


**ID:** 324341
**Sample Name:** Invitation - Prime Minister of Israel.pdf
**Cookbook:** defaultwindowspdfcookbook.jbs
**Time:** 09:01:30
**Date:** 29/11/2020
**Version:** 31.0.0 Red Diamond

# Table of Contents

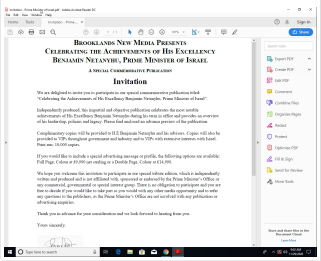
# Analysis Report Invitation - Prime Minister of Israel.pdf

## Overview

### General Information

| | |
|---|---|
| Sample Name: | Invitation - Prime Minister of Israel.pdf |
| Analysis ID: | 324341 |
| MD5: | e3f4a57d14090a2. |
| SHA1: | 0163a63054fd5da. |
| SHA256: | 63f3f7706c4d6ca.. |

Most interesting Screenshot:



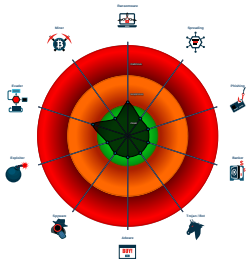

### Detection


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

### Signatures

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

### Classification



## Startup

- **System is w10x64**
- AcroRd32.exe (PID: 1744 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5792 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 2148 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6316 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=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=129495829832415726 --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=129495829832415726 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6340 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,12072885215581891837,16927562936397834584,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAAOAAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9376569714315728772 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6392 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=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2060730633019401765 --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=2060730633019401765 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6516 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=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6479133236096394756 --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=6479133236096394756 --renderer-client-id=5 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6696 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=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=301876132503772327 --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=301876132503772327 --renderer-client-id=6 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

