


**ID:** 756144
**Sample Name:** Review Document.pdf
**Cookbook:** defaultwindowspdfcookbook.jbs
**Time:** 17:40:13
**Date:** 29/11/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

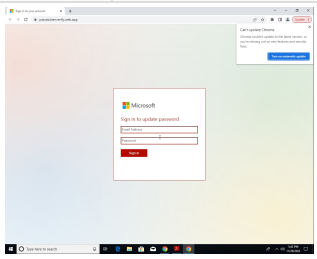
# Windows Analysis Report

## Review Document.pdf

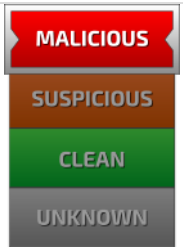
## Overview

### General Information

| | |
|---|---|
| Sample Name: | Review Document.pdf |
| Analysis ID: | 756144 |
| MD5: | db3d4eea0b2f09.. |
| SHA1: | 9ef2e56b31af633. |
| SHA256: | 96f73cb2b9fa43f.. |
| Infos: | |



### Detection



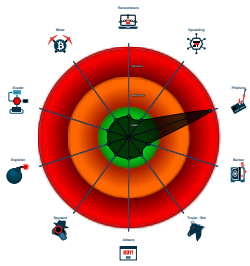

HTMLPhisher

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

### Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Yara detected HtmlPhish29
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- No HTML title found
- Form action URLs do not match ma…
- JA3 SSL client fingerprint seen in co…
- HTML body contains low number of …
- IP address seen in connection with …

### Classification



## Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 5016 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Review Document.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 476 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 6948 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://passatuhenverify.web.app/ MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 7120 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1784,i,7271988810475612612,8623558977825433660,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Signatures

### HTML

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 56225.0.pages.csv | JoeSecurity_HtmlPhish_10 | Yara detected HtmlPhish_10 | Joe Security | |
| 56225.0.pages.csv | JoeSecurity_HtmlPhish_29 | Yara detected HtmlPhish_29 | Joe Security | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Antivirus detection for URL or domain

### Phishing

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

Yara detected HtmlPhish29

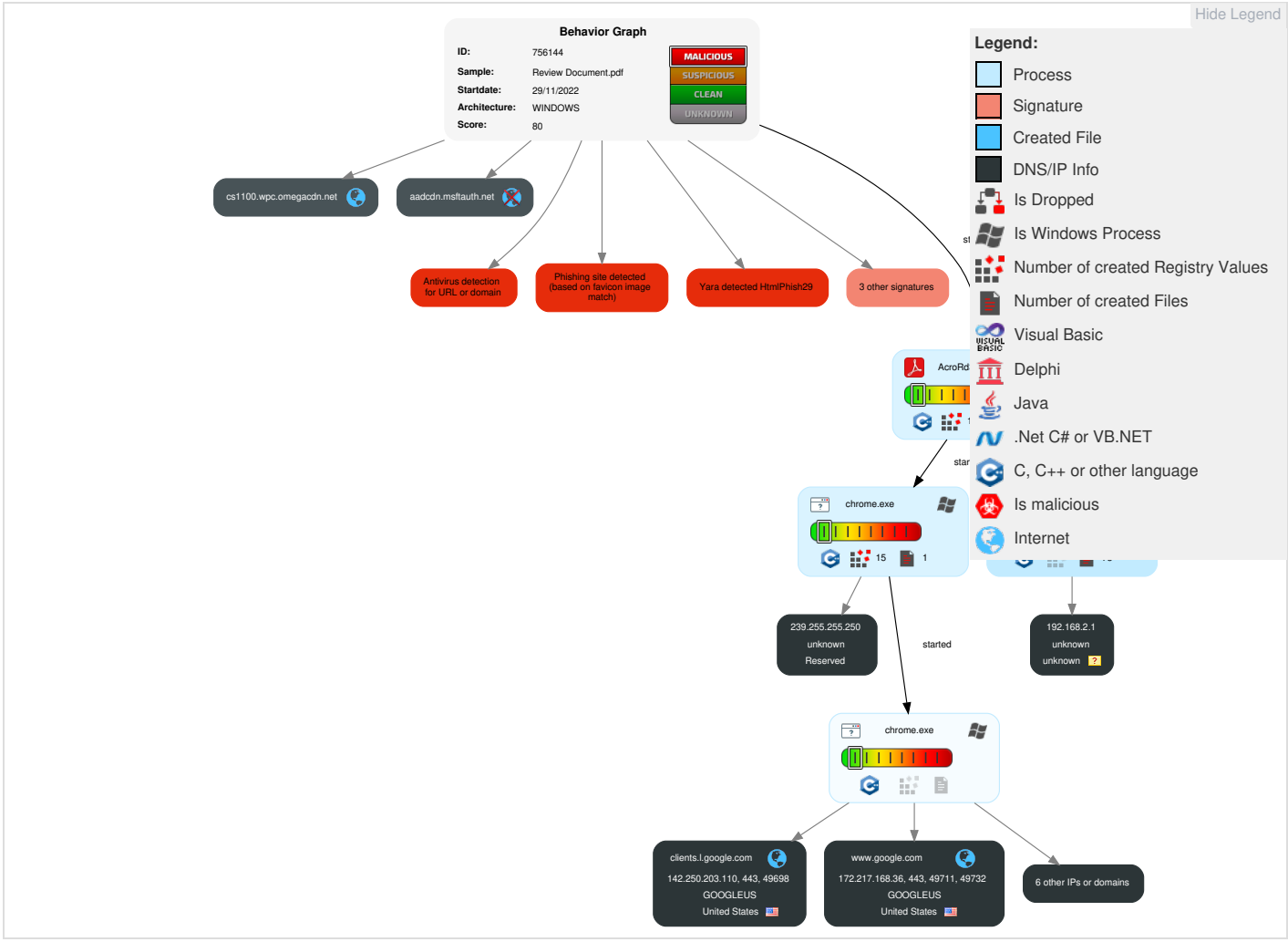
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

## 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 | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 Spearphishing Link | Windows Management Instrumentation | Path Interception | 1 Process Injection | 3 Masquerading | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 Process Injection | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 3 Non-Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 4 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 1 Ingress Tool Transfer | SIM Card Swap | | Carrier Billing Fraud |

