A9D8F0F5F2C9C96012CD4B1A74CC76F7E1C6
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .....R./....."#.D.h....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....<.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.634358389450929
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp78x/HLVPu1TK6tDBsRPYOFLvEWIa7zp7iXrfLVPu1TK6thE5:BPHmTcgPH4cXTPHDCq5Rc
MD5:	884ABDC18593DA7709BF5E573414447F
SHA1:	E1ED3A370F3944397BD7CC62CB0898757622F123
SHA-256:	AF2BB8C39DBDEB435753B32A3B8E56F8B1D6046810158CD55492A82375FA0FC6
SHA-512:	CFD4E40FE462694AE51BA2D48B814B7592FE2F5EEE20BC0CABB1C73734F93FB45AE52AC252067A69734373E1F4F5A9FE71266527A01DFEAFECF1906FA61272B6
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .m.Z.R./....."#.DeS....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....Q.S.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...R./....."#.D.....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo...../..x.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .j...R./....."#.Dy;h...A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....p.C.....

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):	5.596053679490328
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
SSDEEP:	6:mKPYOFLvEWdENU9QNZXFiM3Y1TK6t1Rj:bJRT9Inr07
MD5:	4A6FE20417CD8BEBBA895B60ECD6828A
SHA1:	7039A28A31FCFCFD0F6EEFCE56472F6D4FE344F4
SHA-256:	E64CD842CDB9AB7418838EC2837A82A38B9A7CD95049065634C14C2E9FF2A248
SHA-512:	7CCDCA91C14D6440A5EB4825E9AA7B127C334F5BFFC9BEC2D4F73FF82984D27D4C49CAA07BBA187DADA10C51B6E9F79695BC2E2773D3C29146D4A4347675F67
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....R./....."#.D+0....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....s.4.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.621048846955409
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ7Gbt9RjBRCh/41TK6t:XRc9lDi/E
MD5:	7B919A5EA5823B6A61E41012E99CDE7E
SHA1:	663EBFF4C3B5F6CEFAD7C09D073B858838330E5F
SHA-256:	F17714171A88B8680D0E997BC0336D3515D67C5FCC501D6A51CC3B157E81C4DD
SHA-512:	46B9A5382D714DCFBC1DB71781E365F9868328D94DF00AF791221622E13CC6A5DF240307652C5FBA354B32F803910DC2F41803DEB84B6E9B8B10A539B16AC378
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .A...R./....."#.D{. ...APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....F..G.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	462
Entropy (8bit):	5.609998122743198
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuTKXHojULlF4r1TK6tFlMqs6XYOFLvEWdFCi5mhuEPx/J:bs6xRkikZLlF4ntxs6xRkiCPx+LlF4n
MD5:	9D447067612449B29B1C455BCF199228
SHA1:	C9B4221AA807EB8B9B6A734B0BA3C2E6E228F071
SHA-256:	BDD35AB77F3244010768E346E2C787B7EFA8A3516062911C6DDADB44C86A842C
SHA-512:	10831338D65418840C4F322BA3BC42E1B818813A59354B7B215B5EE43429EE91EB68A5BD5AF8427A158F4F69EAAC3BFDC36541DAE1558259FAE6A2B951C68FB3
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...w.R./....."#.D.X....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....s.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .....R./....." #.D.d....A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....s.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.565886900514177
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvKJ3Z//6sTi4cu1isLK5m1TK5kt4:mhYOFLvEWd/aFuob6sk941TK6tg9
MD5:	41C483B6B64E90CAF2717FF085B7BBF6
SHA1:	DEDDA28A879E9AA3B3BC8805689A6DA55D0D4A97
SHA-256:	304AB13457BC13A4410AB6F190D574FED25460223B0AB5EA6CEC7000FC70F005
SHA-512:	6B0DD3584C1C13C388A5C5132AD43B7DDC820499823D32A6ABA513DCB013747128E253F71CDA53546FC819E5C998FC942A527289D2B7257301EEAD1AFF077AE
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .Z'..R./....."#.D.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....G.=.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Size (bytes):	208
Entropy (8bit):	5.559393306696692
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQCkphW/BoBMqVd3G4K41TK6t:2DRuRPkrcoB9Vd2k
MD5:	5CD9964173061B52B7535ABE6EDFB892
SHA1:	31BCEA9D329178C62F7AC19D6901AB3A73F4A8F4
SHA-256:	11E949007BE8C9AED3C9EC091DABED1D6EF682A35AFAA63DF87D2F8E181B36C8
SHA-512:	1BE4B0055D65DD64725ED563AAADECF1496FF89B4F4DA6FA44C5EB0E32E90D57D5F1A93A3D09ABE434A32AB7D6BEA1C053E62C810CEB5D40C71F74660EF54D7D
Malicious:	false
Preview:	0\r..m......P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..''..R./....."#.D.R....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.69657786148044
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QHpS2QNuA424r1TK6tvkqYOFLvEWd8CAd9QZZK5oNuA424rf:+RQX38rnRRQO05ZrnURQ/0Mrn
MD5:	9C772F01AD767F8468EB7D2600A1C78D
SHA1:	D1B8CDA867F41212F421F9851F233A795D4850C6
SHA-256:	BD5714D350A3EC2491D8F2CBC6E74ECE126CAF540365CE994DED28E8FA31CB1E
SHA-512:	9C674A044E2CF167A5D85219488748C3CC99412FA880ADEB3795EB5286861FCF6144C78F43B3E6574895EEA5AEAEE869BB11C9135981A7FF24FC34BA0D9473CI
Malicious:	false
Preview:	0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...z.R./....."#.D|....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....0\r..m......P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .m&..R./....."#.D.l....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 ..q..R./....."#.D#.!...A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....M.f.....