## Malware Configuration

No configs have been found

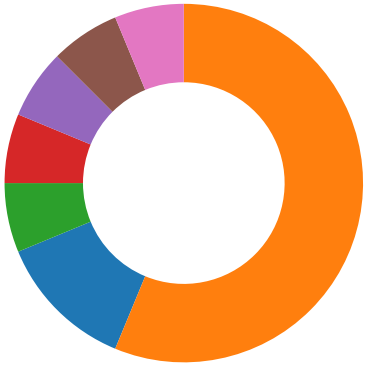
## Yara Overview

No yara matches

## Sigma Overview

No Sigma rule has matched

## Signature Overview



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

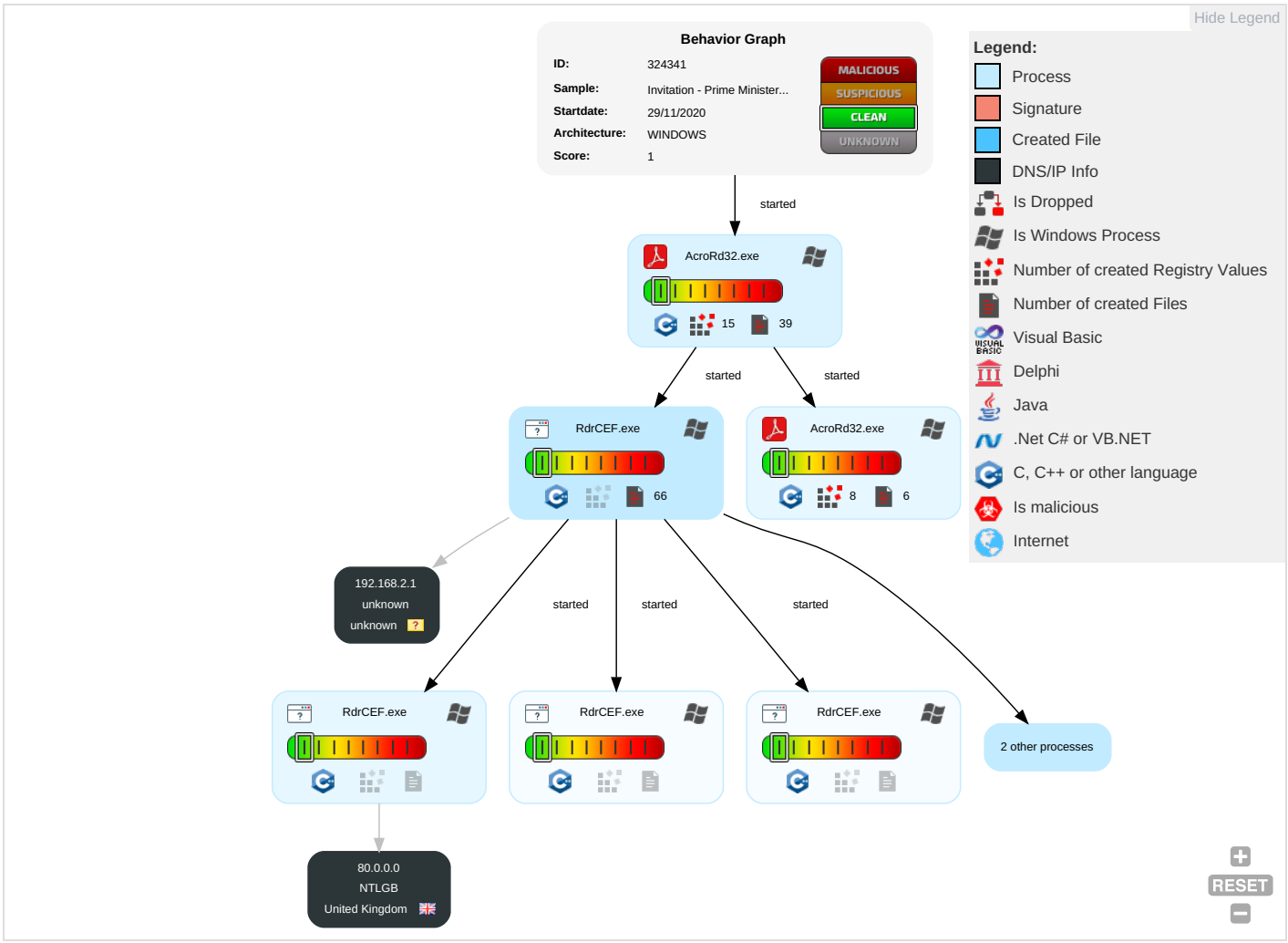
Click to jump to signature section

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

## Mitre Att&ck Matrix

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

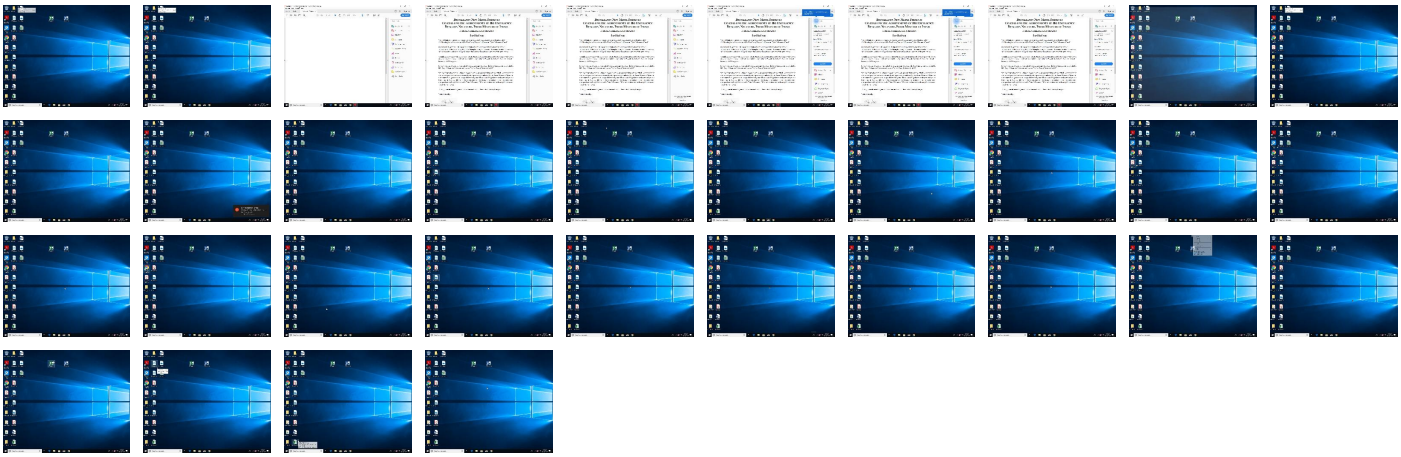
## Behavior Graph

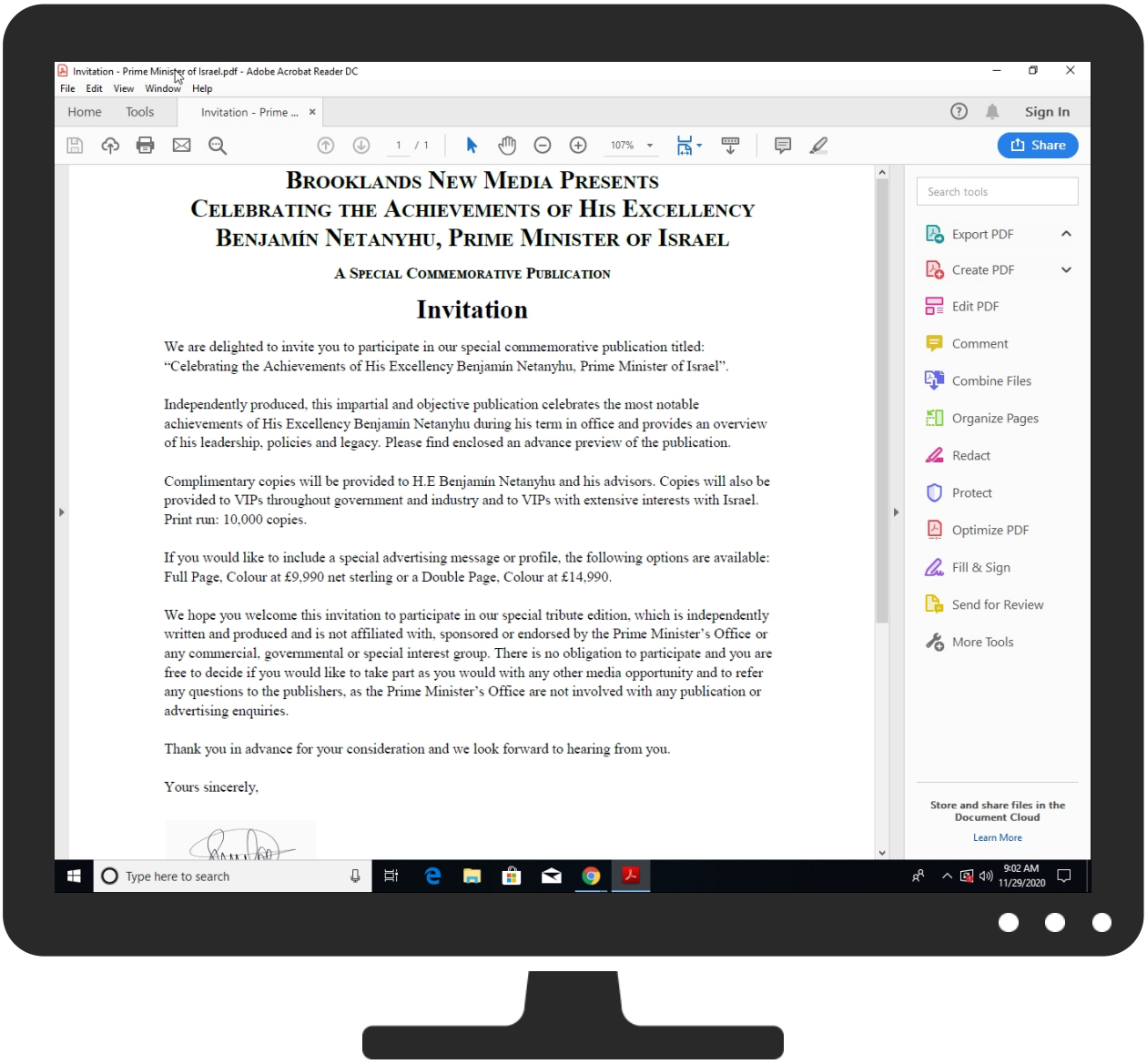



## Screenshots

### Thumbnails

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






## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

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

### Dropped Files

**No Antivirus matches**

### Unpacked PE Files

**No Antivirus matches**

### Domains

**No Antivirus matches**

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://cipa.jp/exif/1.0/) | 0% | URL Reputation | safe | |
| http://cipa.jp/exif/1.0/) | 0% | URL Reputation | safe | |
| http://cipa.jp/exif/1.0/) | 0% | URL Reputation | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/i | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ns.useplus.org/ldf/xmp/1.0/ | 0% | URL Reputation | safe | |
| http://ns.useplus.org/ldf/xmp/1.0/ | 0% | URL Reputation | safe | |
| http://ns.useplus.org/ldf/xmp/1.0/ | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/ | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/ | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/ | 0% | URL Reputation | safe | |
| http://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://iptc.org/std/Iptc4xmpCore/1.0/xmlns/G | 0% | Avira URL Cloud | safe | |
| http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs | 0% | URL Reputation | safe | |
| http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs | 0% | URL Reputation | safe | |
| http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/ | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/ | 0% | URL Reputation | safe | |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/ | 0% | URL Reputation | safe | |
| http://cipa.jp/exif/1.0/)_1 | 0% | Avira URL Cloud | safe | |
| http://www.brooklandsnewmedia.com | 0% | Avira URL Cloud | safe | |
| http://cipa.jp/exif/1.0/ | 0% | URL Reputation | safe | |
| http://cipa.jp/exif/1.0/ | 0% | URL Reputation | safe | |
| http://cipa.jp/exif/1.0/ | 0% | URL Reputation | safe | |
| http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default | 0% | URL Reputation | safe | |
| http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default | 0% | URL Reputation | safe | |
| http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default | 0% | URL Reputation | safe | |
| http://ns.useplus.org/ldf/xmp/1.0/0/xmlns/ | 0% | Avira URL Cloud | safe | |
| http://https://api.echosign.comg | 0% | Avira URL Cloud | safe | |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/m | 0% | Avira URL Cloud | safe | |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/em# | 0% | Avira URL Cloud | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es | 0% | Avira URL Cloud | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ | 0% | Avira URL Cloud | safe | |
| http://ns.useplus.org/ldf/xmp/1.0/t | 0% | Avira URL Cloud | safe | |
| http://www.npes.org/pdfx/ns/id/ | 0% | URL Reputation | safe | |
| http://www.npes.org/pdfx/ns/id/ | 0% | URL Reputation | safe | |
| http://www.npes.org/pdfx/ns/id/ | 0% | URL Reputation | safe | |
| http://www.osmf.org/drm/default | 0% | URL Reputation | safe | |
| http://www.osmf.org/drm/default | 0% | URL Reputation | safe | |
| http://www.osmf.org/drm/default | 0% | URL Reputation | safe | |
| http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes | 0% | URL Reputation | safe | |
| http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes | 0% | URL Reputation | safe | |
| http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes | 0% | URL Reputation | safe | |
| http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn | 0% | URL Reputation | safe | |
| http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn | 0% | URL Reputation | safe | |
| http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn | 0% | URL Reputation | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/ | 0% | Avira URL Cloud | safe | |
| http://www.quicktime.com.Acrobat | 0% | URL Reputation | safe | |
| http://www.quicktime.com.Acrobat | 0% | URL Reputation | safe | |
| http://www.quicktime.com.Acrobat | 0% | URL Reputation | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4 | 0% | Avira URL Cloud | safe | |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s | 0% | Avira URL Cloud | safe | |
| http://www.osmf.org/subclip/1.0 | 0% | URL Reputation | safe | |
| http://www.osmf.org/subclip/1.0 | 0% | URL Reputation | safe | |
| http://www.osmf.org/subclip/1.0 | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

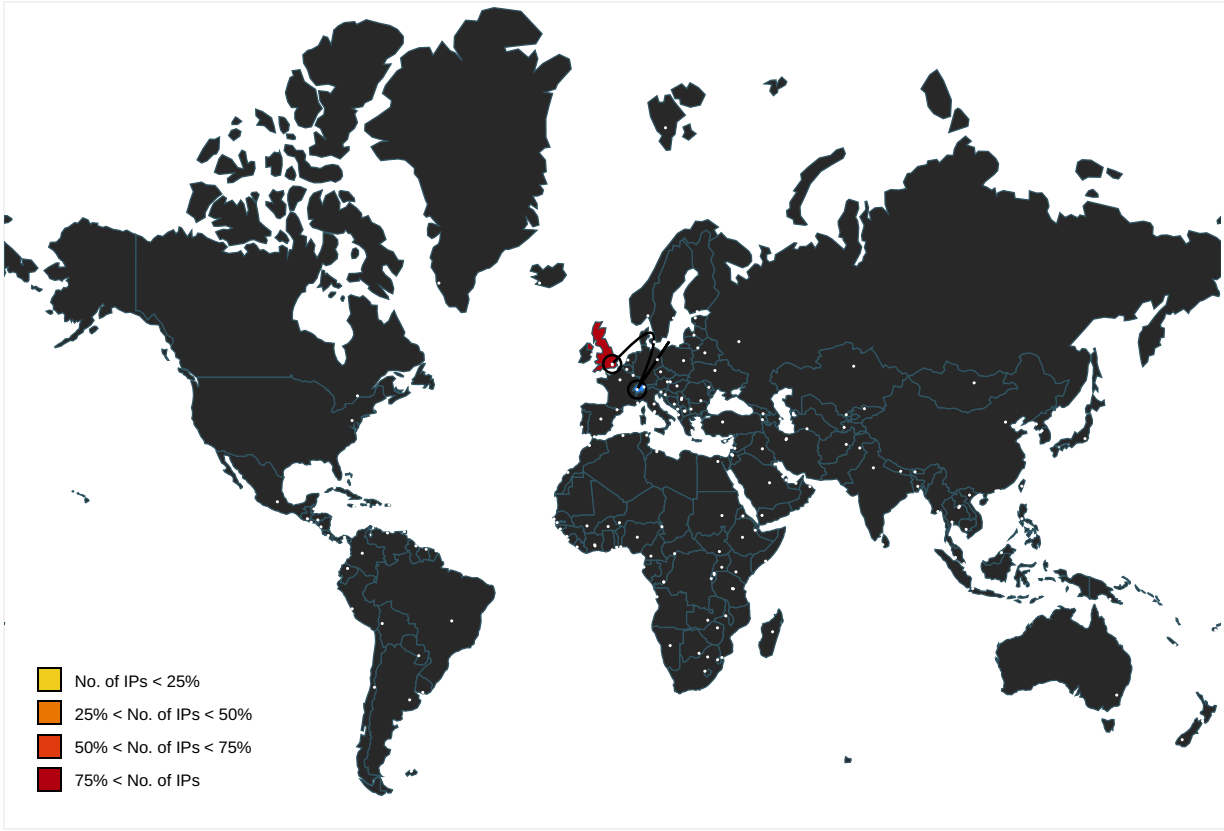
**No contacted domains info**

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.aiim.org/pdfa/ns/property# | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://cipa.jp/exif/1.0/) | AcroRd32.exe, 00000001.00000002.385710595.0000000009150000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/i | AcroRd32.exe, 00000001.00000002.396410708.000000000B170000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://ns.useplus.org/ldf/xmp/1.0/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.aiim.org/pdfa/ns/id/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.osmf.org/layout/anchor | AcroRd32.exe, 00000001.00000002.381352458.0000000007970000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/G | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.aiim.org/pdfa/ns/schema# | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs | AcroRd32.exe, 00000001.00000002.381352458.0000000007970000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.aiim.org/pdfe/ns/id/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://cipa.jp/exif/1.0/)_1 | AcroRd32.exe, 00000001.00000002.395861240.000000000AF7D000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.brooklandsnewmedia.com | AcroRd32.exe, 00000001.00000002.397663107.000000000B35F000.00000004.00000001.sdmp, AcroRd32.exe, 00000001.00000002.399945552.000000000D79F000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.aiim.org/pdfe/ns/id/8 | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://cipa.jp/exif/1.0/ | AcroRd32.exe, 00000001.00000002.395861240.000000000AF7D000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default | AcroRd32.exe, 00000001.00000002.381352458.0000000007970000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.aiim.org/pdfe/ns/id/7 | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://ns.useplus.org/ldf/xmp/1.0/0/xmlns/ | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.aiim.org/pdfa/ns/id/P | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |
| http://https://api.echosign.comg | AcroRd32.exe, 00000001.00000002.399945552.000000000D79F000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/m | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/em# | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.aiim.org/pdfa/ns/type# | AcroRd32.exe, 00000001.00000002.398780493.000000000B547000.00000004.00000001.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.aiim.org/pdfa/ns/extension/j | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/es | AcroRd32.exe, 00000001.0000000 2.396410708.000000000B170000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://https://api.echosign.com | AcroRd32.exe, 00000001.0000000 2.399945552.000000000D79F000.0 0000004.00000001.sdmp | false | | high |
| http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ | AcroRd32.exe, 00000001.0000000 2.396552980.000000000B1BF000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://ns.useplus.org/ldf/xmp/1.0/t | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.npes.org/pdfx/ns/id/ | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http://www.aiim.org/pdfa/ns/field# | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http://www.osmf.org/drm/default | AcroRd32.exe, 00000001.0000000 2.381352458.0000000007970000.0 0000002.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http:// www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes | AcroRd32.exe, 00000001.0000000 2.381352458.0000000007970000.0 0000002.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http://www.aiim.org/pdfa/ns/type#N | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http:// www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn | AcroRd32.exe, 00000001.0000000 2.381352458.0000000007970000.0 0000002.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http://www.aiim.org/pdfa/ns/extension/ | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/ | AcroRd32.exe, 00000001.0000000 2.396410708.000000000B170000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://www.quicktime.com.Acrobat | AcroRd32.exe, 00000001.0000000 2.381352458.0000000007970000.0 0000002.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4 | AcroRd32.exe, 00000001.0000000 2.396552980.000000000B1BF000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://https://ims-na1.adobelogin.com | AcroRd32.exe, 00000001.0000000 2.385710595.0000000009150000.0 0000004.00000001.sdmp | false | | high |
| http://www.aiim.org/pdfa/ns/property#l/1.0/ | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http://www.aiim.org/pdfa/ns/schema#X | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/s | AcroRd32.exe, 00000001.0000000 2.396410708.000000000B170000.0 0000004.00000001.sdmp | false | • Avira URL Cloud: safe | low |
| http://www.aiim.org/pdfa/ns/field#y#festItem#2 | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |
| http://www.osmf.org/subclip/1.0 | AcroRd32.exe, 00000001.0000000 2.381352458.0000000007970000.0 0000002.00000001.sdmp | false | • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe | unknown |
| http://www.aiim.org/pdfa/ns/type#08-02-29/ | AcroRd32.exe, 00000001.0000000 2.398780493.000000000B547000.0 0000004.00000001.sdmp | false | | high |