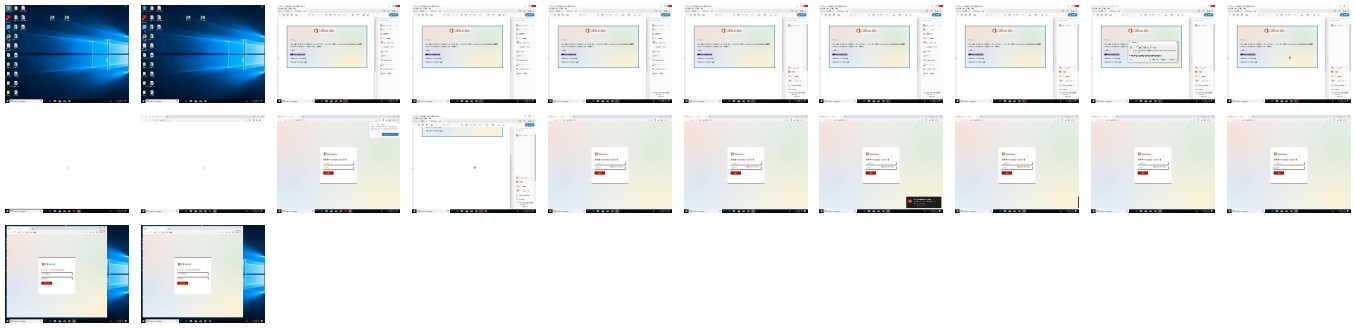
## Behavior Graph

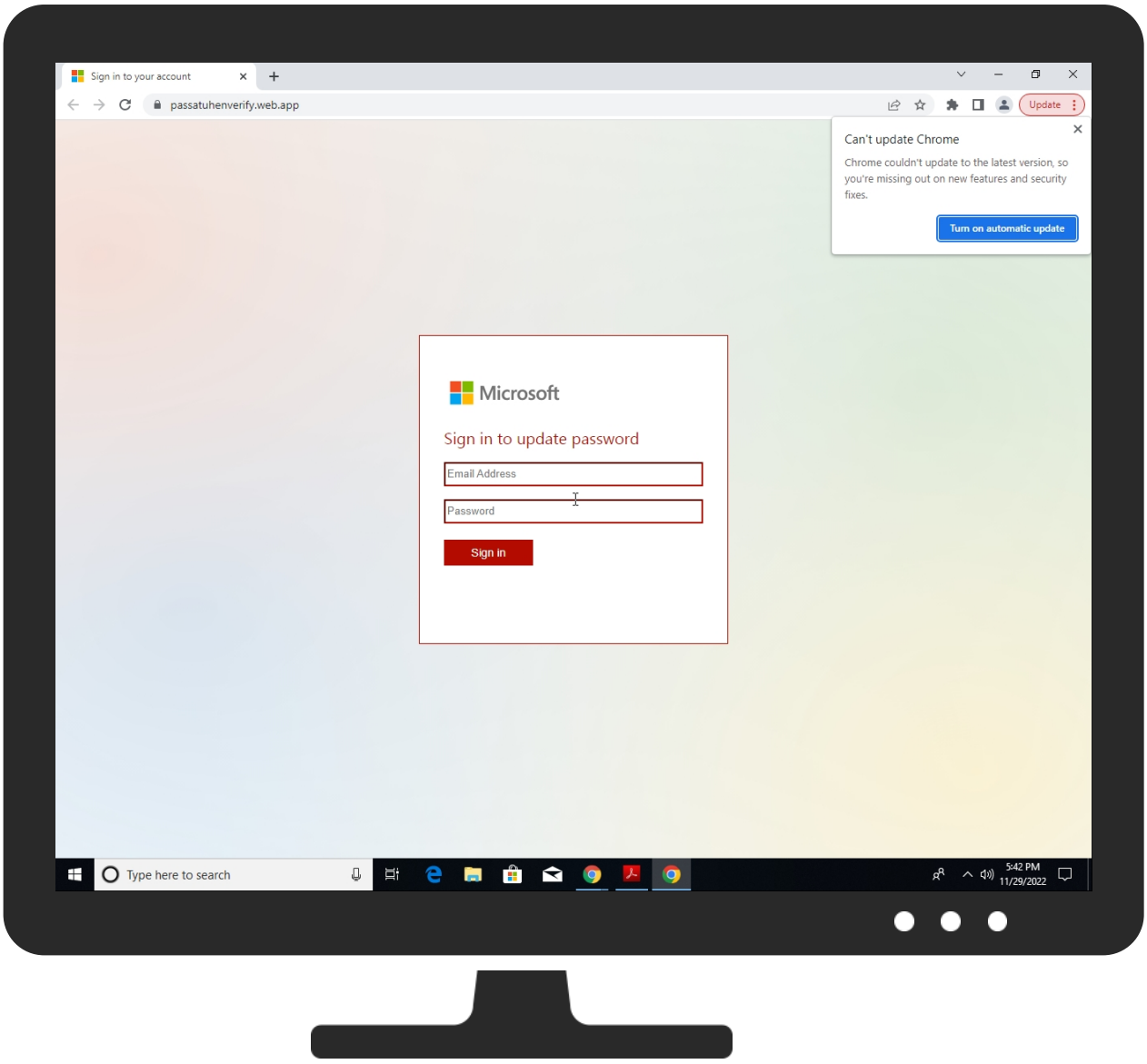



# Screenshots

## 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 |
|---|---|---|---|---|
| Review Document.pdf | 2% | ReversingLabs | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| cs1100.wpc.omegacdn.net | 0% | Virustotal | | Browse |
| aadcdn.msftauth.net | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://passatuhenverify.web.app/ | 100% | SlashNext | Credential Stealing type: Phishing & Social Engineering | |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg | 0% | URL Reputation | safe | |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico | 0% | URL Reputation | safe | |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg | 0% | URL Reputation | safe | |
| http://https://passatuhenverify.web.app/) | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| cs1100.wpc.omegacdn.net | 152.199.23.37 | true | false | • 0%, Virustotal, Browse | unknown |
| accounts.google.com | 172.217.168.45 | true | false | | high |
| www.google.com | 172.217.168.36 | true | false | | high |
| clients.l.google.com | 142.250.203.110 | true | false | | high |
| passatuhenverify.web.app | 199.36.158.100 | true | false | | unknown |
| clients2.google.com | unknown | unknown | false | | high |
| aadcdn.msftauth.net | unknown | unknown | false | • 0%, Virustotal, Browse | unknown |

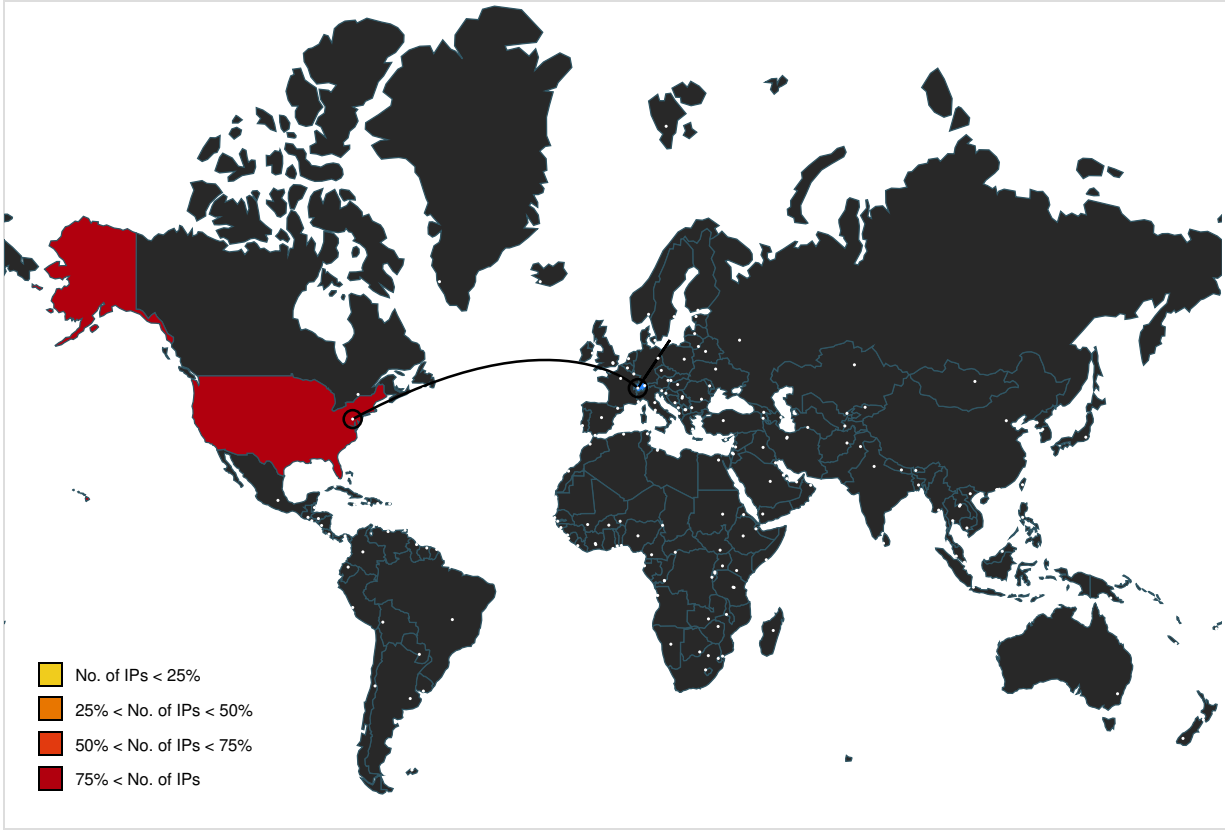
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 | false | | high |
| http://https://passatuhenverify.web.app/ | false | • SlashNext: Credential Stealing type: Phishing & Social Engineering | unknown |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg | false | • URL Reputation: safe | unknown |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico | false | • URL Reputation: safe | unknown |
| http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard | false | | high |
| http://https://passatuhenverify.web.app/ | true | • SlashNext: Credential Stealing type: Phishing & Social Engineering | unknown |
| http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg | false | • URL Reputation: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://passatuhenverify.web.app/) | Review Document.pdf | true | • Avira URL Cloud: safe | unknown |

## World Map of Contacted IPs




**Public IPs**

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 199.36.158.100 | passatuhenverify.web.app | United States | | 15169 | GOOGLEUS | false |
| 172.217.168.45 | accounts.google.com | United States | | 15169 | GOOGLEUS | false |
| 172.217.168.36 | www.google.com | United States | | 15169 | GOOGLEUS | false |
| 239.255.255.250 | unknown | Reserved | | unknown | unknown | false |
| 142.250.203.110 | clients.l.google.com | United States | | 15169 | GOOGLEUS | false |
| 152.199.23.37 | cs1100.wpc.omegacdn.net | United States | | 15133 | EDGECASTUS | false |