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):	5.570810222625245
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAukZ2RUryC8n1TK6t49:xhRTaXr7Qm
MD5:	9232A4D739B03528FE9B5DD5102AB2E1
SHA1:	E434988C80381791DA31486DBF67E65CED0DC997
SHA-256:	E9290C39EE365E68AB5054035A2F3B8FB5026E057C18E13E09284EBD10DF577E
SHA-512:	F337617D625EA0B96938310A8FBCCCF23C69C4B09ECBD238898BEB9F2E33D6562008E04E7E0BF1606D0A2815311ECE550D4EF92D09595F83CF3090B33C88D2E
Malicious:	false
Preview:	0\r..m......R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .9...R./....."#.D.&....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....-BI..

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.690750513381804
Encrypted:	false
SSDEEP:	12:nRrROk/VSVml1RrROk/Vi58DmFRrROk/VGIslm:nPJ/THPJ/wmCFPJ/tt
MD5:	7ADA5AC0787BA6558EFF4ED36B2D0611
SHA1:	DEB015C12AE4FA71E19EBFFEA1B0114CE43AF073
SHA-256:	2434170E24A41BFF6C365BB976759E9445E16897AAAFBA247397B3C97083E31B
SHA-512:	9BA101EE511E86FAECFC7B1E92CED525671DF8BFC1EE9C12D29C936167AEC95C0562B53B113F406D98FB10E184FDD19060A5E13468F47180BC63125B0AC0D93
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...r.R./....."#.D.Z....A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....3.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .X...R./....."#.D.<....A ./.ev.....N~..6.b. ....$.j;:C...A..Eo.....A..Eo....._P].....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..;..R./....."#.D.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....i.....

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):	5.567374587764299
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuhXKzAdm9741TK6tqo:qxRcBdu7Ej
MD5:	376CEEE7A69BD86721A17C6E5ABF8979
SHA1:	C6CDB89CA0A878764F379437D26B58893804FA97
SHA-256:	090D9BF6707D156259D106BE73D0FB98B334D77CDE488DED9794E01F95AA2A28
SHA-512:	263BFBD87F1F91B4A9AF55CFEADA50283E24D67D7FE6B9E617FA83DB3426BBA2DE820674364A4CEC48B51EAF1EAD934C18841D4E4C0890FA51EDE9E34702DB B3
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .+|..R./....."#.Dp(....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo .....05du.....

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):	5.5683273087969685
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvHTyKXqSyAfB6shoq+Nem1TK5ktVN:mMOYOFLvEWdwAPVusqqxAfkJn1TK6tV
MD5:	7D82473066C942CA8B44E097A1E42D02
SHA1:	FDD1C97D42AAB731CFBB3F21069C078746FFF3B3
SHA-256:	D424283B1C7AC7AFC26C6B0BD68D4209CC86CA7B3613C2D8627B4F06950BA3D6
SHA-512:	7AE9309878ED50408215030D3BC58B340D9680295AE67A559C21699174AE823B7A988DA7D0188120D54A57D6C48448EB5ACA06EBA19698C4EC81DE54A7E96BE/
Malicious:	false
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .`...R./....."#.D.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... ...n.....