## Contacted IPs




## Public

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

## Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Red Diamond |
| Analysis ID: | 324341 |
| Start date: | 29.11.2020 |
| Start time: | 09:01:30 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 30s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Invitation - Prime Minister of Israel.pdf |
| Cookbook file name: | defaultwindowspdfcookbook.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 40 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |

| | |
|---|---|
| Analysis stop reason: | Timeout |
| Detection: | CLEAN |
| Classification: | clean1.winPDF@15/48@0/2 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .pdf<br>• Found PDF document<br>• Find and activate links<br>• Close Viewer |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, svchost.exe, UsoClient.exe<br>• Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 2.20.143.130, 2.20.142.203, 92.122.146.26, 92.122.144.200, 51.104.139.180, 2.20.142.209, 2.20.142.210, 20.54.26.129, 51.132.208.181, 92.122.213.194, 92.122.213.247, 52.155.217.156, 13.104.215.72, 40.90.23.154, 40.90.137.120, 40.90.137.126, 40.90.23.208, 40.90.137.125, 40.90.23.247, 13.104.215.69, 93.184.220.29, 51.124.78.146, 40.127.240.158, 204.79.197.200, 13.107.21.200, 13.107.42.23, 13.107.5.88<br>• Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, a122.dscd.akamai.net, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, acroipm2.adobe.com.edgesuite.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, blobcollector.events.data.trafficmanager.net, au.download.windowsupdate.com.edgesuite.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, e4578.dscb.akamaiedge.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, l-0014.config.skype.com, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, armmf.adobe.com, a-0001.a-afdentry.net.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net<br>• Report size exceeded maximum capacity and may have missing behavior information.<br>• Report size getting too big, too many NtSetInformationFile calls found.<br>• VT rate limit hit for: /opt/package/joesandbox/database/analysis/324341/sample/Invitation - Prime Minister of Israel.pdf |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 09:02:28 | API Interceptor | 11x Sleep call for process: RdrCEF.exe modified |

# Joe Sandbox View / Context

## IPs

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

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| NTLGB | CHoyU.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | ggBNN.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | KKjNA.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | IFPoj.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | MXNYB.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | npmiu.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | sCpYf.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | sIdiW.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | UsBzT.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | VFznx.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | mGhdt.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | b6egewgab.pdf | Get hash | malicious | Browse | • 80.0.0.0 |
| | purchase order.exe | Get hash | malicious | Browse | • 80.0.0.0 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | http://post.spmailtechnolo.com/f/a/h2coVIte-PnQgGolAw1FlQ~~/AAH5oAA~/RgRhk9ssP0QiaHR0cHM6Ly93d3cud2F6cC5pby9kb3dubG9hZC82MTI3L1cDc3BjQgoAJyxWsV-4NRnDUhVzY290dC50YXlsb3JAdG1hZy5jb21YBAAAAG4~ | Get hash | malicious | Browse | • 80.0.0.0 |
| | 5wnaEGcbc7.exe | Get hash | malicious | Browse | • 80.0.0.0 |
| | Kpw6TB725f.exe | Get hash | malicious | Browse | • 80.0.0.0 |
| | EnkIyRDCVr.exe | Get hash | malicious | Browse | • 62.31.150.202 |
| | LWwoiTLRjW.exe | Get hash | malicious | Browse | • 80.0.0.0 |
| | Gt2YstXx3K.exe | Get hash | malicious | Browse | • 80.0.0.0 |
| | ForQuotation_RMS22100.exe | Get hash | malicious | Browse | • 80.0.0.0 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 820 |
| Entropy (8bit): | 5.663025080403339 |
| Encrypted: | false |
| SSDEEP: | 12:vDRM9SmmZiET0DRM9BqX3ZiEZDRM92MVZiEwnDRM9zyBhVZiE:7xAEGOZE9DhEUfeE |
| MD5: | AF636C031D644CC2910D88F8B998391A |
| SHA1: | CA4DCBEA84C0A582BE7F54130D21D362FF153B67 |
| SHA-256: | FF030CD9B4F7CEEB3B41027DDE8C93EB74B57134EFEC0CD50CC5E8FE45D50684 |
| SHA-512: | 3686F5B1BCCAE7F134888464CB16095AB2740BC1F363AFDD0E51044789E4A42CF7A15643285442B7B39913997D268D83A69DC141D338624ABC162204873C5BE8 |
| Malicious: | false |
| Preview: | 0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .c..$../....."#.D> .....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....g9.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .9.1%../....."#.D.Z.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....`c].....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .+.;%../....."#.D.....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....pd.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .<.r%../....."#.D".....A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....F..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 696 |
| Entropy (8bit): | 5.675400566434189 |
| Encrypted: | false |
| SSDEEP: | 12:V9z30pj9PQn99zz9PQpNH9zg09PQXH9zFZ9PQE:Xzkp9PQnfzz9PQRzz9PQNzz9PQ |
| MD5: | 1996F92288126C1C1E7291F477B9F885 |
| SHA1: | 474700BE367AD70BDEB48F4DBFFDD304AFA15F44 |
| SHA-256: | 34FB54D87E727CCA243D79E897E169A7748ED4BE5A955F97FEE77F396A148A13 |
| SHA-512: | 347CF56E34AA479D20B9A40175B382680A958A576AA598FFF97B514F4A3C9A056F6331133799AC23C925F3E20E9F476491273B351E4C02C27468C587B44AE9D9 |
| Malicious: | false |
| Preview: | 0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..(.$../....."#.D..;....A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....b.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .W..%../....."#.D7.]....A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....)(!.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....%../....."#.D*.....A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....T.0a.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..CZ%../....."#.D.`.....A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....^..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 984 |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0 | |
|---|---|
| Entropy (8bit): | 5.613578263617053 |
| Encrypted: | false |
| SSDEEP: | 24:tB4v41y5SBYvB4v4GSBMB4v4RSBcB4v4aSBEF:nMP5SBY5MBSBkMWSBUMJSBE |
| MD5: | D3E92C3E50395780B35958FA5900B64A |
| SHA1: | 97165E513F524665F65BA8EBA7E266DDF15F5969 |
| SHA-256: | 978DA9CC5FDA2F186082EB5061D1000BD8228B79F9263B6BD743D718887752DA |
| SHA-512: | ECAFAC952E28526C220C9658DF22390D7E90A37ED6B26ED81A5243C9D322D5054559D65B5FA68AC73DD27B246D3C84B043FCC12AE7CA8080B2233DE23D6CC<br>9 |
| Malicious: | false |
| Preview: | 0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....$../....."#.D.&.....A..hvDO.N.t@...<br>..n.*..... ....A..Eo.....A..Eo.....1.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-vie<br>w/selector.js ._./%../....."#.D[.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....c!.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/track<br>ed-send/js/plugins/tracked-send/js/home-view/selector.js ...;%../....."#.D.I.....A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....zD.!.....0\r..m.....v...n....._keyhtt<br>ps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .S.p%../....."#.D.....A..hvDO.N.t@.....n.*..... ....A..Eo.....<br>.....A..Eo.....j..... |