**Private**

| IP |
|---|
| 192.168.2.1 |
| 127.0.0.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 756144 |
| Start date and time: | 2022-11-29 17:40:13 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 17s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Review Document.pdf |
| Cookbook file name: | defaultwindowspdfcookbook.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 16 |
| 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: | MAL |
| Classification: | mal80.phis.winPDF@31/55@9/8 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .pdf<br>• Found PDF document<br>• Find and activate links<br>• Security Warning found<br>• Close Viewer |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.21.22.155, 2.21.22.179, 23.211.4.250, 172.217.168.67, 34.104.35.123, 172.217.168.10, 172.217.168.42, 172.217.168.74, 142.250.203.106
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, armmf.adobe.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, a122.dscd.akamai.net, update.googleapis.com, clientservices.googleapis.com, web.app, acroipm2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 17:41:07 | API Interceptor | 1x Sleep call for process: RdrCEF.exe modified |

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### 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): | 205 |
| Entropy (8bit): | 5.645190549499311 |
| Encrypted: | false |
| SSDEEP: | 3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuV01O/SMUk9kRkt4trXiTFJrqzOJkvP5y:men9YOFLvEWdM9QPmSwtSi7Z+P41 |
| MD5: | 3B0A59BB2319E5BD4D49EB707E37558E |
| SHA1: | 9E0782ACCA0DEE63B97973044E713D0ED4CA1027 |
| SHA-256: | 249E2F262B9EB351AC7607FE1378FE89195E11327C45DCC00DC4D94EA8EF937D |
| SHA-512: | D8BF75BB8128132171F2E3C871F4A736F143CE423A98BEC5EC9FF1A42593DF06AFF7739FD8CD87CD230C8B859036D4C8286F564B39E7820C0DD3D7B3CA0271 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....4M/....."#.D.....A.A..Eo.....-.H&.....d.{v.^.G...d.W.:...P..k%..A..Eo..... ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 174 |
| Entropy (8bit): | 5.541274574792175 |
| Encrypted: | false |
| SSDEEP: | 3:m+lF9NX6v8RzYOCGLvHktWV0ahTRktWNle98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkZh+tWN48Be7Ywcr1 |
| MD5: | A4292F3AF51F5A5B59069E9EEC984E8B |
| SHA1: | 109961A0CCB4A96F166FAADDE7BF2BB19E1A8720 |
| SHA-256: | AC8C9338827A923764148AA4808D27DD4E4C7E9EE4B2506672BE105CF70E040E |
| SHA-512: | 0A0F568F9EFEAB439ACB7A9FDF2338F895FEEDADA0C872059F16542DD135308FBD923C3372934FCB17F742211E467242FAAB5B1C8907CB38C8B9CE38AB76D0C |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ./...4M/....."#.D..p....A.A..Eo.....1.x.'.vl..*\|Z..o...+.4....0..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): | 246 |
| Entropy (8bit): | 5.587419164488398 |
| Encrypted: | false |
| SSDEEP: | 6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhu/Ymp0tfot/RlUoSjGY1:DyeRVFAFjVFAFbYm+lotZlUo6 |
| MD5: | 76093E541A9367A9146E1B89CAA61823 |
| SHA1: | 0732D2062DCC16D149A7FFE2CC85D35D3F219A73 |
| SHA-256: | 00C7B5C6CD59B9382B6F446FA9424C4997F5A626EB70731804A43784C6587BA6 |
| SHA-512: | D908A88AECFB3999AFAA88DF06607BAFCCEC73483CCBDBB998C544A43A7EEC09223DBBB16CD8D6368A15C3A63871C3C6A10293F3BCE99A24803A9A218276F062 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .WD..4M/....."#.D.}....A.A..Eo.....3.3.....hvDO.N.t@.....n.*..... ....A..Eo..... |

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

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 232 |

| | |
|---|---|
| Entropy (8bit): | 5.6601422303342055 |
| Encrypted: | false |
| SSDEEP: | 6:mNtVYOFLvEWdFCi5Rsm/a2FEG9ttbuiWulHyA1:IbRkiD5JEG9LjWus |
| MD5: | 9EF25E78DEE9106AAB8B37B6729C9AF6 |
| SHA1: | CC4823FA53009933DAB156B806340E695B9320E6 |
| SHA-256: | C005302E5BABB6C5DA79393AF41FBB2F51D35A6B7CE251DF36D923B988616E40 |
| SHA-512: | F44CF3097ED49D714D3BF122C0082CB6158D60B98666AD8E3AF2B05EEE88BAA267666454A947E06D5393DE50379B7227F306AC47B0AB0430406992B5AD23F300 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .....4M/....."#.D.c...A.A..Eo.....9y.....8 P..a...R..Y. ...7.@..2Dm{..A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.585535076370483 |
| Encrypted: | false |
| SSDEEP: | 6:m+yiXYOFLvEWd7VIGXVu4gQ9tmVyh9PT41:pyixRuzckV41T |
| MD5: | 4A80446736B5A856CD92CAFBDB724114 |
| SHA1: | D7C7D67429FB0BECFD25080E2149CCDA9FF15D82 |
| SHA-256: | 1DCAEBD1AA8FE57B245FE0E7B9D07963E50BF86A0BF598E5B4DF3F068EC43B85 |
| SHA-512: | DA80D662506C7D1D426D40A990889E457B6E48B1AF3D6C5B869D98746ED5DA63633ACBEF4126EE67DDA9C144F87C81128719109700E09437ECE087F3A0FC9B5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....4M/....."#.D.I....A.A..Eo.....v.....k.Q.....-_..y.....O...>..1....A..Eo... ..... |

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

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 216 |
| Entropy (8bit): | 5.627412314394969 |
| Encrypted: | false |
| SSDEEP: | 3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVPlt3LTXRktl/hlYo2sZI8xeGvPo:mvYOFLvEWdhwjQOFLTStlL3Zll6P41 |
| MD5: | C619B4B18CC6604EEADA8981A5389705 |
| SHA1: | 73631851F04D367B99DE84A1E1787DEC239B9AA3 |
| SHA-256: | E5E0EA6A3F994A10BE2D6AB6E031F998EB86C8EB356A91A519B5A9FB7D66F8FE |
| SHA-512: | 98D486905D75E41E1CA6F1718DEF4C2F3FFF840B7DE1B29F53C7949CDD13AB87C1E486A01A95AC801DCCF548B2CF5DB89CC4E6ABC9DA3EFB7E47D5B22F54 3DE |
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..I..4M/....."#.D.....A.A..Eo.....k.....].>....uUf..N...k.....c..I.A. .Eo..... |

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

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 209 |
| Entropy (8bit): | 5.548866550567805 |
| Encrypted: | false |
| SSDEEP: | 3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVe1ZST6Rkt7nXVcyxMtv9EWm1:mJYOFLvEWdGQRQOdQ/1w9t7nlD6g1 |
| MD5: | 84E95D478576BE020EE6EDBE715E9DAD |
| SHA1: | 3A3AEB49F6D192C181C90E5BBD3B08A0CB3B0058 |
| SHA-256: | DBA85D8BD4F2BB219DA843B507EDAA71B18DF449ECA7BB635FA26BF06DFDFB83 |
| SHA-512: | 6AEE575173C5D6D2C4153A464271C45C26BA0419A4F1EC37C9FADF6E1614764D89D15B65A507EACDCEECA9DA4F0673284F5AA8C29383AE4463083B409F049E 0 |

| | |
|---|---|
| Malicious: | false |
| Reputation: | low |
| Preview: | 0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .....4M/....."#.D.w....A.A..Eo.....K.....c..y/L....\|y.n..C/l.....X7-ne.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): | 179 |
| Entropy (8bit): | 5.5878346752558015 |
| Encrypted: | false |
| SSDEEP: | 3:m+lLp08RzYOCGLvHkfaMMuVhR1lxk6RktvF9lll/VQMWqg4nRb7om5m1:mOYOFLvECMLVlxk9tvUuR/41 |
| MD5: | F4023E790BF2B79A6A6979DD9E27C97A |
| SHA1: | 770C604C33F8C0CFDB2E00D05AC1AACCE4ECAB48 |
| SHA-256: | 6A94E7C60BDDC09400E46E8ED2EBC725C5FEC1FF9987F8AAB6FE6D5BD6D0BD19 |
| SHA-512: | 75D5C9CCFDE532E3DD9830DD5C4B3D931A72969C723036F4E329B2937FE6A9831F18D008616757419DA8C6417562A74410DDFE004934A8E08B72EE556F812F5 |
| Malicious: | false |
| Preview: | 0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..&..4M/....."#.DT.q....A.A..Eo.....^2p.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 214 |
| Entropy (8bit): | 5.554660149104483 |
| Encrypted: | false |
| SSDEEP: | 3:m+lS8FlC8RzYOCGLvHkWBGKuKjXKSO7p/KPWFv+BE9JRktyNYuuUy0tlBUKSx/yA:m4fPYOFLvEWdtugE9Qtoby0zBUKSAA1 |
| MD5: | 7CBA8E291527DB9ED8D5DDB76ED66BB8 |
| SHA1: | EA9835EFD3298FEAC518AA99DFFE5AF978A17F8C |
| SHA-256: | A96EB6833B73AD86FC7D8FF059B7967AE887E4C8A7C9E29993FA7969D0748AA4 |
| SHA-512: | A6207D5D23AB601A868A588C343C5F8A831AAA6EB19FB9BE17CF557C0F050519908487E925BC2F11902C70BFBC3D33555DAB4B200F236F48B711922238BDC33 |
| Malicious: | false |
| Preview: | 0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .^...4M/....."#.DI.....A.A..Eo.....Q..E.=....=h`t..t..3%A.F $..w..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): | 177 |
| Entropy (8bit): | 5.538745447533871 |
| Encrypted: | false |
| SSDEEP: | 3:m+l64HXlA8RzYOCGLvHkjXMLOWFvxTVllliqUT9JRktW/F+d1dn76KohyP5m1:md4HXXYOFLvEjMSWFv/llliqUTStW/8s |
| MD5: | 86B2D19DC4EBA789E2F7ED43F1AB593E |
| SHA1: | B102C6261822454368626 82E217DEFCBF508BD61 |
| SHA-256: | BF84F16A5EFA6193970550C417F426E372C18BD720A5B655C5EF795918895205 |
| SHA-512: | B8B8C0054BAB77856E86C4C8A0ABB853FD0F09B356CE1DAFEFEF24CF4E691ADFE3E6D4D1D0AEAE2CA735F3CA2FF7C719FE706840CB25E8B008ACE8A1EB9 CE4E0 |
| Malicious: | false |
| Preview: | 0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..!..4M/....."#.D..q....A.A..Eo.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 187 |
| Entropy (8bit): | 5.496907974869488 |
| Encrypted: | false |