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):	5.688783366837366
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQxtLm4zhcsBXIh1TK6tS:mxRBJQ2JDB0k
MD5:	FC96A43264538AF0C50F41F41F75B262
SHA1:	221F28F84CA2BFD9BED41CD46D966D00CB8639DF
SHA-256:	BB89A839698B8E127A450763118758AEE64AB03B355D64965BFAA5868F537192
SHA-512:	BCDD659B476A81C2FFBE478F1B4F54C8D6B86551942D121D48964EF1E4CF098BCA6F79A0CD9A909CE61DF4A5B1FAE887683BF43CA05F8B3A05EC2BDB437475 01
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .Y...R./....."#.D.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....*Y.9 .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	684
Entropy (8bit):	5.641828631128729
Encrypted:	false
SSDEEP:	12:3RrROk/sanlV7cfRrROk/s250G7ckRrROk/s4BP7c:3PJ/nn0fPJ/WbkPJ/a
MD5:	89B2FB5B53E248DAE16512B3139D002B

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
SHA1:	7B4CAB897CC3D7EF7A8C10A495023E90A4C8ED4C
SHA-256:	C2271E77D19752DF7AA4E441C76263E69FA1173DC046BD23D3156F6067916723
SHA-512:	5602F7BFA5FA1B5697D3A6549B32DEA13A834753FFE8EE7762834B494F515EBB307A4394C4A7564AB352B48625CF22FD990190D3F76F94A64A0DF5D5529BE073
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .].r.R./....."#.D,.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo..... .....A..Eo.....g.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....R./....."#.D.|....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo..... .....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..?..R./....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....R.tQ.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.311677530405763
Encrypted:	false
SSDEEP:	24:0I2bYdB8J6MbkeljKqRomj/kt/jygqUA/Ir3wz95g5/YMz/xCyMeVmVJG1x/Ex/a:t2kdhMkCqmjMtOTBSgc9Hzx8xBiCn/I
MD5:	6E526F5B071A78FFD26C298CB182CF59
SHA1:	44E2A0D6DCC7192433B2E7B5601B08657E4DD3C3
SHA-256:	DD274AD4E832434B11A2AA7C3F9DF45AFED3A09CB175D92D2A8709153130BF34
SHA-512:	BF9E85A9560537E12D24EEE63EE735AE228006A02E053E09A38F370D9AC1DA6D3F110CA1C8491E5A8E697AAB075F189BA986B067435E0B4763F7875A7312C735
Malicious:	false
Preview:	.....goy retne....'.....'.....:.y~A.@.....*..@.....oB*.....#...(@.....k7A.@.....D.4.@.....[.i..%.@.....<...W..J..... ..,+..._.#@.....J..j...@.....6<|.....A?.2:..@.....+.{..'@.....*)....J:@.....2q....@.....P....V@.....+.U.!..V@.....P[. q@... .....!...0.o@.....u\]..q@.....@.....*....@.....o..k..@.....^.~..z.@.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@..... .....v...q..@.....C..M..@.....a.....~.,.4>.@.....&.S....@.....@..x.@.....=....m..@.....;/...@.....q.@.....MV3..@. .....:..N.A..@.....Z..... !..oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	294
Entropy (8bit):	5.09644209661831
Encrypted:	false
SSDEEP:	6:mEcyq2P92nKuAl9OmbnIFUtpYyz1ZmwPYylRkwO92nKuAl9OmbjLJ:RRv4HAahFUtpf1/Pv5LHAaSJ
MD5:	64A83CB2A2BB650DCCF61408F5EC0E5B