| 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): | 5.701812754582569 |
| Encrypted: | false |
| SSDEEP: | 6:mNtVYOFLvEWdFCi5RsA/RVSiWulHyA1TK6tkF/MNtVYOFLvEWdFCi5Rse55yiWuD:IbRkiDVWussy/ebRkiDp53Wuss |
| MD5: | 6E2D873D17C99847CAF42676A6D17AE7 |
| SHA1: | 26D4C39750D07BD4B585056A44F423C2D3467DD6 |
| SHA-256: | 2106D6F63812E930D829ABD01BBB19C02703F3F77FD29ECA952C6EA1B3FD7574 |
| SHA-512: | BC2245ACB70BFCC2145B511CBD677FC48036D1DEFEDA96BA698494C139B01882702D566FB8537596ACB8D83CD62AE4716FF84AB674A0126ECB114FFF8906377 |
| Malicious: | false |
| Preview: | 0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ....$../....."#.D.....A..8 P..a...R..Y....7.@..2Dm{<br>..A..Eo.....A..Eo.....tN.1.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .M5@%../....."<br>#.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): | 420 |
| Entropy (8bit): | 5.570426096411107 |
| Encrypted: | false |
| SSDEEP: | 6:m+yiXYOFLvEWd7VIGXVuHMxdPVyh9PT41TK6t7flM+yiXYOFLvEWd7VIGXVuGQpx:pyixRuxsV41TE5fl7yixRuN0AVV41TE |
| MD5: | F6DC72F99CD2B391316BC5720E9CD2C3 |
| SHA1: | 603BF683362E1A84CBE96B24C2C7CE8C156C3D9C |
| SHA-256: | 600441EF6847D7DA0EED13EA24A08A48055B439B9E3EF88C5DC06703070D29A4 |
| SHA-512: | A44AEE053722983347C65C8F98E4AAA857573AEC5AFA5C294D86C3810A0598DB0E99C7F86D70EE54626F67043CC7389ACB75A43809D122A654B8B5DA0FCC848 |
| Malicious: | false |
| Preview: | 0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..r0%../....."#.DF.....Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.<br>.....m.O{.....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.....<br>.....A..Eo.....Xb.X..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 432 |
| Entropy (8bit): | 5.624017159916301 |
| Encrypted: | false |
| SSDEEP: | 6:mvYOFLvEWdhwjQ9bqlDLZIl6P41TK6tg9/l2vYOFLvEWdhwjQud1oLZIl6P41TKQ:0RhknDLZCOyRhkd2LZCF |
| MD5: | E7264887C2597A6F620B0CAAED9A001B |
| SHA1: | 1FD9310868F89D08B1D0557C3948723619841A2B |
| SHA-256: | EFED8259257EACCC2E7C193ED57B83E5443E9E06C1F4FF226F22DFF2DE5CABE7 |
| SHA-512: | 52C705F87492B16471D80E37C0FC791E79866E924C983DD2A72AA5F98ACC7F759973AE6FE132BCD8BBC73431DAFBE17FD4447DCF54A6C2C24073C5F34709C5 |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0 | |
|---|---|
| Preview: | 0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...+%../....."#.D.....A.].>....uUf..N...k.....c..l.A..Eo.....A. .Eo.....r[.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .@:m%../....."#.D.....A.].>....uUf..N...k.....c..l.A..E o.....A..Eo.....p..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 418 |
| Entropy (8bit): | 5.538133878932782 |
| Encrypted: | false |
| SSDEEP: | 6:mJYOFLvEWdGQRQOdQzDSpg76g1TK6t2KllEJYOFLvEWdGQRQOdQrXYtlt3E06g1U:2RHRQCQP71U+ORHRQC1R91i |
| MD5: | 9B74AE99B3DD816D53049294C0126DD8 |
| SHA1: | 5A45A2A343BECEFF3B3AF96C1D56EE5B7CB80986 |
| SHA-256: | FDF5FCEF0743D800E1736F10B43F006FC0C0D73295BC0B6CB9C73F8699F83433 |
| SHA-512: | 168B5D0F819B88B3ABE6AA185260F9E7472918BCA99F08BB2056DBAF2092678A0E0B0E857CF4A1539D0C540102D39A45878E23BF622501BB009EE73B4BB13583 |
| Malicious: | false |
| Preview: | 0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .u.1%../....."#.Dh.....A..c..y/L....\|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...r%../....."#.D.....A..c..y/L....\|y.n..C/I.....X7-ne.A..Eo..... ...A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 716 |
| Entropy (8bit): | 5.629157379146751 |
| Encrypted: | false |
| SSDEEP: | 12:Z5MZMzkhMuR/E1h5MGUMuR/Emwr5MLuMuR/EZJ5MixMuR/E:ZS2zkmuR/ErSGNuR/EmwrSLfuR/E3SFn |
| MD5: | 3B31DB1A919F350B68A71A1CCD144358 |
| SHA1: | 0CC1F376F8AAC55554ACDC8E5B6AB87129A87928 |
| SHA-256: | 491E9EC389B85A43BA29F6E534E98DE019A78B38F0AB1427EE41AD13DF03F0C7 |
| SHA-512: | 9EC0F70C0CCFE170E5498F130966255E46FBE8C5756080D51BE51CCB26A5223EB31B22D54EC65BD0DCAACC719635D64A63A5F596186944A1732E884046B0AB2 |
| Malicious: | false |
| Preview: | 0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....$../....."#.D.H<....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 ..".%../....."#.D..]....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....\.....0\r..m.....3....<lb...._keyhttps ://rna-resource.acrobat.com/base_uris.js ....%../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....J._.....0\r..m.....3....<lb...._keyhttps://rna-resou rce.acrobat.com/base_uris.js ..sZ%../....."#.D.....A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo....."M.O..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 212 |
| Entropy (8bit): | 5.6061326523080774 |
| Encrypted: | false |
| SSDEEP: | 6:mGpYOFLvEWdzAAuqhSm0bbsIDMGH41TK6tl:XfRM+KsIZEz |
| MD5: | 3339A670F8B6C0B88B15F3AD298A5E08 |
| SHA1: | ABABDECF0A80525469564BC15B381F094D194D30 |
| SHA-256: | D19DAF10750D9836F72AB084C3161186B02C57843457CEEEDED04D3F2A50366C |
| SHA-512: | 378749F2D3D310B84BC8FFA21633EE58FE28EFEC6577805E9EF7E8367169F3B1D575161B757317898E9C72D69408A2C39A818302078E01A4D5A13A90AD248193 |
| Malicious: | false |
| Preview: | 0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .[7B%../....."#.D.....A..`.....^....L>..Xa./.....C.y.A..Eo.....A.. Eo.....4'A..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 428 |
| Entropy (8bit): | 5.569439572091551 |
| Encrypted: | false |
| SSDEEP: | 6:m4fPYOFLvEWdtuuo9eqJby0zBUKSAA1TK6tb484fPYOFLvEWdtuFDDby0zBUKSAk:pRWbeB4DRObe |
| MD5: | 2A0418DB53B9B4DE48C714AE3312FC8B |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0 | |
|---|---|
| SHA1: | 8E9267346A943ED90637F21C49A2C6CC7E80A8BC |
| SHA-256: | 4EFB007F6CB16B033C3642CF3BC64D68CA3DD1344D3F3F9B3600624BBBB048C0 |
| SHA-512: | 648E80E90DB93348D46AF43F7883272877A877BD0FA120D206DF6CC9878B30EC95D3103E1B0984505B77656B4B1B003DE0C5DDAD3DAF1D4735097CABC68A428 |
| Malicious: | false |
| Preview: | 0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...2%../....."#.DZ.....AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....<br>.....A..Eo.....0\r..m.....V.....\_keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...s%../....."#.D0.....AQ..E.=....=h`t..t..3%A.F$<br>..w..A..Eo.....A..Eo.....?..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 708 |
| Entropy (8bit): | 5.648467155172093 |
| Encrypted: | false |
| SSDEEP: | 12:KkXxKMSCvC2xPtUlJwkXxKMSCvbqtUlx0kXxKMSCvqJy3tUlTkXxKMSCv5tUl:KkXxiC6yWJwkXxiCTqWx0kXxiCs4WTk+ |
| MD5: | 6D54FA5896FD8AF4657539F0CE12682D |
| SHA1: | 07CF65B3DA563B5083D47AC08B61F7D9E915220D |
| SHA-256: | 7C428740AECE7EECF3F676033561CD4D4CD835716208677953F895277CC1E319 |
| SHA-512: | 0C90AF68FA7F848E27ABF03F27841EA720D03FCDF8F91224277B2A96D25785F7B952AD6FF523AC5709485A29D869AA688D17897A201C44BEDE5528EB55766541 |
| Malicious: | false |
| Preview: | 0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .v+.$../....."#.D..;....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....C.....0\r..m.....1.....5...<br>._keyhttps://rna-resource.acrobat.com/plugins.js .2 .%../....."#.D.]....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo....."".....0\r..m.....1.....5..._keyhttps://rna-<br>resource.acrobat.com/plugins.js ....%../....."#.D.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....B.....0\r..m.....1.....5..._keyhttps://rna-resource.a<br>crobat.com/plugins.js ..qZ%../....."#.D.w.....A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Y..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 748 |
| Entropy (8bit): | 5.627499010443845 |
| Encrypted: | false |
| SSDEEP: | 12:5h6OLJ8akph6OLv1Ukjh6OLz/nkCh6OL07k:5h6vvph6Wjh6u/kCh69g |
| MD5: | 5A45D6FC58D204982292C8BAB6F594E6 |
| SHA1: | E27E1423D288F428F0CADEB9C76B9A0C4539DDE1 |
| SHA-256: | F99ADDACBF80D4A47965233B00BA5C97B4CDD03626B14045C309D48E5D2A6B35 |
| SHA-512: | C392228317DE519D5CA652AC25DD2EF48B70389657883F1B72F12C57AC9B8A357EF0AE1CE8A02E428E2B11FE855A656631B33D9FC9EA098B8183DDA6FDBB672<br>7 |
| Malicious: | false |
| Preview: | 0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....$../....."#.D.Et....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....m.....0\r..m.....;..<br>.I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .AS(%../....."#.D.....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....0\r..m.....;...I....._keyht<br>tps://rna-resource.acrobat.com/static/js/desktop.js ...2%../....."#.D.v.....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....,.....0\r..m.....;...I....._keyhttps://rna-resou<br>rce.acrobat.com/static/js/desktop.js .n.i%../....."#.DG.....A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....q..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 976 |
| Entropy (8bit): | 5.657140206630935 |
| Encrypted: | false |
| SSDEEP: | 24:UB4v4eivwzXLnxB4v41+wzXLnIB4v4XCwzXLnvB4v4WwzXLn:8MtbnrMerbngMubn5MGbn |
| MD5: | 3561E143A559266CDE634163994ED7A6 |
| SHA1: | 99214A1A90E23D7C7017731B1421FB4A05CB1194 |
| SHA-256: | 558CA8C73AC0779BF326F3D4D9E4307FC1A0A53E33DAC74A41DE4B49BD305A1E |
| SHA-512: | 39272E59CD17C6FCD3A09AAD942C0A3D389DE95AC2227C7E3531A292485B2C87A79FFDC52B888CA739B3F4FB0E9B257CB01E2D7CCBDBE930C3F41560DF73E<br>AE |
| Malicious: | false |
| Preview: | 0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ..N.$../....."#.D.c.....A.....H...{...2.<br>./.k`..r4.C. .A..Eo.....A..Eo.....k.....0\r..m.....t...R.1<...\_keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-<br>view/plugin.js .Bo1%../....."#.DF.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....r.....0\r..m.....t...R.1<..._keyhttps://rna-resource.acrobat.com/static/js/plugins<br>/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...;%../....."#.D._.....A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....F+.....0\r..m.....t...R.1<...\_ke<br>yhttps://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.....<br>.A..Eo.....Q.w..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.548970234652054 |
| Encrypted: | false |
| SSDEEP: | 6:mq9YOFLvEWdzAHdQ0Y9U45GFCaa+41TK6tb:NRMHdK5Gda+E |
| MD5: | 54979AB7691BEE18530166820518C87C |
| SHA1: | 5D49E4CF7776001C7AA44C6EC31CC16ED54A5C62 |
| SHA-256: | 2F24E0CE23C86155D004CCD26BF2DAE3B8A58E3B1205B330033F1A5E3B3307D1 |
| SHA-512: | 427E170EE8AB3235938416C00CF97606A94690358767A6FD8434586482026B2B8F0992649174EDC3A0594DDD30C49DFF1E5B700D57E09F07AA96886FB95594EB |
| Malicious: | false |
| Preview: | 0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..8B%../....."#.D5.....A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....T..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 422 |
| Entropy (8bit): | 5.528637553790728 |
| Encrypted: | false |
| SSDEEP: | 6:ms2VYOFLvEWdvBIEGdeXugER11TK6tRs2VYOFLvEWdvBIEGdeXuEqCXY11TK6t:BsR2Ese8PMsR2EselXG |
| MD5: | ECEE6285165E88803D6C5020393BBB0C |
| SHA1: | 1870E50F98BB9ACF0FF8F101D45B3D5458D4193F |
| SHA-256: | 1D424A6FACEEACE1A7F8005261D5A54D86C4F18E525CEE9E1711B36D801B80FB |
| SHA-512: | 6AD5A5A45AEB4F8DF0F0274FEF0E9E5E339C687913439DB9DD7B3EFDC90003FF90C7698C03D6ACE41AEB156EC120A140B02F51E3C08F5279670E2D99AD4948A |
| Malicious: | false |
| Preview: | 0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .. 0%../....."#.DI.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....y$f6.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .U#q%../....."#.D.V.....A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 404 |
| Entropy (8bit): | 5.6643571495715745 |
| Encrypted: | false |
| SSDEEP: | 6:maVYOFLvEWdwAPCQZrXHB7OhKlvA1TK6t++aVYOFLvEWdwAPCQ3lHmB7OhKlvA13:RbR16K1Jk4pbR16HJk |
| MD5: | E8D71D7B18C00DCF40DF976315FC8D5D |
| SHA1: | 16A5ADCD1A7E8E1674B4CA8ED12C1EB13849A9BC |
| SHA-256: | 27CCF008F929AA0906F311CF9E66C16196961712F8BE874CA2238FB171BD9411 |
| SHA-512: | A2811D2F74128385184DE022270E2D8DBA705196A1348BBE63732231F09448401BB9E88B7E34D54207BFAD9C45D9218D4708E4DD7CC8EF5EF76CC52F4D824D1 |
| Malicious: | false |
| Preview: | 0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...+%../....."#.Dq.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....<.:.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..5m%../....."#.D.s.....A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....$X/..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 422 |
| Entropy (8bit): | 5.56201580130646 |
| Encrypted: | false |
| SSDEEP: | 6:ms2gEYOFLvEWdGQRQVuhXlKjQdFt1TK6tuF/Ms2gEYOFLvEWdGQRQVuMbqGQjQdb:B2geRHRQMQ08T2geRHRQS0/// |
| MD5: | 0703F2B346B4379F0B8AF5CCD54D88C1 |
| SHA1: | E8A4532B5E9379A01D144CC2D7C3E30548A37FAA |
| SHA-256: | ACE3F286C64166DF678DDBA2B6E1BC1BE07CF043F39B98D518DF8FD12058F3C3 |
| SHA-512: | 767B5CFB4DE6762846FFFECDDACC8055B8C0A1BC9954F74817F7742461C9D1A2A566652D967C6B884DC21AC667BF10CFE093CCA4665DCE29573727CE3EA0743 |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0 | |
|---|---|
| Preview: | 0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .b./%../....."#.Dy.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .5!q%../....."#.D.A.....A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....+o..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 824 |
| Entropy (8bit): | 5.645432627768767 |
| Encrypted: | false |
| SSDEEP: | 12:WyeRlo3t1w/+yeRliBSt1wQMyeRlSt1wdmyeRl91Vowt1wMB:WJgfw/+J7fwQMJafwEJphfwm |
| MD5: | 4A3FA578EA92355EC031F07FC4E8E3DF |
| SHA1: | 9A01A676F5C3650E1BF97B95E11563DC50A964C5 |
| SHA-256: | 246FFB426B4BCA5F1047FE1843A166CA5FB455E9BE611E02EAE8524C270D87D0 |
| SHA-512: | 8FF48DC9D9BF8324A6439FD93038A788DDF27858382C0E7D3170092D6593751A1C5A6681972B445270511414C6190514FA980F8EA063D3D1CE5C5BAD7839AF7C |
| Malicious: | false |
| Preview: | 0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .v`.$../....."#.D..{....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...)%../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....Y.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .kr5%../....."#.D~;....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...j%../....."#.D.....A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....:.D..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 436 |
| Entropy (8bit): | 5.57021784546122 |
| Encrypted: | false |
| SSDEEP: | 6:mnYOFLvEWdhwyuj9WQIqwK+41TK6tC8nYOFLvEWdhwyup092qfyIqwK+41TK6ty:wRhkxwK+EHRhIPhwK+E |
| MD5: | 22F765CDA26BA57EA5550B52F7066541 |
| SHA1: | 1126437811F052CDA6F771418F509DB813E5651B |
| SHA-256: | 8384793AFF9BE14A78DD84927FF384E527170ABE9B5D946696181CA618C6F940 |
| SHA-512: | 5AE7E372EB147E8874E1A9D91CBBAEB31D26441EB57A85BCC8A00BFC6F240C5EE17F5D05AFDD647BD32AD572BC2CA2C109555BEF8C9C1319951AE381B1307A6 |
| Malicious: | false |
| Preview: | 0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .|.+%../....."#.D.I.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....I.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .&.l%../....."#.D5A.....A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....lnk..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 920 |
| Entropy (8bit): | 5.648501959532308 |
| Encrypted: | false |
| SSDEEP: | 12:/RrROk/mfLE43RrROk/iZfLEGRrROk/WE8mfLEeRrROk/a6fLE:/PJ/m443PJ/u4GPJ/d8m4ePJ/b4 |
| MD5: | 38A5A501B3EA2144D22AB1B0A6046682 |
| SHA1: | 1E3C2DC2EF45E58F116EB1B2FE416E1B4ED70475 |
| SHA-256: | E849174CC20DEE64E507A022E801F9F71DB8123972D6BFC7C07C9766A3C55E22 |
| SHA-512: | 4C87CFE3975FAC6307F0AA55F46C3F302A95A2E954C49D694C0A881FDEC79635949BA9FBC827882445CED673868788D14E757682F560DADF705DEBCCADCD19F |
| Malicious: | false |
| Preview: | 0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .}&.$../....."#.D0.{....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 .f|)%../....."#.D.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....I.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..65%../....."#.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 ...j%../....."#.DW.....A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....IU..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 744 |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 | |
|---|---|
| Entropy (8bit): | 5.617671764333004 |
| Encrypted: | false |
| SSDEEP: | 12:xqToNCPLngjqTg64NCPLn+ZqTp0zNCPLn5BqT7NCPLn:AeMnfchMnlQMnC1Mn |
| MD5: | 4176AA638810910BDD8CE8944B7BEEFD |
| SHA1: | E2DC468FED109E8437187805A7453836776490E2 |
| SHA-256: | 235C6F284F64EB6427E8E6EDFDE097D3E446FB19F154755428138169895E48BD |
| SHA-512: | 1418F6AA0A3A99EA3E20EE63A6B387BA94264DF80ED1AE1C778B28C6E3A09D463B3CCE63945A94B1E3E6688DCAB7EC698DAC7CD173F8C43E6C91948400199291 |
| Malicious: | false |
| Preview: | 0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....$../....."#.D.5t....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....1.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..D(%../....."#.Du.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....\.....0\r..m.....:....f....._key https://rna-resource.acrobat.com/static/js/config.js ...2%../....."#.D.n.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....2}.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...i%../....."#.D+.....A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....f;~..... |