| | |
|---|---|
| SSDEEP: | 3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLUYK/OcRkt1l9/7UPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLUYft1ICPqVyM+VY1 |
| MD5: | D94BC358024F969756245E18EC5E4907 |
| SHA1: | 875027E1E35C879174DB57CCFC26D0CC8DD98BCE |
| SHA-256: | 42F7A395061F165AD94401600A02FA6E9CFD8C9F4E091D6D11509F8E704340E5 |
| SHA-512: | F0137FCCE70D477B444E0D1E1AA31B9A7953089E739E89A5AD67DFD27555BCE587800323D643BF07BE267443F89F650A0666D97A09BBABE79378D1CDCFE2131<br>8 |
| Malicious: | false |
| Preview: | 0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....4M/....."#.DB.....A.A..Eo.....m.WS.....q.O...j...._y..L^z...?..@N..A..Eo..... |

**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): | 244 |
| Entropy (8bit): | 5.6287040649022995 |
| Encrypted: | false |
| SSDEEP: | 6:mt9YOFLvEWdVFLBKFjVFLBKFlyRGNtd6twSeKaT9pr1:URVFAFjVFAFqGNb6twSeKaTL |
| MD5: | 255F045D3E5D8B8375E07B739FCE7C1D |
| SHA1: | 2A6AF3563F3C6B8CBB8E9DE6E8FBEB95ADEC9136 |
| SHA-256: | 172E03BA2A60C03AEE9652E064BD2752E47C6053B5DA0C253964009BDFDC3FD4 |
| SHA-512: | A4436AC5296615C052A7EED39E3531AD060976B6345904E0A1800DC0C830D376B7AC8A65BCD6D7449905C4990646CB6A92F9E6F168E8C44E15A76B4B2B6F1A6 |
| 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 .....4M/....."#.D.....A.A..Eo.....O....<br>.....H...{...2../.k`..r4.C. .A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 211 |
| Entropy (8bit): | 5.518423690292057 |
| Encrypted: | false |
| SSDEEP: | 6:ms2VYOFLvEWdvBIEGdeXuaRoKsoctJ11:BsR2Ese5coc |
| MD5: | ECEC6B740576886B882DBB22EC43910D |
| SHA1: | 0BD82E472298D40FDEAF4371DD16375BE0F07584 |
| SHA-256: | 52DCE85E91D7D3905B4130F796F1A5E6E9BF2777064B83CBD1320515EEEFB287 |
| SHA-512: | 94165BADBEECC50DCC69271E594F0D31BE559D1FBA68592C439260AC70EB6E0489E9C41398A82F722E13863FBF018B12D7A528AADE545BF80F3E8E39E10FB1<br>B |
| Malicious: | false |
| Preview: | 0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .-...4M/....."#.D.....A.A..Eo.....G.....A.o]@r..Q.....<w.....].n\....A..Eo..<br>..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 202 |
| Entropy (8bit): | 5.675137340496586 |
| Encrypted: | false |
| SSDEEP: | 6:maVYOFLvEWdwAPCQiUl6kt1oxm7OhKlvA1:RbR160fQxmJ |
| MD5: | 61C319C3CEBDAF0E6010324F0301E7C7 |
| SHA1: | E85FC0161A56D146DDDAE1369967D5F65EA18EB3 |
| SHA-256: | 267DB833D63999B403997E0B37415847D5A379174B55DF68DCCEB48C278DEF3B |
| SHA-512: | DD91CDC87BA350A54C889A0E08745E2F52A7F2FBCF6E70462D3BD2DD615DBF3C938A4B17B7D0B05E7399698E9F21A9571B894EE433003A06BD735A0755AD86<br>B |
| Malicious: | false |
| Preview: | 0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..B..4M/....."#.D.....A.A..Eo.....C.....4T].....Tw.....(..b...EO....9.A..Eo.....<br>..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 211 |
| Entropy (8bit): | 5.59772132022504 |
| Encrypted: | false |
| SSDEEP: | 6:ms2gEYOFLvEWdGQRQVuM3ld3UQtdlddFt1:B2geRHRQr3Tb |
| MD5: | 05840FF0ACDCC7369B09DDD96609DEB7 |
| SHA1: | B9981997C400A5D87C1B32E30060558DCBC31611 |
| SHA-256: | 4956CDCFF8CAE77F901319035A2374DAE356048C95E95D894C8BB0D632C42A63 |
| SHA-512: | B08A443CF54CB85D4C4A626939BE8EEC430B53D3BB4DFDD9561A73CDCB912F2DB529D6E156235C49F86ECD751D8906DAD6E5A57DE2B49C3C45112909A0000 4A |
| Malicious: | false |
| Preview: | 0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .3...4M/....."#.D.....A.A..Eo.....Z.....@..{o]...9o\|..qY....T....{ ..u.b..A..Eo..... |

**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): | 206 |
| Entropy (8bit): | 5.596819938885584 |
| Encrypted: | false |
| SSDEEP: | 3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVCdRETRktZREnNWQ1SUm1:mzyEYOFLvEWdrIOQpg+tZREt1S/1 |
| MD5: | EE0B21D83AC51D5CAB23668B891A3979 |
| SHA1: | 414C4561FB780EA36305F89D36FAA771F4D12327 |
| SHA-256: | F697F6C4BB27FF81D853092D0727FC48CC22E82479CBF88CF48D840E1FC4EBF9 |
| SHA-512: | 2028A8F89D0D48D358AAA624F06A334AF8603E437D433D069040803DDE70BA7B2A066103A41FD33FC039E28DEB32494CBBBAB2EDADD8725B00DF4C610FC0B2 F3 |
| Malicious: | false |
| Preview: | 0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .h...4M/....."#.DLQ.....A.A..Eo.....'.0.....t\a.....x5.'OuE.C..@.....x..A..Eo.... ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 218 |
| Entropy (8bit): | 5.574734988275098 |
| Encrypted: | false |
| SSDEEP: | 3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFv8g/eloUk6Rkt+lwJNqww6U+5m1:mnYOFLvEWdhwyuh2l49t+lwrqwK+41 |
| MD5: | 68B00BA52980B4496D13AA8B57CD5624 |
| SHA1: | 768F1886C69547016681E38843A45CD6BA2EBDD4 |
| SHA-256: | 22C23E4C7BFD5D0A0FEFDD7671F4F1556D82B8B5C8CEFED5DF03235CA3E47CAA |
| SHA-512: | 01928B86F62535ED32D5B4CB8EB7364E69C7E601D0846D39505018053B447AAACB8B1916518B6FF3D95DEF1D589F384A1BF637A2BCF455530F35C6C196952B16 |
| Malicious: | false |
| Preview: | 0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .T...4M/....."#.D.....A.A..Eo.....V.l.....7...o..a=.98l.....(3. $G.A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 230 |
| Entropy (8bit): | 5.585154863658557 |
| Encrypted: | false |
| SSDEEP: | 6:mYXYOFLvEWdrROk/RJbuzQJtG/+fO441:/RrROk/8QJw+fL |
| MD5: | 519926718CDE9B7D4D92C458580EBEC6 |
| SHA1: | 5FA7B034DCD7E1FABEF17A180557955DA2BA9D2A |
| SHA-256: | E6DDC30E7AFF913BFD613AF985BD2D92226F62A772B6886D81EE8AC0E4EBF86D |