SHA1:	E5F80B2D1F2A8A018D14F31256E6E213941F678A
SHA-256:	8DA1A4C1BA46D7D9254C5CA5CF47A6AEA2D1B485AB6BD09303D368E66556B6F9
SHA-512:	1391786B170257EA697098A73EAF577BB958DB20F3391910FF20E559A1FC75881DA65BF87165F51CDFB0EA45ECFE78BBE4A38F2D325481F20BD21A512AE696B1
Malicious:	false
Preview:	2021/01/12-15:40:57.510 1a50 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/01/12-15:40:57.511 1a 50 Recovering log #3.2021/01/12-15:40:57.511 1a50 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):	1310720
Entropy (8bit):	0.0084423731585201
Encrypted:	false
SSDEEP:	24:T13rz13r+fUrjUVJjUVJjUVJjUVJjUVJjUVJjUVJ:T13/13KUvUvUvUvUvUvU
MD5:	20C2D53F3F6BF479288D699773FA372A
SHA1:	D18859D4EF1A2B4F96A6ACD1F09AB61AAAEB323A
SHA-256:	D6C5C9640C916DF6010AF982C733684606233C1632676FE69EA946B53C438E0F
SHA-512:	4A2A80FEAFDD414C93E701D268262C8F065DDFEC45211DA8A0A30762731DB0E7A21A44E9CEE09375C731C512652D5CFE20EE7821769E35AB95DF2563AB4493A 5
Malicious:	false
Preview:	VLnk.....?.....+.}.^1..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2101122340512-203.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210112234051Z-203.bmp	
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	0.2111895101587603
Encrypted:	false
SSDEEP:	48:8xqDgXTkSHKA+VTTM8Dl9DUosnK0SDnTwmoHKqpN3:hD+khVTTN9VW
MD5:	F34581810CD41EABC99B99130A0CC39F
SHA1:	86501D1DD8FBD9181EC8AA69999113F2067865C8
SHA-256:	ACC878385CC502B9E1637BF48D0C4883309CD73B150E44C2D0252BF7F82657A5
SHA-512:	D4875F04FC295F2610EF7A3405DB90E2BB1B6BD46F5E5A2FCB3605ADBE7E4A7C673C1B682B4E7F0D7E0924B26BA937FF3A8BA880A8C2BAF985A09D40F61AC2AB
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:	modified
Size (bytes):	32768
Entropy (8bit):	3.385425495268058
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQ7OhFVCsL49IVXEBodRBkRW7OhAVCs749IVXEBodRBklW7OhOJ:iGedRBNedRBQedRBkedRB1
MD5:	CE93920AE5203350F0EE15576838503B
SHA1:	C3A6E26E49D7D3512146FB90FE26844A62FC4946
SHA-256:	9C89A428FDF0E0D2524A0E0ABF512C72E3FE827A3357B79ECA27BF107FC3536E
SHA-512:	AE484EDFBBB04180B00403EBA36FEDC8B24DE5D3ED41EA0FEC1A08DEE6CED7F127C73610E03C24CC71D62575577C5B6C84AF9AA9DF91A5306575728C013FC1C
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.1988688437823734
Encrypted:	false
SSDEEP:	96:z7OhFVCPN949IVXEBodRBkJ7OhFVCsiLR49IVXEBodRBkwW7OhAVCsdd49IVXEBL:zBiedRBcLGedRB0CedRB7yedRBm
MD5:	F42BA7CE6B7EFCCE1F6C248CC59152D9
SHA1:	EC3150E34BEA430B686A5327F86F820844B31017
SHA-256:	BAF0D421554AE9759E44A09F791F9889B66B54B09FCB96E9D10E869C8229748D
SHA-512:	48047547597932348E0B46DF65AF3D6F5B28DC5CC325A3CBC740C67FC3D793E986583D56DB60BA62721BE045D95C0D3B1CE4A1BD542FB42C5F445DCCFEA0CBD1
Malicious:	false
Preview:	.....3..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1752	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1752	
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