| 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): | 828 |
| Entropy (8bit): | 5.696312668262038 |
| Encrypted: | false |
| SSDEEP: | 12:zRMFK+oQZsDwBRMNsDbXRMW6sDRRM+TxsD:z6oQGD0bDbXpDRAD |
| MD5: | F682117439CDFF8015147ABBDC293FE2 |
| SHA1: | D771B82229C3BC0A0ED9E4C5522C5D4A075E0121 |
| SHA-256: | F3755B305FE4DF7A4AD31A0FBCE5924D0A45CB2FE7800A3C019CC028C94B32D2 |
| SHA-512: | 262FECD130326A72067C3A8AC08437E4FB62563B08B54D596AE28944EF19BE0B110CD3002F32032E96309AB377B959368DDA4668D995FA0ED96FCC1BA307697E |
| Malicious: | false |
| Preview: | 0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ....$../....."#.Du.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..'0%../....."#.D.M.....A..z._a...'.v.....4p3..1.']...A..Eo.....A.. Eo.....;.@.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...:%../....."#.D.....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....t.$.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..(q%../....."#.D .....A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 840 |
| Entropy (8bit): | 5.629332953365433 |
| Encrypted: | false |
| SSDEEP: | 12:6lJRqIoMmClJR1GXJJoMgclJR0soMjqlJRYeBWRoMN:YNoM1qoMrmsoMjoaBRoM |
| MD5: | 05FD7A8239FDD4A438AFE16A93C40F4E |
| SHA1: | 68BC9A86B8B9C5B2333B8064539499720353D974 |
| SHA-256: | 54AB982D6E724D9C8E013D9C14D7377911686C285B2DB3109670CBDBBAB2D967 |
| SHA-512: | A05916370624908E6F169663A05FE61198F2E71E25801A8E3B297D70C86E469C6314F30BEEA5ABBC3FA99138B6B5F6EABF86481941B6DF5F47E110ABBFCDA391 |
| Malicious: | false |
| Preview: | 0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ....$../....."#.DU.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo .....4..#.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..n0%../....."#.D.v.....Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo..... .....A..Eo.....R.M.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...:%../....."#.D./.....Ac}.H7M=M..-.....Ix..R.I. ..}Rl.$q.A..Eo.....A..Eo.....2..^.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...r%../....."#.DM.....Ac}.H7 M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....Oz..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 892 |
| Entropy (8bit): | 5.651980617786554 |
| Encrypted: | false |
| SSDEEP: | 12:F8hRrROk/r2L8hRrROk/A1YQ2G8hRrROk/MC/2Sn8hRrROk/dq62:UPJ/r2ePJ/gYQ2bPJ/MC/2SSPJ/dq62 |
| MD5: | 2529F0523022FD6C00C9FC646DAD9DE1 |
| SHA1: | B59622CB0C94B01C5248A10C1C6A145BA5F0CC4A |
| SHA-256: | 5426D33906ED5D14F15C0E11070F21CE8776030AF079C937461B73AFA327B53E |
| SHA-512: | 38C5BF5FD60C139712B46A0E234356666472A1CFF000EE7A3BAD0DAD64E3248CF19B6AB43943CF06A33266620A5219C299C952D69827C1F30F3CD51912E6F402 |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 | |
|---|---|
| Preview: | 0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .Z..$../....."#.DG.{....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....4.:>.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..n)%../....."#.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 .{.5%../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....R.%.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...j%../....."#.D.....A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....:..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 852 |
| Entropy (8bit): | 5.711160516972116 |
| Encrypted: | false |
| SSDEEP: | 12:ehRc0QNJICa4hRcK5NJICs4hRcGT/5NJICvhRcfNJIC:ehYJICLh9vJICthNT/vJICvheJIC |
| MD5: | B5C947A0F3B2DF9A825999B4932E8C3A |
| SHA1: | 5D0BF5A535A7C3AF022FBA465B81FEEE6E20E57F |
| SHA-256: | DD7D872A7F7411F55871E1883F66EFE4A6C239161CF14A9121CFAE11D6712A3A |
| SHA-512: | 50E8FC86680D1D5ECE0B92D87321B413E2A0963139521A9DF0BDBD6B391A3417A992B16CECC9CFA334F0A37C29F1D17D2F0768899934A9A81F874C182537645A |
| Malicious: | false |
| Preview: | 0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .]f.$../....."#.D..\|....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....4.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .z.)%../....."#.D\>.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....~.Nm.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..t5%../....."#.D.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....}.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .f.j%../....."#.D1~.....A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....6p_]..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 832 |
| Entropy (8bit): | 5.644810589497441 |
| Encrypted: | false |
| SSDEEP: | 6:mOEYOFLvEWdrIhuiJXebxhLzgm2d/1TK6t2OEYOFLvEWdrIhuhDkfrhLzgm2d/1X:0R9ZReiRUfrZReaRF8hZRegRr6RZRe |
| MD5: | 8649ADD7CBBE269C9661BD046758DBD4 |
| SHA1: | E6C44575DB0719234DCE0270EBA5B98FB2BB94FB |
| SHA-256: | 9C78D0A8E65B44E4E0561774026E110DCF3CF16E5608F461C69D6C1B713CFCC6 |
| SHA-512: | 003D933C51DB6A756C05D26B615903B12500095E479FFDDCB62D81FB658CBB68BDBD7C6F7C557164DEC13B0CD046C9AA5EB91CBAB06EFC639008A8B8C5E3098 |
| Malicious: | false |
| Preview: | 0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .k..$../....."#.D..x....AZ.Z}Q..4.o....0+..[\|..n:*..U.W.A..Eo.....A..Eo.....+x.z.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..E)%../....."#.D.....AZ.Z}Q..4.o....0+..[\|..n:*..U.W.A..Eo.....A..Eo.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...5%../....."#.Dgc.....AZ.Z}Q..4.o....0+..[\|..n:*..U.W.A..Eo.....A..Eo.....^.P].....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..j%../....."#.DHQ.....AZ.Z}Q..4.o....0+..[\|..n:*..U.W.A..Eo.....A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 752 |
| Entropy (8bit): | 5.677267067665749 |
| Encrypted: | false |
| SSDEEP: | 12:6JJK5OI8wJJK1foIwJJKdPIqJJKgfChI:6JI5VBJI1HwJIdQqJIDK |
| MD5: | 610D0F9601CDC54B20F4D972F732ECB3 |
| SHA1: | 6992E1D8302DA607B8AA159FF2D6E57CDFB8DF9F |
| SHA-256: | 0ACE602CB54A865B8A98AA47049C9F5F7302CFE3B2A4918F94DAB4521D47C7A6 |
| SHA-512: | 318B078EDBEC4E939AC8C5C06C0AC0C47E8300B47A3E51B14315958C08D3EFBD5004A8B59C8B7F8BA9C84662E295BBC99F1606CA20939197E3492EB92AFF1C1 |
| Malicious: | false |
| Preview: | 0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .).$../....."#.DT.P....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....P.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..W.%../....."#.DF(y....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....w.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...!%../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....J./.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .S.]%../....."#.D.....Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....I.)..... |

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

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 428 |
| Entropy (8bit): | 5.653088637634913 |
| Encrypted: | false |
| SSDEEP: | 6:mWYOFLvEWdBJvvunYXt+HyhUDLYtmOZn1TK6tZXMWYOFLvEWdBJvvuJTN4yhUDLE:xRBJsqIHDcFZLvjRBJLHDcFZL/ |
| MD5: | CEE7E2B2A1FCDA979B610431FE9C3109 |
| SHA1: | 585848EF08AFEBE9C48CD1286F954054E34E40BF |
| SHA-256: | E69198B26D7DB00C5D7AFB66691AB9CE5CE129A05B895D8A0A31A0C9034F2877 |
| SHA-512: | E1B7587278CF472D77A38FC663DB456C0108DE05395F4631A62B217EB485F8089B922F177C6DCD8A65E3FA90C373E01039706BAF61D1345FA96727C2C44537AF |
| Malicious: | false |
| Preview: | 0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .\|$0%../....."#.D,+.....A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A ..Eo.....bj.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ."q%../....."#.D.r.....A....t.q..W.EZ....1...[.zC.7mD..A.. Eo.....A..Eo.....G8Xo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 844 |
| Entropy (8bit): | 5.685344461641282 |
| Encrypted: | false |
| SSDEEP: | 6:msRPYOFLvEWIa7zp7D/65VPu1TK6tCesRPYOFLvEWIa7zp7VXivVPu1TK6tHesRe:BPHhAcqPHGcXPHKRcGPH4T7c7f |
| MD5: | 20C0676E24B14625E4109455DFD10AB1 |
| SHA1: | 82C90BDB94153B99D2F875B373C13884FCC8AD4F |
| SHA-256: | 85CDAEF95C21758CE556BDB6487B8AE323716B8427A03F08E7078F4B9042F4B5 |
| SHA-512: | E03CBA4B6699F22AD29FFF05D27CA89053543BFB887369FD2AD3458A8045D257038FA7940415C210044F98BD5DBF34169C2BE3A8852C892C440950D8C62B80EA |
| Malicious: | false |
| Preview: | 0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .D>.$../....."#.D.<....A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo .....8.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .4$.%../....."#.D..]....A...L...Im.@.....E.nW...IP..A..Eo..... .....A..Eo.....FI.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....%../....."#.D(.....A...L...Im.@.....E.n W...IP..A..Eo.....A..Eo.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..uZ%../....."#.D.....A...L. ..Im.@.....E.nW...IP..A..Eo.....A..Eo.....+..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 416 |
| Entropy (8bit): | 5.625243934963749 |
| Encrypted: | false |
| SSDEEP: | 6:mKPYOFLvEWdENU9QYDv3NiM3Y1TK6tnKPYOFLvEWdENU9QN9tXFdiM3Y1TK6tO:bJRT9vNr0kJRT9W9t3r0E |
| MD5: | 7BC4E7A6B608BBD3CC8859107025F83D |
| SHA1: | 77EF9C4158552044D8D9A0D3AD3F86A9C913EC01 |
| SHA-256: | 6B89B0ED9B7063ACE51318DE4D34E627650C5D5C91E5337966EA321380A69F84 |
| SHA-512: | 70CC1F2DD5692E1021A329CFEA2F3BC92DF98D6459C54FBEF24EDE20C077634A0F56EC066970A3CFEDA4AEF24CC142FAC2FDA3E74B2E56A8C3132983D90B2 F3 |
| Malicious: | false |
| Preview: | 0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...+%../....."#.D.3.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo. .....C.1.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..8m%../....."#.D.....A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... .....A..Eo.....Y+..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 416 |
| Entropy (8bit): | 5.614505485644331 |
| Encrypted: | false |
| SSDEEP: | 6:mQt6EYOFLvEWdccAHQlBL0jBRCh/41TK6tP+Qt6EYOFLvEWdccAHQ5rqqoZVGjBf:XRc9Wh0Di/EJ/Rc9KrJDi/E |
| MD5: | 6A5FF1E9C2BA47EAA8AA3C0882DB0CB7 |
| SHA1: | 7C9D7C6DC304E282B2133756F32B7FA42B75C1DC |
| SHA-256: | C62828B83B4FC53750B79DF10C4F47CB89514AD652B2BA3AD2501AA5152A4CA5 |
| SHA-512: | BCE98CFF9A9861F374C53E57F3E0B2034519F144B457B03C78E7BDCB43FD7832AAFB6EAF4854D850721FCA9631E568D157987EC4B526592139C1B21F3F771BDE |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 | |
|---|---|
| Preview: | 0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .@q1%../....."#.D.@.....APJm...0x.x..RD...BB!@5..<..]....A..Eo.....<br>....A..Eo.....iEz.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .L.r%../....."#.D.....APJm...0x.x..RD...BB!@5..<..]....A..<br>Eo.....A..Eo.....!T..... |