| | |
|---|---|
| SHA-512: | 321F8CCCDAE19646AE39F683408B04816DD4C1819607C853DA05ED3949666C77BBE08719A92AE1A7B6B4F115E7CFB5970551D08032E380E95B4F5A2AB9269F6 |
| Malicious: | false |
| Preview: | 0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .<...4M/....."#.D2;.....A.A..Eo.....-W>.....~..rw.+[....!.)?..f.U..(=.=.A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 186 |
| Entropy (8bit): | 5.5564044232776615 |
| Encrypted: | false |
| SSDEEP: | 3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVQgspDJRktqRzoIN1OFPL4m1:mmDEYOFLvEWXIQJ0tszV1QPLr1 |
| MD5: | 7A6EF1E0889F4329413402ECFA094243 |
| SHA1: | A6AA05061F7A5EFC2965E9D653543E22A373AAB3 |
| SHA-256: | 5AED4E3A3F41C89B6DB7AAC24705AFFA3700D27C293EE74B170A433DEE662D09 |
| SHA-512: | C0044A69DBBEB730D7AE4012910F3754F3D79DC3A2A4B0D795FE05E5EE9438A28EBFE1E4F54FA2C458C1050C7E625243B0EB0EA2C043D41AA008D7E2CB4D3E26 |
| Malicious: | false |
| Preview: | 0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....4M/....."#.DK.....A.A..Eo.....l"e.....~]...%s..<...n.f..<.....1#..U..A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 207 |
| Entropy (8bit): | 5.606979550587912 |
| Encrypted: | false |
| SSDEEP: | 3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFv1tUFngTXRktPW8D6EsEJeUm1:m52YOFLvEWdMAuNUd5tPWEvsEJ41 |
| MD5: | 0190227310C3948FE724A09A372CCECD |
| SHA1: | F27EE6D6D8B91FF18F04A8A17348F0F333EBB71D |
| SHA-256: | 4D585D322529E48384308C4A41B778879E7ADB92E6F5BF8E92253F9E96ED672B |
| SHA-512: | 28AA7689149E033805A1B7AF38EC3342C1B46E85511DC2A3FA8D6E43E027F94B3D3A3F5775DCF359B679D7BE5D22C8E7737EC585E4A71F2A065FB224765D7A8 |
| Malicious: | false |
| Preview: | 0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .R ..4M/....."#.D.....A.A..Eo.....,.....z._a...'.v.....4p3..1.']...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): | 210 |
| Entropy (8bit): | 5.563690569212748 |
| Encrypted: | false |
| SSDEEP: | 3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvU9EXRktmll/GFoDb7T2/My:mYilPYOFLvEWd8CAdAumltmAong1 |
| MD5: | F7732E7964A89A05306F1B373577F7C1 |
| SHA1: | A4002EFE3B120F8A2A1B8EDB7EBF2494F49D7922 |
| SHA-256: | 4A15EA87F17DE0D4D22446529059AC1DBB385CAEEB8C7B60A46442050E5D63FA |
| SHA-512: | 0F11E17813B5B95CD9406287802DF32E3460B12941C20A648DD9D8BE6222BE0786E2AF1BBF51173BCDCA43BE6A15D912FA8756178FC0FDD40F1FF5643BDC3C0 |
| Malicious: | false |
| Preview: | 0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..!..4M/....."#.D.....A.A..Eo.....pq.....c}.H7M=M..-.....lx..R.l...}Rl.$q.A..Eo ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 223 |

| | |
|---|---|
| Entropy (8bit): | 5.5589041388404645 |
| Encrypted: | false |
| SSDEEP: | 3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVlJ/2oKPWFvlXlnTRkt1LOe28WlJLkxwyB:mY8nYOFLvEWdrROk/luI+tlN16wG1 |
| MD5: | A06108241E7E695892FFB954AD4B3510 |
| SHA1: | C086A26C03C6AC279EB3D7C50AB6A27AA513B4CE |
| SHA-256: | B8143345EC78E5A8A14E5FE58D209E57466DA861E5973CE027D99D7E5E33DA0E |
| SHA-512: | ECC6E4B31B765C8FC81C8966FBA1970E5E6B1448F3D47234ED1CDC111A96E66CF83B16D0D6C8B22D2E6C68C85C1F240A8A9B37AE3DF0FCF37A5F73ACB8587BF6 |
| Malicious: | false |
| Preview: | 0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....4M/....."#.D9).....A.A..Eo.....c.....%.k.SZ..~W.... .:)'B..ad.....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): | 213 |
| Entropy (8bit): | 5.643006093393573 |
| Encrypted: | false |
| SSDEEP: | 3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVjV5ekRkt74PmJelc0Rm1:mLrnYOFLvEWdrIoJUQG+tseJli1 |
| MD5: | 38A03D3DADAB4B024CC9E3A7BA481795 |
| SHA1: | 5479FC09C29AC0018A3DA54D82A4BE865398F3F1 |
| SHA-256: | D34683E2A2C73509B0B063B105364BCD90EE1D2868254E54A8ED6A9C77A07880 |
| SHA-512: | B248744C4D355B55404B1FBA34542FAB963ACD355B03F766BD54DA0E3272347F71DD502811B930EF09F9D6D42528E4CC7485B2A5A46AFDF48828AC1DFD651EE8 |
| Malicious: | false |
| Preview: | 0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .E...4M/....."#.D.....A.A..Eo.....F.....;"./N_.,.:C..2....9L.H...3:...A. .Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 208 |
| Entropy (8bit): | 5.539649193493628 |
| Encrypted: | false |
| SSDEEP: | 3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvnURoX96Rktutlx6mgmOZLhT7Uy:mOEYOFLvEWdrIhuNRrtOxzgm2d/1 |
| MD5: | 7287F80670EADF0EC5D9C0548793E712 |
| SHA1: | D619E72236523E35E3BCDEBE87A35913FA729214 |
| SHA-256: | 0DAED56A748C992C3575291A1D46B8C32E83DB37041FF9C1ECB51BEF30C321B9 |
| SHA-512: | F670AD08978B4326D1F20E72AAA7853CE95CC1769A5966A128C761632A779ADBA4B0559885260F5ED3DE938ECB99DF89FC4113B0BBAC8F48521AB840004C247 |
| Malicious: | false |
| Preview: | 0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....4M/....."#.DA.....A.A..Eo.....L.....Z.Z}Q..4.o....0+..[|..n:*..U.W.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): | 188 |
| Entropy (8bit): | 5.606320392905866 |
| Encrypted: | false |
| SSDEEP: | 3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cva1lcYoEG9kRkt5eBiaQ562HvpMm1:mAElVYOFLvEW1KBlcYoEG9t5rx56uvp1 |
| MD5: | E87D0CE4B224E6A5B369C19EB8BEADF3 |
| SHA1: | AC51A4EEDAA67956CA58E7688E48036CDDA244D1 |
| SHA-256: | 62BC65845E84E9535D3DA9F2EBEE687557F345245D7833E18D1C68C6E6E14063 |
| SHA-512: | EB50C6BFCF235907898C99942987DAB1D8AC947ECCC68B512F93DD2FB40556A74A11CA19CBC29F08BDE92DC07B258E55EBF072FC70477C1B1A3CA36E3E4CA602 |
| Malicious: | false |
| Preview: | 0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .9...4M/....."#.D.....A.A..Eo.....z?...SwC...^..y.....V..7R-O.....A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 214 |
| Entropy (8bit): | 5.657289538475569 |
| Encrypted: | false |
| SSDEEP: | 3:m+lSy/08RzYOCGLvHkWBGKuKjXKBRSJvBCv1KPWFvq+QHEXRktfXdY8UDLY3PHVV:mWYOFLvEWdBJvvu44StfjUDLYtmOZn1 |
| MD5: | A3DA479DD2E8150A096A50018A0B6FDE |
| SHA1: | ABD35C1E829E1EA00187E2D3BC66392416B4BB47 |
| SHA-256: | A20379CC655FA4C59A2B170921B8EA6FF89614FA9DCCD0EF540BF42EF373FB04 |
| SHA-512: | 50D52545E5D24E0A4D802E43355A8797E8E86DCDA3BE51B7CEEB4C03001EA8C9A99A84D2C09904FA8ADE621EE2C4B24DC8549DE3D2B26193C10F871369F907<br>88 |
| Malicious: | false |
| Preview: | 0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ....4M/....."#.D.#....A.A..Eo.....J.....t.q..W.EZ....1...[.zC.7mD..A..<br>Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 211 |
| Entropy (8bit): | 5.6002344938407695 |
| Encrypted: | false |
| SSDEEP: | 3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvGwaFpdRktbPpSKGoSSl0Jk:msRPYOFLvEWla7zp7xwaF+tbP8VPu1 |
| MD5: | 842D1F0B1569E92E9F9984547C0B78FB |
| SHA1: | 50BDED4A8AD04E1708731FF5F21D68B7BD39E1AB |
| SHA-256: | 2A2171167E19CA61F55A51474930820872FED217B80C81E5A7EC0C9E70CAE344 |
| SHA-512: | 425BED6A5B1A67D4213E6E66513D2C08238B9018495613B11CF8FD3C7D2E1FFBD5C22B65DA542D7D6400AD912E6302AC4BB3E12AC26E1D564A3FBFC36314A2<br>5 |
| Malicious: | false |
| Preview: | 0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .J;..4M/....."#.D3.q....A.A..Eo.....L...Im.@.....E.nW...IP..A..Eo<br>..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 208 |
| Entropy (8bit): | 5.628911693221753 |
| Encrypted: | false |
| SSDEEP: | 6:mKPYOFLvEWdENU9QJhIXWQt+PswiM3Y1:bJRT96hIXp8r |
| MD5: | 3624CA7DF1190E2712A90062DC977C74 |
| SHA1: | AF1A56DE2F778816077A30A51DCFC56D990B1EF7 |
| SHA-256: | 64415DA2BC33CF5F078199F8E2C533353D369483D2DDA78CBBEE61580121F6E1 |
| SHA-512: | FF9038F74E4610E95F83C835B2542F66E4A691A785EDA818992F0780CD2993B239AEDF5D9A11AD9AFA6D1ECB5EF47A24BB9048583541C22C154E5AD8C7EC31A<br>E |
| Malicious: | false |
| Preview: | 0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .IF..4M/....."#.D.....A.A..Eo.....=z.....M....m+lS..e.....<7.U.P8*<br>.0K.A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 208 |
| Entropy (8bit): | 5.61203777493172 |
| Encrypted: | false |
| SSDEEP: | 6:mQt6EYOFLvEWdccAHQTf+g20tKNjBRCh/41:XRc9g30NDi/ |