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):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZCSl2mLCpcf3pLSjmkT6QH+VVdKeYyu:J0GpiyVFiBhl2mGp5pT6++VnKeK
MD5:	F1F22D7BB5792FBCC5EFD5B8CDEA461F
SHA1:	D3F15700B17527E8B3DA3F9881D5A0582721D8EC
SHA-256:	AF58775151B3E36876BA427B222130F8F33D9E1597741FBCAF62CCA08EE72AD1
SHA-512:	5BDC10D3B1FF04FD0198569B55342F11CE73ED7A2FA040023FF414249E835BA9B3F204715FC1FA0F1549FAD5107669B96891EC7735D42BE76C83019065A28BEE
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:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."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 1.4
Entropy (8bit):	5.971235223965398
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	NORNIK COVID-19 NAMES.pdf
File size:	2363
MD5:	9de37675ac573d74e356275780324a4a
SHA1:	3777f82c37f773eeb8552916f9877bac2137bea9
SHA256:	39325b29e921762bcb93a32c74bdcf252c4255c1a9bc379d771a1db6d3d9dd1c
SHA512:	6901d719da56ddb71b77e7f17ceecbdddbff9dc374a0148f1cc278a54889e0bf5ba13bfcb6204baf28c1ea9f5816753182cfc3265f734dc13a43a09c91e8fe68
SSDEEP:	48:ALyi6vWsHPHjwGRMHLgW0KDOqyGCYIQR0AITii3n:ALyi6eIswKLgW9DdPmRii3n
File Content Preview:	%PDF-1.4.%.....1 0 obj.<</Type/Page/Parent 6 0 R/Contents 5 0 R/MediaBox[0 0 612 792]/Annots[2 0 R]/Resources<</ProcSet[/PDF/Text]/Font<</FTmznIEwMh 4 0 R>>>>>>.endobj.2 0 obj.<</Subtype/Link/Rect[88.56 604.79999 509.76001 678.23999]/Border[0 0 0]/C[.945

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	5.971235

General

Total Bytes:	2363
Stream Entropy:	6.156976
Stream Bytes:	1108
Entropy outside Streams:	5.357350
Bytes outside Streams:	1255
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	9
endobj	9
stream	2
endstream	2
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	2
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

UDP Packets

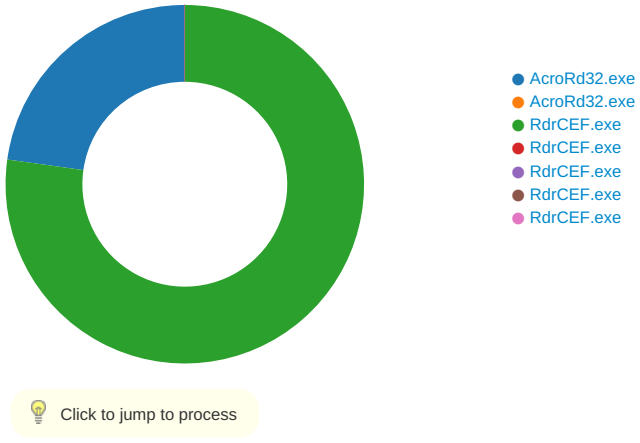
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 15:40:41.805696964 CET	59596	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:41.853467941 CET	53	59596	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:42.985053062 CET	65296	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:43.044231892 CET	53	65296	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:46.177241087 CET	63183	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:46.225087881 CET	53	63183	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:47.361491919 CET	60151	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:47.419085026 CET	53	60151	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:48.850728989 CET	56969	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:48.898606062 CET	53	56969	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:50.921775103 CET	55161	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:50.972646952 CET	53	55161	8.8.8.8	192.168.2.5
Jan 12, 2021 15:40:55.109035015 CET	54757	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:40:55.156871080 CET	53	54757	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:00.489839077 CET	49992	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:00.494808912 CET	60075	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:00.549166918 CET	53	49992	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:00.559067965 CET	53	60075	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:01.010900021 CET	55016	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:01.069458008 CET	53	55016	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:01.513741970 CET	60075	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:01.513787031 CET	49992	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:01.573565006 CET	53	49992	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:01.575117111 CET	53	60075	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:02.373099089 CET	64345	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 15:41:02.429683924 CET	53	64345	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:02.526350975 CET	49992	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:02.526416063 CET	60075	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:02.586040974 CET	53	60075	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:02.588743925 CET	53	49992	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:04.574568987 CET	49992	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:04.576025009 CET	60075	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:04.633789062 CET	53	49992	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:04.635221004 CET	53	60075	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:08.614243984 CET	60075	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:08.614305019 CET	49992	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:08.673557043 CET	53	60075	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:08.674120903 CET	53	49992	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:20.587481022 CET	57128	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:20.635576963 CET	53	57128	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:26.585300922 CET	54791	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:26.716603994 CET	53	54791	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:26.737200022 CET	50463	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:26.787888050 CET	53	50463	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:26.880136967 CET	50394	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:26.928150892 CET	53	50394	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:28.409167051 CET	58530	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:28.470585108 CET	53	58530	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:33.800478935 CET	53813	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:33.860568047 CET	53	53813	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:43.151649952 CET	63732	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:43.208211899 CET	53	63732	8.8.8.8	192.168.2.5
Jan 12, 2021 15:41:50.446119070 CET	57344	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:41:50.512886047 CET	53	57344	8.8.8.8	192.168.2.5
Jan 12, 2021 15:42:13.831808090 CET	54450	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:42:13.879647017 CET	53	54450	8.8.8.8	192.168.2.5
Jan 12, 2021 15:42:14.362592936 CET	59261	53	192.168.2.5	8.8.8.8
Jan 12, 2021 15:42:14.429969072 CET	53	59261	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 5872 Parent PID: 5540