| 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): | 5.6257557989373 |
| Encrypted: | false |
| SSDEEP: | 6:mqs6XYOFLvEWdFCi5mhuY5nwULlF4r1TK6tjEqs6XYOFLvEWdFCi5mhuVVSu+ULs:bs6xRkiWpLlF4nTs6xRkiDLlF4n |
| MD5: | F22B3B6ED4449E159EA693363D582DB9 |
| SHA1: | 60BC707F0A22801F1F4E1F5F56400D9230B40BDD |
| SHA-256: | 8A97CF303EDF0FB46063C3CC6F18835D0D22B9AB371E878699B0EE94137BEF92 |
| SHA-512: | 77C85D50F38839A3573BE4F9EB3B0E1614821C85A67C6E1790B9B6865597C324FA655E3BF832042D003472B060ECEA4E40C3376B60337C1627A59A6ACDD8A763 |
| Malicious: | false |
| Preview: | 0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....$../....."#.D^J|....A.P...#4..l....5...5..).w.. .h.~..A..Eo.<br>.....A..Eo.....v.m.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .._6%../....."#.D.....<br>A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....Q..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 430 |
| Entropy (8bit): | 5.550569201703456 |
| Encrypted: | false |
| SSDEEP: | 6:mhYOFLvEWd/aFuFptk941TK6t1EhYOFLvEWd/aFu00qNhT941TK6tL:WR169EkRexhT9Et |
| MD5: | DC7F1A732086CD7A5B811226DCBE6910 |
| SHA1: | 2B83940408EEFAC31EABD41072505319A7343DD4 |
| SHA-256: | FB81BF2442800423086F5303C3F55F30A709E652F792457772CB8DB551227188 |
| SHA-512: | F527D4C392AC327245FDEC16539C64557D19E1E425EB3793473ECCA99A5D4655B69080BD21DEBC81FC7A5FBCB23B553B4A4686144B3EBCCB5B3FA544229AC9<br>C |
| Malicious: | false |
| Preview: | 0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...2%../....."#.D.....A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A.<br>.Eo.....c..1.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..$s%../....."#.D.3.....A...a.f.m.i.o.p..3U5.....^...I.A..E<br>o.....A..Eo.....R..X..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 416 |
| Entropy (8bit): | 5.55533562511296 |
| Encrypted: | false |
| SSDEEP: | 12:2DRuRM6AQooB9Vd2kFYDRuRuoB9Vd2kQ:8n63VbdT8UbdTQ |
| MD5: | AA4A69820E005B631915C63695F9E64B |
| SHA1: | BCB43E4E5C85CB06A919C7FCD4A7E3ADCB637773 |
| SHA-256: | 18FDCF55CC2D54BFE5C24972AE500035F9A190D1181A6E4D02374E57FD26FAB7 |
| SHA-512: | 5761A9E96004CB643636902A336178FE3556248C8504DEB1BBF8955B810DEAACAF6DCC24B828AF60BE57FF707FE845FDCF124BE6B9B151DCADEE5DB6CAA52E<br>7D |
| Malicious: | false |
| Preview: | 0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...2%../....."#.D.e.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo..<br>.....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .+.r%../....."#.D.....A..y.$..$.v5j...T...z.]..._S....A..Eo.....A.<br>.Eo.....BK.A..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 832 |
| Entropy (8bit): | 5.616852384017715 |
| Encrypted: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 | |
|---|---|
| SSDEEP: | 12:+RQgzrn22RQ5PzrnZWRQ8GzrnvURQLWFzrn:+b/n/YP/n4a/ncZ/n |
| MD5: | B44194C1C5C8B390C13E4ADFBFF4EAFE |
| SHA1: | C53FFB632BA4581F9ECAC4F7675F34244A8F481B |
| SHA-256: | 6B861F6C1EF03120F76ABD04738925B6553F6771701A8729710A7693FAFFE063 |
| SHA-512: | 0CBF41CFBAE04E4A9D96C3AAF0284CFFEB25E36DD782300F170B2AD503F5F65D1A40150480F5A52DF8F2DB162D5E663816AEFFE318BD95C18A4C1914611959( |
| Malicious: | false |
| Preview: | 0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .`..$../....."#.D.O.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....o.e.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .?\|2%../....."#.Dr.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....)W.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...;%../....."#.Dsd.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....g.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...r%../....."#.D.:.....A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....(.^..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 420 |
| Entropy (8bit): | 5.588951793083332 |
| Encrypted: | false |
| SSDEEP: | 6:moXXYOFLvEWdENUAutSNAyC8n1TK6tLoXXYOFLvEWdENUAu1UXT+AyC8n1TK6tx:xhRToA7QShRTEiA7Q |
| MD5: | DCA8AA1E2BD71258E38201FA55690375 |
| SHA1: | 13C060B5C841F33733A481CA1074CC99E4451E00 |
| SHA-256: | FD727B12BE90684807BEB21778AEF08B4202B7A148336D7C81D637E1CE1B03C9 |
| SHA-512: | 498F9025067D058800D39FAC70FBD2E9DFDC0AC0B538E692B2927FD48CE51EA04083827C923DCEBF223B08D4C49F66D1C3DB774CB0B78D74FC9AA275CE17AE EA |
| Malicious: | false |
| Preview: | 0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ."5+%../....."#.D\Y.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....*. .....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...I%../....."#.D.'.....A8.../...;.\\o....1.....+..A..Eo.....A..Eo.. ....U.8..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 884 |
| Entropy (8bit): | 5.663976697917138 |
| Encrypted: | false |
| SSDEEP: | 12:nRrROk/VONyFTmBRrROk/VfmlRrROk/VCmbRrROk/Vq14Xm:nPJ/QNygBPJ/slPJ/pbPJ/K5 |
| MD5: | 9DC1BBD143D85193F46F5CDF878C7336 |
| SHA1: | 79E603CF22FCED51B01BF6688CFB92043E52A2DE |
| SHA-256: | CEF492AA59DA61C4FCE24ED88DAAF49B8A58D324F86E6E6072702D37E0AF288F |
| SHA-512: | 2A2194202BF54C00FCD088F56C0C67ED64275C99E16885889F775471F7121FA566BFB8034B7413D8EA2FBB1F6BE5B8FD06D1F4A2DEFA9753CC3964D7AF75D69/ |
| Malicious: | false |
| Preview: | 0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..j.$../....."#.D..\|....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A. .Eo.....H6.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .*.)%../....."#.D".....A ./.ev.....N~..6.b.....$.j; :C...A..Eo.....A..Eo.....&.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..w5%../....."#.DC;....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....s*.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .. .j%../....."#.D.....A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....Dx..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 420 |
| Entropy (8bit): | 5.607527168276607 |
| Encrypted: | false |
| SSDEEP: | 6:mZ/lXYOFLvEWdccAWuQDSnAdm9741TK6t6Z/lXYOFLvEWdccAWuytwAdm9741TK8:qxRcaVdu7EExRcIdu7E |
| MD5: | 834B341191BF83DC2A78D15D4B6C5F8F |
| SHA1: | DE0C14195DABD412296EFCD15DA231D803DBAE35 |
| SHA-256: | A2358CF75D03F4707FB4D1809A60FF1991DB759661690F3D9CE9B316ED986A3E |
| SHA-512: | F797054EC8A294B1FA32D792D3F0012951840A0BE8859B2CF5BCE7CECCE3B8BD652876DD312603DF293934FA76FE7856B5AE0FFE02E71A8549BF9434C4C8AB0 0 |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 | |
|---|---|
| Preview: | 0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .W./%../....."#.D{.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....#.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .9.p%../....."#.D[.....A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....h1.J..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 408 |
| Entropy (8bit): | 5.62231219004443 |
| Encrypted: | false |
| SSDEEP: | 6:mMOYOFLvEWdwAPVuWOOK3Jn1TK6tc/lMMOYOFLvEWdwAPVuPvATltlV3Jn1TK6tL:2R1YL6eR1qvApbDLd |
| MD5: | 7649E8B80F5E7C5D7F5D6C63561B7D6C |
| SHA1: | 348AB1FC81852ED1A96A16DBB6B4F75923AC2B12 |
| SHA-256: | A4E6E2FAA37B6CA409BC1602C66EABC3730C97B48ECD6B96D816B77E2A9684E1 |
| SHA-512: | 44CA65ABA5B5D9418A5576BD6390EF719C3005BEBB28421169A1E9270C664A58E0978394076799BA19A51DF135BA4C00A5CB93994A21013538B5B2DFE7508236 |
| Malicious: | false |
| Preview: | 0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..!+%../....."#.DS?.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....%.5.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...l%../....."#.D.....A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 424 |
| Entropy (8bit): | 5.6716580721938765 |
| Encrypted: | false |
| SSDEEP: | 6:m3PXYOFLvEWdBJvYQYj3SzhcsBXIh1TK6tC/E3PXYOFLvEWdBJvYQREodzhcsBXs:mxRBJQN3SDB0UAxRBJQQDB0 |
| MD5: | D3076C8E713DCE1E7BCF7FEB2A7D9616 |
| SHA1: | F778293FD681BE992D3FAD4816B4B6B5A194A6FA |
| SHA-256: | 2B2BEAFF1C565120CA058A85007CD05B6E0C5C10D5143FA6D755296E952F0015 |
| SHA-512: | D2998426BD65ADBD77B937B116FCFAB6DFF36281485284DF2DB12614D34475F5FD8886C53637FD54D61B7406D826ADA3E9C8F9275C2B421558F1D2D45342CA6 |
| Malicious: | false |
| Preview: | 0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .9.1%../....."#.D8.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....@.x.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .k.r%../....."#.DuV.....A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....W.]r..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 912 |
| Entropy (8bit): | 5.642711364113169 |
| Encrypted: | false |
| SSDEEP: | 12:3RrROk/swgBHc4FRrROk/stxiHchHRrROk/saAPHcy/RrROk/sh+Hc:3PJ/6B84FPJ/a48hHPJ/28CPJ/L8 |
| MD5: | 0AC8314F1ED72A062597648FB90D3906 |
| SHA1: | 4FDF9F5D21004392A447500F986E936E33014D24 |
| SHA-256: | 7684A7F4817AF0E2FFACE977089384A83ED68199C1FE5267BD5EC3CC8601BA89 |
| SHA-512: | 7673AD26CF3588D2843FF9226A69C87B27F8C2BDBC83A60B1F20F1331F1EA82D18BEA7124F782FF187D616FB77A69C33288C522DD942BAAFB096EF9E25086CB |
| Malicious: | false |
| Preview: | 0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..l.$../....."#.D./~....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....z.(.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...)%../....."#.D.P.....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 .X.5%../....."#.D.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....(H[.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...k%../....."#.D.e.....A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....9..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2064 |
| Entropy (8bit): | 5.292639119526273 |
| Encrypted: | false |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index | |
|---|---|
| SSDEEP: | 24:Mfg1zZFufGMisp6r6C9QPhBMOy1yEA1MXRQokik+nk97VR:h1zZ4+dsp6oBMOH191Tyk97z |
| MD5: | B92E0A827274037EE3C44347F2538EA6 |
| SHA1: | 9EB743CEF049DAAA23D1C65B7B305993022E612E |
| SHA-256: | 54FBF3C0540CAD59961A142F8616AF108C9D4ABE302ED335B38AC05D9B879683 |
| SHA-512: | 0F629341EC8BE0B4B25A4E29747B8DEE115D335B7B647F5CBD41C6B5BA715CE1F0F8B3C6FE7C6D6560ECADDA7642A6EE29B35114CEBD7B42CF45FDBF4F77482F |
| Malicious: | false |
| Preview: | ....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<\|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0...<..voy retne |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 292 |
| Entropy (8bit): | 5.219563682381253 |
| Encrypted: | false |
| SSDEEP: | 6:ctNFIq2PWXp+N2nKuAl9OmbnIFUtwxfcHZZmwyxvkwOWXp+N2nKuAl9OmbjLJ:civaHAahFUtwxfc5/yxv5fHAaSJ |
| MD5: | 161DB55204E6C5F4E443BB73518968FB |
| SHA1: | 9F1470CE061CF2AB35468AC637E4B511B1DF3F37 |
| SHA-256: | A57CE05914A790B971DD30DFB592F0A6CC1702B2E40407554C7ABD209E173275 |
| SHA-512: | DDA5EAF7C71BB00F4267565700931A29CD2F63E6DCC4542FD2CA3E002EB6D87EF7C7D16386E9C36F2B506B2CBB31DA4DC240FBC750D2C97781A70B43499CCB5 |
| Malicious: | false |
| Preview: | 2020/11/29-09:02:33.956 1964 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2020/11/29-09:02:33.964 1964 Recovering log #3.2020/11/29-09:02:33.965 1964 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log . |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1835008 |
| Entropy (8bit): | 0.00934913909958969 |
| Encrypted: | false |
| SSDEEP: | 48:TGEiaGEiCsMi9sMiDgsMiDgsMiDgsMiDdsMhCDdsMhCDdsMhCDOsMhCDo+sMhCDg:trrrCCCXononono |
| MD5: | 5CB4EE66DE605ACDFB5E558442585349 |
| SHA1: | 6C0C68F28E13B8700AE00DC1FB7E342DB8BE0255 |
| SHA-256: | 653F2729D6DA642B5A015E7BC1570985F28B8277D7EDED164ED5B02058235D1A |
| SHA-512: | 7C682EEE944A0520262CB0C503097F5954A3E9D016B4B532F5AA904F00D41B396C61343BF5F91696057622704DB7EB8D656ED8C0B5880E49D87CFB474C3D8079 |
| Malicious: | false |
| Preview: | VLnk.....?.....Tq.>..j..... ..... ..... ..... |

| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129170229Z-209.bmp | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PC bitmap, Windows 3.x format, 117 x -152 x 32 |
| Category: | dropped |
| Size (bytes): | 71190 |
| Entropy (8bit): | 1.8860963472929324 |
| Encrypted: | false |
| SSDEEP: | 96:E3hNtouS8u27Q40JN1hNaw5pIPEwb3G94d0zFqv7ZKIZPZHv35ZMzUP7PJum2zl4:yz7ZaX7FGxR4lXbXXdWW+R |
| MD5: | 11FAC24280131BDB9F5B3A68F18CECBF |
| SHA1: | BB6D156299CE74E6043D6F2AD6C84572F964637A |
| SHA-256: | 14722BAD22E332CDA1B6D4FB7067FD489725E491EC4238DB53102EB25B1AFEE7 |
| SHA-512: | 384F7BF137ED78791AD1AFCAC4AC8460191A54F20A42D046318BFC3A9243B7492BFBB97D909C6ECD16272FC16D2DD7068AD2FEC2042FD7C77C88ABE6DCC840A |
| Malicious: | false |

| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129170229Z-209.bmp | |
|---|---|
| Preview: | BM.....6...(...u...h..... .....DDD.UUU..... ..... .....www.fff.....___.....DDD..... ..... .....'''''.333.DDD.'''''.DDD.'''''.'''''.....www.fff.....333.....fff.....???.....'''''. .....UUU.....'''''.---.....'''''.www.fff.....'''''.999.....fff.....'''''.....''''' ..... |

| 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): | 3.3603136550694637 |
| Encrypted: | false |
| SSDEEP: | 96:iR49IVXEBodRBkasMOhbVCPL49IVXEBodRBkmsMOhpeCP749IVXEBodRBkJCd3sj:iGedRBGedRBLedRB8edRBg |
| MD5: | BCB8FA43E954A0EABE232093A7ABC83B |
| SHA1: | 1DD320D2B1A2EB5834DC5EA816AABC60E4A8719E |
| SHA-256: | B0F2D9BDADBF174E5C00967825E9FE3DE6A7EC660628D393CC5B79E2AAC57084 |
| SHA-512: | 92CB9DFB60E20AFF3B5DC45E1CE565D7E2A3FE0C52332B194D7C104CAF336E1FEF89CE15E9436CB7E1355F80CD539848D2ADDE1631CA3A264CB69D9BF5F04B4 |
| 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): | 3.1743408353963725 |
| Encrypted: | false |
| SSDEEP: | 96:Q7OhFVCPI949IVXEBodRBkxsMOhbVCPWLR49IVXEBodRBkQrsMOhpeCPBd49IVXa:QEiedRB5LGedRB1QCedRBhyedRBW |
| MD5: | 86B5E1CDE0F9F6FA8B368A9234DCF2DA |
| SHA1: | 3E8D76FD5BAF38D0520630EBF9AF6A4DB33D1B88 |
| SHA-256: | 7469CD281FB6858B379A345584A0BCF6986063002F193B07D9A14A09ED67E255 |
| SHA-512: | 7FD7A1F63EBE096FBBA5414C9E6016A3E9B76DC674DADD0E1000AF7E8C1999D8BD6E82EF7336C5B3B4F4FBA770EBC9C6AC3A142A24CD639C639C85E080FB269E |
| Malicious: | false |
| Preview: | .....T..... .....X... h...y..... ..... |

| C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5792 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 157443 |
| Entropy (8bit): | 5.172039478677 |
| Encrypted: | false |
| SSDEEP: | 1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2 |
| MD5: | A2C6972A1A9506ACE991068D7AD37098 |
| SHA1: | BF4D2684587CF034BCFC6F74CED551F9E5316440 |
| SHA-256: | 0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65 |
| SHA-512: | 4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4 |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr |

# Static File Info

## General

| | |
|---|---|
| File type: | PDF document, version 1.4 |
| Entropy (8bit): | 7.941002651961782 |
| TrID: | • Adobe Portable Document Format (5005/1) 100.00% |
| File name: | Invitation - Prime Minister of Israel.pdf |
| File size: | 118780 |
| MD5: | e3f4a57d14090a2866c16e4f2321bb30 |
| SHA1: | 0163a63054fd5da40c44e685cb7601decb8a2cd0 |
| SHA256: | 63f3f7706c4d6ca347ec95beb3e9401fcc3d8d263e8da4cf809d663f837757d0 |
| SHA512: | 919c3ee1141c8eeaa7fc219da8fecdc713477bdaf99b230c5ce2a622fd97737ab26c5b2d0ec968286efc5abad397518b121ffa9b298a8fd45e1a727b53c50d84 |
| SSDEEP: | 3072:MpK3dmmACoS0/MHEOFsYZjqO3iUaiJFs3YR:MpWdm5LjysViJF/R |
| File Content Preview: | %PDF-1.4.%.....2 0 obj.<</Length 3 0 R/Filter/FlateDecode>>.stream.x..[[....~._.....%0.[.@..0....$....=/...[wWKj.wC.agm./u.....\..?o.N.~.u.4...../.....Nq..w.q<M..q...]NV.;.....a....5.>..nJr.F5.....e./..?..t../.K..v..|.....X+S.;.=..|1...2 |

## File Icon

| | |
|---|---|
| Icon Hash: | 74ecccdcd4ccccf0 |

## Static PDF Info

### General

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

### Keywords Statistics

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

# Network Behavior

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2020 09:02:15.755975008 CET | 60100 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:15.783355951 CET | 53 | 60100 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:16.417495012 CET | 53195 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:16.444897890 CET | 53 | 53195 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:17.165832996 CET | 50141 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:17.201463938 CET | 53 | 50141 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:18.288870096 CET | 53023 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:18.316076040 CET | 53 | 53023 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:18.914027929 CET | 49563 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:18.941128016 CET | 53 | 49563 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:20.018062115 CET | 51352 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:20.053534031 CET | 53 | 51352 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:20.659615993 CET | 59349 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:20.697244883 CET | 53 | 59349 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:21.643280029 CET | 57084 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:21.670562029 CET | 53 | 57084 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:22.720118046 CET | 58823 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:22.747234106 CET | 53 | 58823 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:23.481014013 CET | 57568 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:23.508161068 CET | 53 | 57568 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:37.812949896 CET | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:37.822741985 CET | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:37.854274988 CET | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:37.868813038 CET | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:38.875530958 CET | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:38.875653982 CET | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:38.913240910 CET | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:38.914963007 CET | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:39.875773907 CET | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:39.875895023 CET | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:39.911204100 CET | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:39.918694973 CET | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:41.920407057 CET | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:41.920455933 CET | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:41.955881119 CET | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:41.955949068 CET | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:45.965594053 CET | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:45.970385075 CET | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:46.001044035 CET | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:46.007864952 CET | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:48.732259035 CET | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:48.770941019 CET | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:02:51.417119980 CET | 57762 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:02:51.444288969 CET | 53 | 57762 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:03:04.883447886 CET | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:03:04.920846939 CET | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:03:19.302372932 CET | 50713 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:03:19.345668077 CET | 53 | 50713 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:03:27.418625116 CET | 56132 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:03:27.445627928 CET | 53 | 56132 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:03:30.969587088 CET | 58987 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:03:31.007107973 CET | 53 | 58987 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:04:02.362142086 CET | 56579 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:04:02.389401913 CET | 53 | 56579 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:04:05.199237108 CET | 60633 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:04:05.234854937 CET | 53 | 60633 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:06.645500898 CET | 61292 | 53 | 192.168.2.3 | 8.8.8.8 |