| | |
|---|---|
| MD5: | 497261EDD39A490E03280AB884838587 |
| SHA1: | EF56A591F6AB8FEB14B0106204D34036FB20A267 |
| SHA-256: | 6988731F68D6DC92F0FA8C46BC39EFFEF9735D41A26D688D10F4013AA2116D3D |
| SHA-512: | 0B6B691ECF84A095497A1A9A1AA33E9C6FB1848FE6B038E159E43F0EE7CD8FA0E6DEC116A12B7AAA9E96ED1545B64F7476BCB894859B9F2BE97EB1A6C2D030CF |
| Malicious: | false |
| Preview: | 0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .P...4M/....."#.D.....A.A..Eo.....e.....PJm...0x.x..RD...BB!@5..<..]. ...A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 231 |
| Entropy (8bit): | 5.585461595442176 |
| Encrypted: | false |
| SSDEEP: | 6:mqs6XYOFLvEWdFCi5mhujrtY9kULIF4r1:bs6xRkiFC7LIF4 |
| MD5: | 86C20E38797BC375CA101CD3729F44B8 |
| SHA1: | CA2A7F11706F63900C37FB8A7DD27227CEFAEB7E |
| SHA-256: | 32F021A649B20CF944170D5719E383409432EDF71D5A29A993F77B0B31C0AA6B |
| SHA-512: | 69DDDF46CFDE9EBFA361C1FB482F8AA77BF2CD4D216E747514F53C96E8EB3F86C8A148E4D0C615DA62D2394DBA0822ED68B6B472BAC463A2704A22AA0FC2F5F9 |
| Malicious: | false |
| Preview: | 0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .....4M/....."#.D3....A.A..Eo.....G.....P...#4..I....5.. .5..).w.. .h.~..A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.54377114469016 |
| Encrypted: | false |
| SSDEEP: | 3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFv8WsIXIDH9JRktFCtlECcu1isLKo:mhYOFLvEWd/aFuKj5Qt4lEN941 |
| MD5: | 2B059ECF965AF171A4F8E82E85BD16E8 |
| SHA1: | CE01F7F125C20ED241669386F32EDCB93507ECEC |
| SHA-256: | 69EE047B9E30536E35C0B271BA71BF769FC2BDC3E69A114793FCCF104382F9AA |
| SHA-512: | DBD3367005E9A00580D7D5A9BFCFBB13F7B69C3D0562E5066E9057268ECAC62DBCA91A76F9224E65A738EE229E2A4F26B0F95CA6F3C2B5DB6FA9467359354BDC |
| Malicious: | false |
| Preview: | 0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .....4M/....."#.D.....A.A..Eo.....z.....a.f.m.i.o.p..3U5.....^...I.A. .Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 208 |
| Entropy (8bit): | 5.546148655243984 |
| Encrypted: | false |
| SSDEEP: | 6:mR9YOFLvEWd7VlGXOdQzlQt0lBMqVd3G4K41:2DRuRglQKlB9Vd2 |
| MD5: | CA6861C33202C08F3FF1096544960A8F |
| SHA1: | 98C7EE4CA9DFB19DB5F70AF2BF2BE3696083406B |
| SHA-256: | AA1CB1F7102132BA6FD9AA895E3B238B8014601142CE693C262847DCF1D1A18F |
| SHA-512: | 1CB4B28A9EB9A4820A6AE75B4B03277C760489A00CC62604C9BB0E203FE0E509DDAE954D9346AAF7E97B0F23224FDF71DE3F814F57808DCF320CBC0AFDB2E663 |
| Malicious: | false |
| Preview: | 0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .}...4M/....."#.D.....A.A..Eo.....k.....y.$..$.v5j...T...z.]..._S....A..Eo.... ..... |

| 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): | 208 |
| Entropy (8bit): | 5.588573426271932 |
| Encrypted: | false |
| SSDEEP: | 3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVlluAUUJRkt3l/W4ThzJuA4N:mkqYOFLvEWd8CAd9QUoAIt3DuA424r1 |
| MD5: | C3040F4749C615DBFBF4CB60409B1E9E |
| SHA1: | B4C71C7EB42857DC03CF6D4B751EB90F0224647A |
| SHA-256: | DFD40D22332FB790814947DBE32FC3D7C5465BC9FFF32C5C8E6203F75B96EA98 |
| SHA-512: | 8C8061A1EAC1A8E190529CB415F53A3CD17248A61CC9A9D7DF90094E06A4010C55AEEC65D2C5841668657AEA259256B9255C711A1BAB48C1B9AEFA2F7C9EA1<br>1A |
| Malicious: | false |
| Preview: | 0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .n...4M/....."#.D.e....A.A..Eo.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....<br>..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.545833496445072 |
| Encrypted: | false |
| SSDEEP: | 3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvgB/9EXRktPMltNAg2iHio/My:moXXYOFLvEWdENUAuWBuStctGyC8n1 |
| MD5: | F00F16FA61B87F7D324E93E66C5E78DC |
| SHA1: | D4930470B7CF526868967CF00F0F82A511D334D8 |
| SHA-256: | 7D17912075510C2A62AB7C96A4D01BE48204113AD83CAF9BE2A82B00C8B001A3 |
| SHA-512: | 735519C200D4B657885188842E1369C2D7F59E502B7D125677BDC8D5EAD7C9E4AB5D079AF82C7E3EA089CBDDAA851CD67D078ACD3926DD37DFC98F42FA56F<br>48 |
| Malicious: | false |
| Preview: | 0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .i...4M/....."#.Dx.....A.A..Eo.....A.....8.../...;.\\o....1.....+..A..Eo.....<br>..... |

| 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): | 221 |
| Entropy (8bit): | 5.5974466691657385 |
| Encrypted: | false |
| SSDEEP: | 6:mQZYOFLvEWdrROk/VQ5grBGEStzsLmB41:nRrROk/VugrB+ZN |
| MD5: | 1638B01AB2332458FD0CC96A514ADD16 |
| SHA1: | 66AA1752A5C6770E2D735EE001ECBAEA14AFD4C7 |
| SHA-256: | 53DD226BFCB533CEE0846D37AC80AE23AF6B4D0F9DDE91B88930C9003155DC78 |
| SHA-512: | FE2734D778609FAECE1FC4297209DAD07372A8E47FDDBCDEAFD21B11F4055346D02DE9DF14A16CB22F501D50C28EF65C29CE47B15C08E0FD1C2BE2DF39DB<br>8DC |
| Malicious: | false |
| Preview: | 0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .....4M/....."#.D.t.....A.A..Eo.....n ..... ./.ev.....N~..6.b.....$<br>.j;:C...A..Eo..... |

| C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.593611611594427 |
| Encrypted: | false |
| SSDEEP: | 6:mZ/IXYOFLvEWdccAWuUiD2QtT95dm9741:qxRcu2JJdu7 |
| MD5: | 4FF146B748CD37CE0DAF0D35C6CC8F64 |