General

Start time:	15:40:43
Start date:	12/01/2021
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\NORNIK COVID-19 NAMES.pdf'
Imagebase:	0x920000
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	success or wait	1	9565C3	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	success or wait	1	97AE05	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	96EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210112234051Z-203.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	96EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1752	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	96EA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock5872.1.2604170926.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	9A2657	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9E83C8	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	9E83C8	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	9E83C8	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	9E83C8	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	9E83C8	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	9E83C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R2ebtnt_r5pyr3_1co.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	96EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	96EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rkw3tuh_r5pyr4_1co.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	96EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R9bsg9i_r5pyr5_1co.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	96EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R11yjmht_r5pyr6_1co.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	96EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rahmi45_r5pyr7_1co.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	96EA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.1752	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	9AD405	NtSetInformationFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	96CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	96D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	96D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	96D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	96D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	92EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	92EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	92EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	96D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	96D41D	NtCreateKey

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	97DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/NORNIK COVID-19 NAMES.pdf	success or wait	1	97DF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	NORNIK COVID-19 NAMES.pdf	success or wait	1	97DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	97DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	97DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 61 6C 66 6F 6E 73 2F 44 65 73 6B 74 6F 70 2F 4E 4F 52 4E 49 4B 20 43 4F 56 49 44 2D 31 39 20 4E 41 4D 45 53 2E 70 64 66 00	success or wait	1	97DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 31 31 32 31 35 34 30 35 31 2D 30 38 27 30 30 27 00	success or wait	1	97DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	2363	success or wait	1	97DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	97DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	97DF47	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	97DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	97DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	97DF69	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	97DF69	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 33 35 32 30 2D 30 37 27 30 30 27 00	success or wait	1	97DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 1752 Parent PID: 5872

General

Start time:	15:40:44
Start date:	12/01/2021
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\NORNIK COVID-19 NAMES.pdf'
Imagebase:	0x920000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 6312 Parent PID: 5872

General

Start time:	15:40:50
Start date:	12/01/2021
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:	0x830000
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
\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	14	9383E5	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	56	938447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	164	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	17	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	9259E2	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	11	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1626	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	9259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	9259E2	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	5	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	2	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	9259E2	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	17	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	18	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	3	9259E2	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	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	9259E2	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	42	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	45	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	87	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	3	9259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	41	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	9259E2	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	14	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	9259E2	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	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	13	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	9259E2	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	12	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	176	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	214	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	9259E2	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	200	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	195	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	22	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	2	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	2	9259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	85	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	6	9259E2	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	9259E2	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	9259E2	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	9259E2	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	159	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	75	9259E2	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	9259E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	6	9259E2	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	9259E2	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	9259E2	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	9259E2	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	3	9259E2	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	9259E2	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	9259E2	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	9259E2	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	1	9259E2	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	9259E2	ReadFile
\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	9383E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6476 Parent PID: 6312

General

Start time:	15:40:53
Start date:	12/01/2021
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=1636,581213635960850 0254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17107349628966656 63 --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=17107349628966656 63 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x830000
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: 6500 Parent PID: 6312

General

Start time:	15:40:55
Start date:	12/01/2021
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=1636,581213635960850254,1313857005886023345 1,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=2261788824419733270 --mojo-platform-channel-handle=1740 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x830000
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: 6540 Parent PID: 6312

General

Start time:	15:40:57
Start date:	12/01/2021
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=1636,5812136359608500254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9399729911713544515 --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=9399729911713544515 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x830000
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: 6956 Parent PID: 6312

General

Start time:	15:41:02
Start date:	12/01/2021
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=1636,581213635960850 0254,13138570058860233451,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13560670023211164477 --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=13560670023211164477 --renderer-client-id=5 --mojo-platform-channel-handle=1792 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x7ff797770000
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