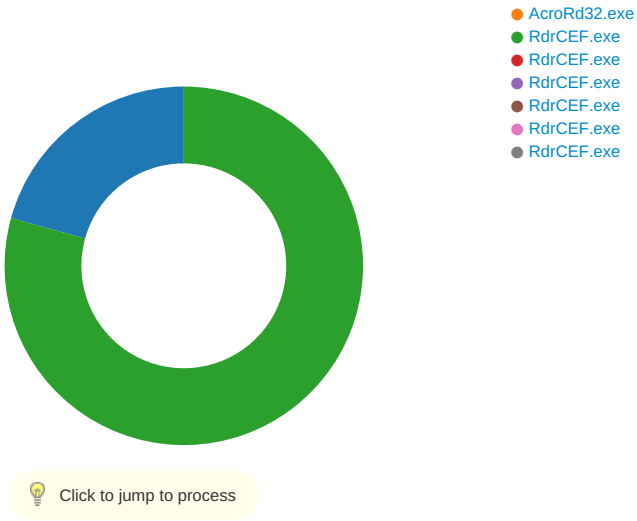
| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2020 09:05:06.705609083 CET | 53 | 61292 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:07.271598101 CET | 63619 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:07.307334900 CET | 53 | 63619 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:07.821237087 CET | 64938 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:07.856683016 CET | 53 | 64938 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:08.228981018 CET | 61946 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:08.305268049 CET | 53 | 61946 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:08.812218904 CET | 64910 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:08.847616911 CET | 53 | 64910 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:09.402070999 CET | 52123 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:09.437333107 CET | 53 | 52123 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:09.936914921 CET | 56130 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:09.972448111 CET | 53 | 56130 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:11.079885006 CET | 56338 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:11.115644932 CET | 53 | 56338 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:11.841186047 CET | 59420 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:11.876555920 CET | 53 | 59420 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:05:12.351352930 CET | 58784 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:13.413202047 CET | 58784 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:05:14.370615005 CET | 53 | 58784 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:04.645685911 CET | 63978 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:04.682924032 CET | 53 | 63978 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:04.940881014 CET | 62938 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:04.967837095 CET | 53 | 62938 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:05.279103041 CET | 55708 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:05.306142092 CET | 53 | 55708 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:05.816929102 CET | 56803 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:05.852444887 CET | 53 | 56803 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:06.224203110 CET | 57145 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:06.251538038 CET | 53 | 57145 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:07:06.384919882 CET | 55359 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:07:06.412190914 CET | 53 | 55359 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:35.417599916 CET | 58306 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:35.444854975 CET | 53 | 58306 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:35.542062998 CET | 58722 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:35.542285919 CET | 56596 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:35.542561054 CET | 64101 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:35.569432020 CET | 53 | 58722 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:35.569497108 CET | 53 | 64101 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:35.579808950 CET | 53 | 56596 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:36.064670086 CET | 64124 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:36.092010021 CET | 53 | 64124 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:09:36.320317984 CET | 49361 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:09:36.347675085 CET | 53 | 49361 | 8.8.8.8 | 192.168.2.3 |
| Nov 29, 2020 09:10:08.977058887 CET | 63150 | 53 | 192.168.2.3 | 8.8.8.8 |
| Nov 29, 2020 09:10:09.020932913 CET | 53 | 63150 | 8.8.8.8 | 192.168.2.3 |

## Code Manipulations

## Statistics

### Behavior

● AcroRd32.exe




# System Behavior

## Analysis Process: AcroRd32.exe PID: 1744 Parent PID: 5600

### General

| | |
|---|---|
| Start time: | 09:02:20 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' |
| Imagebase: | 0x960000 |
| File size: | 2571312 bytes |
| MD5 hash: | B969CF0C7B2C443A99034881E8C8740A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\acrord32_sbx | read data or list directory \| read attributes \| write attributes \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 9965C3 | CreateDirectoryExW |
| C:\Users\user\AppData\Local\Temp\acrocef_low | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 9BAE05 | 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 | 9AEA85 | NtCreateFile |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-201129170229Z-209.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 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5792 | write data or add file \| append data or add subdirectory or create pipe instance \| write ea \| read attributes \| write attributes \| read control \| sync hronize | device | synchronous io non alert \| non directory file | success or wait | 1 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock1744.1.1198220042.tmp | read data or list directory \| read ea \| read attributes \| de lete \| read control \| synchronize | device | synchronous io non alert \| non directory file \| delete on close \| open no recall | success or wait | 1 | 9E2657 | CreateFileW |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | A283C8 | 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 | A283C8 | 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 | A283C8 | 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 | A283C8 | 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 | A283C8 | 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 | A283C8 | HttpSendRequestA |
| C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1odii84_1nyp86d_4gw.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 | 9AEA85 | NtCreateFile |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal | read data or list directory \| write data or add file \| append data or add subdirectory or create pipe instance \| read ea \| write ea \| read attributes \| write attributes \| read control \| synchronize | device | synchronous io non alert \| non directory file | success or wait | 4 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rh0b2v4_1nyp86e_4gw.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 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R7ny5eh_1nyp86f_4gw.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 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rtjmxpn_1nyp86g_4gw.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 | 9AEA85 | NtCreateFile |
| C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R4lvjgc_1nyp86h_4gw.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 | 9AEA85 | NtCreateFile |

**File Moved**

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5792 | C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst | success or wait | 1 | 9ED405 | 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 | 9ACF19 | RegCreateKeyW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 | success or wait | 1 | 9AD41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0 | success or wait | 1 | 9AD41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 \cTab0\cPathInfo | success or wait | 1 | 9AD41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles | success or wait | 1 | 96EA55 | RegCreateKeyExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | success or wait | 1 | 96EA55 | RegCreateKeyExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | success or wait | 1 | 96EA55 | RegCreateKeyExW |

### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | aFS | unicode | DOS | success or wait | 1 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tDIText | unicode | /C/Users/user/Desktop/Invitation - Prime Minister of Israel.pdf | success or wait | 1 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tFileName | unicode | Invitation - Prime Minister of Israel.pdf | success or wait | 1 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tFileSource | unicode | local | success or wait | 1 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sFileAncestors | binary | 5B 5D 00 | success or wait | 1 | 9BDF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sDI | binary | 2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 49 6E 76 69 74 61 74 69 6F 6E 20 2D 20 50 72 69 6D 65 20 4D 69 6E 69 73 74 65 72 20 6F 66 20 49 73 72 61 65 6C 2E 70 64 66 00 | success or wait | 1 | 9BDF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sDate | binary | 44 3A 32 30 32 30 31 31 32 39 30 39 30 32 32 38 2D 30 38 27 30 30 27 00 | success or wait | 1 | 9BDF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | uFileSize | dword | 118780 | success or wait | 1 | 9BDF89 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | uPageCount | dword | 1 | success or wait | 1 | 9BDF89 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | aFS | unicode | CHTTP | success or wait | 1 | 9BDF47 | 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 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | tFileName | unicode | Welcome.pdf | success or wait | 1 | 9BDF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | sFileAncestors | binary | 5B 5D 00 | success or wait | 1 | 9BDF69 | 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 | 9BDF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | sDate | binary | 44 3A 32 30 31 39 30 36 32 37 31 30 32 33 33 34 2D 30 37 27 30 30 27 00 | success or wait | 1 | 9BDF69 | RegSetValueExW |

## Analysis Process: AcroRd32.exe PID: 5792 Parent PID: 1744

### General

| | |
|---|---|
| Start time: | 09:02:21 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\Invitation - Prime Minister of Israel.pdf' |
| Imagebase: | 0x960000 |
| 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: 2148 Parent PID: 1744

### General

| | |
|---|---|
| Start time: | 09:02:27 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 |
| Imagebase: | 0x8d0000 |
| File size: | 9475120 bytes |
| MD5 hash: | 9AEBA3BACD721484391D15478A4080C7 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html | unknown | 4096 | success or wait | 3 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html | unknown | 4096 | end of file | 3 | 9C59E2 | ReadFile |
| \com.adobe.reader.rna.user.DC.0 | unknown | 4 | success or wait | 11 | 9D83E5 | ReadFile |
| \com.adobe.reader.rna.user.DC.0 | unknown | 57 | success or wait | 92 | 9D8447 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css | unknown | 4096 | success or wait | 220 | 9C59E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js | unknown | 4096 | success or wait | 7 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js | unknown | 4096 | success or wait | 24 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js | unknown | 4096 | success or wait | 8 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js | unknown | 4096 | success or wait | 16 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js | unknown | 4096 | success or wait | 2170 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css | unknown | 4096 | success or wait | 60 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css | unknown | 4096 | success or wait | 12 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css | unknown | 4096 | success or wait | 8 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js | unknown | 4096 | success or wait | 3 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css | unknown | 4096 | success or wait | 8 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js | unknown | 4096 | end of file | 4 | 9C59E2 | 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 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js | unknown | 4096 | success or wait | 24 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js | unknown | 4096 | success or wait | 24 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js | unknown | 4096 | success or wait | 56 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | 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 | 59 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | 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 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css | unknown | 4096 | success or wait | 53 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css | unknown | 4096 | success or wait | 60 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css | unknown | 4096 | end of file | 4 | 9C59E2 | 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 | 19 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js | unknown | 4096 | success or wait | 17 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js | unknown | 4096 | success or wait | 17 | 9C59E2 | 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 | 9C59E2 | 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 | 18 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js | unknown | 4096 | success or wait | 238 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js | unknown | 4096 | success or wait | 286 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js | unknown | 4096 | success or wait | 268 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js | unknown | 4096 | end of file | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css | unknown | 4096 | success or wait | 49 | 9C59E2 | 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 | 9C59E2 | 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 | 196 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png | unknown | 4096 | success or wait | 32 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png | unknown | 4096 | end of file | 4 | 9C59E2 | 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 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css | unknown | 4096 | success or wait | 6 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js | unknown | 4096 | success or wait | 8 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 169 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js | unknown | 4096 | success or wait | 8 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 9C59E2 | 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 | 2 | 9C59E2 | 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 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css | unknown | 4096 | success or wait | 16 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css | unknown | 4096 | success or wait | 325 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 9C59E2 | 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 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 150 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js | unknown | 4096 | success or wait | 12 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js | unknown | 4096 | success or wait | 32 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | 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 | 7 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js | unknown | 4096 | success or wait | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css | unknown | 4096 | success or wait | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css | unknown | 4096 | end of file | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css | unknown | 4096 | success or wait | 4 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css | unknown | 4096 | end of file | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js | unknown | 4096 | success or wait | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js | unknown | 4096 | end of file | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js | unknown | 4096 | success or wait | 24 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js | unknown | 4096 | end of file | 1 | 9C59E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg | unknown | 4096 | success or wait | 6 | 9C59E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg | unknown | 4096 | end of file | 2 | 9C59E2 | ReadFile |
| \com.adobe.reader.rna.user.DC.0 | unknown | 4 | pipe broken | 1 | 9D83E5 | ReadFile |

## Analysis Process: RdrCEF.exe PID: 6316 Parent PID: 2148

### General

| | |
|---|---|
| Start time: | 09:02:30 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=129495829832415726 --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=129495829832415726 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1 |
| Imagebase: | 0x8d0000 |
| 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: 6340 Parent PID: 2148

### General

| | |
|---|---|
| Start time: | 09:02:32 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1712,12072885215581891837,16927562936397834584,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAEAAAAIAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9376569714315728772 --mojo-platform-channel-handle=1748 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 |
| Imagebase: | 0x8d0000 |
| 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: 6392 Parent PID: 2148

### General

| | |
|---|---|
| Start time: | 09:02:33 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,120728852155818 91837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2060730633019401765 --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=2060730633019401765 --renderer-client-id=4 --mojo-platform-channel-handle=1844 --allow-no-sandbox-job /prefetch:1 |
| Imagebase: | 0x8d0000 |
| 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: 6516 Parent PID: 2148

### General

| | |
|---|---|
| Start time: | 09:02:37 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,120728852155818 91837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6479133236096394756 --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=6479133236096394756 --renderer-client-id=5 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 |
| Imagebase: | 0x8d0000 |
| File size: | 9475120 bytes |
| MD5 hash: | 9AEBA3BACD721484391D15478A4080C7 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: RdrCEF.exe PID: 6696 Parent PID: 2148

### General

| | |
|---|---|
| Start time: | 09:02:40 |
| Start date: | 29/11/2020 |
| Path: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1712,12072885215581891837,16927562936397834584,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=301876132503772327 --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=301876132503772327 --renderer-client-id=6 --mojo-platform-channel-handle=1860 --allow-no-sandbox-job /prefetch:1 |
| Imagebase: | 0x8d0000 |
| File size: | 9475120 bytes |
| MD5 hash: | 9AEBA3BACD721484391D15478A4080C7 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

# Disassembly

## Code Analysis