| | |
|---|---|
| SHA1: | B082444A56D483E793AF0A5C2FE253F6731FECDB |
| SHA-256: | 9EBE769E5ECB3905F77D773F1357FCB09A9258A27061B5048870A6B39480EECA |
| SHA-512: | C831320EE0FEBEAE7DC92C71ED89286081C1DE1C9668D4AFF4A090BE07FD0754567D477C204CCFAE2D8A52821C89B8BFCD8350B7E346975E42B1FB5B02E172D7 |
| Malicious: | false |
| Preview: | 0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..E..4M/....."#.D.....A.A..Eo.....U...I.>P...X...x..0U.~;m.x.k.A..Eo ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 204 |
| Entropy (8bit): | 5.5548229582961675 |
| Encrypted: | false |
| SSDEEP: | 3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvVW+lkJCG6RktUlEB6shoq+Nem1:mMOYOFLvEWdwAPVu/6UG9tJB6Jn1 |
| MD5: | B9F9FAA2764A8F8484B6A15821F2E07A |
| SHA1: | 089D56901F44911FFCBC263C6E64C8CC69FDBCCF |
| SHA-256: | 8F0993F3A75240A17091411C864960C97D329F81482EC8E55710ECCF53244854 |
| SHA-512: | 6E6C2AEBAD379665DD123A270CE6C4922DC8A5CBBECC7B6F022315C79A9E3C99509D9898F532045CC9745BAD69578A9E84A0B01A90EF6D4768F13C968ED033 |
| Malicious: | false |
| Preview: | 0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .0...4M/....."#.D.I.....A.A..Eo..... .*.....k....F..D..O.n;[.1m.....=..A..Eo..... ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 212 |
| Entropy (8bit): | 5.656449626402114 |
| Encrypted: | false |
| SSDEEP: | 6:m3PXYOFLvEWdBJvYQv165p49tjNqhcsBXIh1:mxRBJQ26305AB |
| MD5: | 84F8E44A4E05A7275BEA8C36AA1ED849 |
| SHA1: | 838155F4756912E0FB8AC09C44BB7F660CD2343E |
| SHA-256: | F4DBE17AACDB7FF49D0C33FCC79CB6A3363E79D2338EEE38D47D8FD4908C03CC |
| SHA-512: | A2B708CA37179C4FD380734A50C08E1B5D73613429BF9D797DABEAB25DA48A73ED73D34B3F6BE66140DF7CA7B051075D1BB553622A3350DC79C3B170503D62C |
| Malicious: | false |
| Preview: | 0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .e...4M/....."#.D.....A.A..Eo.....).C.....k..`..N3.... ..d..$[.....{.A..Eo ..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 228 |
| Entropy (8bit): | 5.606945676174413 |
| Encrypted: | false |
| SSDEEP: | 6:msPYOFLvEWdrROk/RJUQvnIXqtlirc3Me/1:3RrROk/s2V1r |
| MD5: | 1A25C7E6D1A64978DDE0976F6DE1540C |
| SHA1: | 900B1DD884E58EED9CA29BD331EC1EEFB856F4B2 |
| SHA-256: | BE7288317AD4246D0E5B9173814FF3849F16C53FC55281B36401981B0BF87C53 |
| SHA-512: | 8B4EFD87CEC181CC5716547971B63BEAB6D01B2C8649C2E2E20973F7F873EB3C7B20D27BBC24382A309D11090589267B29FC675218109D44A18F2BAB4538267A |
| Malicious: | false |
| Preview: | 0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .18..4M/....."#.DF....A.A..Eo.....9Q].8O.z....=..:.N.{....N{.A..Eo..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 1032 |
| Entropy (8bit): | 5.198172509346943 |
| Encrypted: | false |
| SSDEEP: | 12:VtrUxuSR3GBqyEeMz6+dtLiA20ouy5trFl+A1tAqYU3s1q9:dSRuqNeMm64VFEb3I79 |
| MD5: | 201E484F5BD6BEFC51902BC5B26C78D3 |
| SHA1: | F85B7C13F6E9BAF140085B3E08068DBDDB869C54 |
| SHA-256: | ABD97E83940DADD68BBC598EFF1002535FCEF24F7E4CE666D3E1123F3FE97D97 |
| SHA-512: | B7618DFA97900515EC8531983641BD41B7F17576BE753A12147CD8AC1AF9366DD65B5956332F493CAB94BEF5F18F7CB8DC5882C9AB9D37473EE580F872BF397 |
| Malicious: | false |
| Preview: | .....[~Hoy retne....).....T.....3.....4M/.....v...q.....4M/.....C..M.....k.....#...(...k.....]...I....4M/.....4M/.....6<\|...@n..4M/.....<...W..J@n..4M/..<br>.....oB*@n..4M/.....a....@n..4M/.....;.y~A....4M/.....P....V....4M/.....F..=z;....4M/.....o....4M/.....*.....4M/.....2q.....4M/.....Gy.'.h.....4M/....<br>.....k7A.....4M/.....:..N.A.....4M/.....;/.....4M/.....4M/.....P[. q....4M/.....,+..._#....4M/.....J..j.....4M/.....A?.2:.....4M/.....q.....4M/.....u\]..<br>q....4M/.....!...0.o....4M/.....*.....4M/.....o..k.....4M/.....^.~..z.....4M/.....[.i..%.....4M/.....+.{..'....4M/.....@..x.....4M/.....MV3.....4M/.....*)....J:....4M/...<br>.....&.S.....4M/.....D.4.....4M/.....+.U.!..V....4M/.....~.,.4>.....4M/..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1032 |
| Entropy (8bit): | 5.198172509346943 |
| Encrypted: | false |
| SSDEEP: | 12:VtrUxuSR3GBqyEeMz6+dtLiA20ouy5trFl+A1tAqYU3s1q9:dSRuqNeMm64VFEb3I79 |
| MD5: | 201E484F5BD6BEFC51902BC5B26C78D3 |
| SHA1: | F85B7C13F6E9BAF140085B3E08068DBDDB869C54 |
| SHA-256: | ABD97E83940DADD68BBC598EFF1002535FCEF24F7E4CE666D3E1123F3FE97D97 |
| SHA-512: | B7618DFA97900515EC8531983641BD41B7F17576BE753A12147CD8AC1AF9366DD65B5956332F493CAB94BEF5F18F7CB8DC5882C9AB9D37473EE580F872BF397 |
| Malicious: | false |
| Preview: | .....[~Hoy retne....).....T.....3.....4M/.....v...q.....4M/.....C..M.....k.....#...(...k.....]...I....4M/.....4M/.....6<\|...@n..4M/.....<...W..J@n..4M/..<br>.....oB*@n..4M/.....a....@n..4M/.....;.y~A....4M/.....P....V....4M/.....F..=z;....4M/.....o....4M/.....*.....4M/.....2q.....4M/.....Gy.'.h.....4M/....<br>.....k7A.....4M/.....:..N.A.....4M/.....;/.....4M/.....4M/.....P[. q....4M/.....,+..._#....4M/.....J..j.....4M/.....A?.2:.....4M/.....q.....4M/.....u\]..<br>q....4M/.....!...0.o....4M/.....*.....4M/.....o..k.....4M/.....^.~..z.....4M/.....[.i..%.....4M/.....+.{..'....4M/.....@..x.....4M/.....MV3.....4M/.....*)....J:....4M/...<br>.....&.S.....4M/.....D.4.....4M/.....+.U.!..V....4M/.....~.,.4>.....4M/..... |

**C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF5fc69d.TMP (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1032 |
| Entropy (8bit): | 5.198172509346943 |
| Encrypted: | false |
| SSDEEP: | 12:VtrUxuSR3GBqyEeMz6+dtLiA20ouy5trFl+A1tAqYU3s1q9:dSRuqNeMm64VFEb3I79 |
| MD5: | 201E484F5BD6BEFC51902BC5B26C78D3 |
| SHA1: | F85B7C13F6E9BAF140085B3E08068DBDDB869C54 |
| SHA-256: | ABD97E83940DADD68BBC598EFF1002535FCEF24F7E4CE666D3E1123F3FE97D97 |
| SHA-512: | B7618DFA97900515EC8531983641BD41B7F17576BE753A12147CD8AC1AF9366DD65B5956332F493CAB94BEF5F18F7CB8DC5882C9AB9D37473EE580F872BF397 |
| Malicious: | false |
| Preview: | .....[~Hoy retne....).....T.....3.....4M/.....v...q.....4M/.....C..M.....k.....#...(...k.....]...I....4M/.....4M/.....6<\|...@n..4M/.....<...W..J@n..4M/..<br>.....oB*@n..4M/.....a....@n..4M/.....;.y~A....4M/.....P....V....4M/.....F..=z;....4M/.....o....4M/.....*.....4M/.....2q.....4M/.....Gy.'.h.....4M/....<br>.....k7A.....4M/.....:..N.A.....4M/.....;/.....4M/.....4M/.....P[. q....4M/.....,+..._#....4M/.....J..j.....4M/.....A?.2:.....4M/.....q.....4M/.....u\]..<br>q....4M/.....!...0.o....4M/.....*.....4M/.....o..k.....4M/.....^.~..z.....4M/.....[.i..%.....4M/.....+.{..'....4M/.....@..x.....4M/.....MV3.....4M/.....*)....J:....4M/...<br>.....&.S.....4M/.....D.4.....4M/.....+.U.!..V....4M/.....~.,.4>.....4M/..... |

**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): | 5.198446782887113 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 6:6xbIgq2Pwkn2nKuAl9OmbnIFUtqbx3ZmwYbxBU5kwOwkn2nKuAl9OmbjLJ:ngvYfHAahFUtq/uU55JfHAaSJ |
| MD5: | F913CB5A9C30844B96F630AA2530EF0C |
| SHA1: | 0B7DA58B1A97FBDA02C67E5CD4A22F38EF0080DC |
| SHA-256: | 6BE27E26B4795E788F551F4174D3520661212016A3B1BAB9CE5A14015DF1D3E4 |
| SHA-512: | 80DD085B4AB0486FE85680FEC7C05E504533632287A9A22A3892277B0EBE5579328A250E3D3D4CE487A4B97E1CB3A572802020601E68648233AE1ACBDB9978D5 |
| Malicious: | false |
| Preview: | 2022/11/29-17:41:11.545 14b0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/29-17:41:11.546 14b0 Recovering log #3.2022/11/29-17:41:11.547 14b0 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\LOG.old (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 292 |
| Entropy (8bit): | 5.198446782887113 |
| Encrypted: | false |
| SSDEEP: | 6:6xbIgq2Pwkn2nKuAl9OmbnIFUtqbx3ZmwYbxBU5kwOwkn2nKuAl9OmbjLJ:ngvYfHAahFUtq/uU55JfHAaSJ |
| MD5: | F913CB5A9C30844B96F630AA2530EF0C |
| SHA1: | 0B7DA58B1A97FBDA02C67E5CD4A22F38EF0080DC |
| SHA-256: | 6BE27E26B4795E788F551F4174D3520661212016A3B1BAB9CE5A14015DF1D3E4 |
| SHA-512: | 80DD085B4AB0486FE85680FEC7C05E504533632287A9A22A3892277B0EBE5579328A250E3D3D4CE487A4B97E1CB3A572802020601E68648233AE1ACBDB9978D5 |
| Malicious: | false |
| Preview: | 2022/11/29-17:41:11.545 14b0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/29-17:41:11.546 14b0 Recovering log #3.2022/11/29-17:41:11.547 14b0 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\LOG.old~RF5f4ab6.TMP (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 292 |
| Entropy (8bit): | 5.198446782887113 |
| Encrypted: | false |
| SSDEEP: | 6:6xbIgq2Pwkn2nKuAl9OmbnIFUtqbx3ZmwYbxBU5kwOwkn2nKuAl9OmbjLJ:ngvYfHAahFUtq/uU55JfHAaSJ |
| MD5: | F913CB5A9C30844B96F630AA2530EF0C |
| SHA1: | 0B7DA58B1A97FBDA02C67E5CD4A22F38EF0080DC |
| SHA-256: | 6BE27E26B4795E788F551F4174D3520661212016A3B1BAB9CE5A14015DF1D3E4 |
| SHA-512: | 80DD085B4AB0486FE85680FEC7C05E504533632287A9A22A3892277B0EBE5579328A250E3D3D4CE487A4B97E1CB3A572802020601E68648233AE1ACBDB9978D5 |
| Malicious: | false |
| Preview: | 2022/11/29-17:41:11.545 14b0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/29-17:41:11.546 14b0 Recovering log #3.2022/11/29-17:41:11.547 14b0 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): | 131072 |
| Entropy (8bit): | 0.008907738108328683 |
| Encrypted: | false |
| SSDEEP: | 3:ImtV/CuttMTLS/Jf0lt+urQTlD7vt/lcvmllP62/X:liV1kTLLlousTxvv6m |
| MD5: | 0A339004BCB425813505AE2871E61E20 |
| SHA1: | 9BDA040B5589E1B919A259DB212F4CE8E32AAA8F |
| SHA-256: | 46828E139BE167C9E36B556EB137571DE93A29930C366CE0666B1385BC106517 |
| SHA-512: | DA3CE56FFA0538D022A80F7F6DAE1E89586E27FC484E82CCCAADC9EE163BEBBEDA2CAB446D507C622BAE868086E382F5436E328418BB877FBBF0A2192CB61DF8 |
| Malicious: | false |
| Preview: | VLnk.....?.....).0k.....U....n..... |

| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-221129164109Z-201.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, cbSize 71190, bits offset 54 |
| Category: | dropped |
| Size (bytes): | 71190 |
| Entropy (8bit): | 2.0086002102959255 |
| Encrypted: | false |
| SSDEEP: | 384:+wP4F+ejQ/uz77sLnoDnK33WdAqoEeadBjmP8IbrtUr1ieEOZiEZk:+dd2njadqkiJ3t |
| MD5: | 5FC3BB896EF6797EBBA3A491024E35AC |
| SHA1: | 1B3843AA8C0BE8EE828891DECA6904BBB1CEAC8B |
| SHA-256: | A3093C4C5FCF834026B3DF3A0372E8401DC4A418DEF073B53C30A550D8131848 |
| SHA-512: | C52F0DEDB9D05E32A525217559562F86288A159E761EEC22D6104BF522187EF9E91C5D2DA5FC3E1B1E3CDDC5593ABDB1A7072F8AFAC515AE518AE5568951A768 |
| Malicious: | false |
| Preview: | BM.....6...(...u...h..... ..... ..... ..... |

| C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | SQLite 3.x database, last written using SQLite version 3024000, file counter 16, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 16 |
| Category: | dropped |
| Size (bytes): | 61440 |
| Entropy (8bit): | 3.5677719466908164 |
| Encrypted: | false |
| SSDEEP: | 384:XeT9dThftELJ8fwRRwZsLRGlKhsvXh+vSc:UkYZsLQhUSc |
| MD5: | 4A1B4B63465F84CE3850CD30CB911EAB |
| SHA1: | 498D9C87835370F086310B9049F26FC2E3D7763B |
| SHA-256: | CA5A1B1CE59C62A34CE74ACEEA1B1ADB31F6DC0431A57CCB5F84D84680B03D45 |
| SHA-512: | A65653E07B24F828BBFC3B75DC1B7DAE661F8B6A5C55ADEFD70373B22D323717BB37A0DF1A271700C2919A90DD634D2E4B77A8C4020C62726386838E3A2DB1F |
| 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: | SQLite Rollback Journal |
| Category: | dropped |
| Size (bytes): | 8720 |
| Entropy (8bit): | 3.317612279155263 |
| Encrypted: | false |
| SSDEEP: | 48:7MF2iomVQYom1C9iom8Vom1Nom1Aiom1RROiom1Com1pom1jiomVKiom7nvqQlmI:7/Cg9OhHCK8vN49IVXEBodRBkO |
| MD5: | 6F7F5AE2331FB1E74ABBE106B2145AF4 |
| SHA1: | 0CC8365F650B939DB79D1B0934BEFF9ABF77C16E |
| SHA-256: | 7961A2147E2B1CAFFAB2B736D4CD71A4CD9E9276C720E3733115F003A4D313FB |
| SHA-512: | C5A9BE3ED32C7F89EBB02C232C1755E63679EDB4FCC8BC836539D86E37B188CE6AA5925D5C86AE411231697E743DC8F41E869EC88BC681C4F84D77F51D6EE75 |
| Malicious: | false |
| Preview: | .... .c.....Xe..... .....W.... <.W.L...y.....~..... ..... |

| C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst (copy) | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 536 |

| | |
|---|---|
| Entropy (8bit): | 5.17576513886526 |
| Encrypted: | false |
| SSDEEP: | 12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa |
| MD5: | 4D5E3CD969F14362210F0473720C5528 |
| SHA1: | AFD90E9888759B809F78E87D5550B601A288A0A3 |
| SHA-256: | 79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE |
| SHA-512: | B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D64 |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont.. |

**C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.4796**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 536 |
| Entropy (8bit): | 5.17576513886526 |
| Encrypted: | false |
| SSDEEP: | 12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa |
| MD5: | 4D5E3CD969F14362210F0473720C5528 |
| SHA1: | AFD90E9888759B809F78E87D5550B601A288A0A3 |
| SHA-256: | 79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE |
| SHA-512: | B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D64 |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont.. |

**C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 536 |
| Entropy (8bit): | 5.17576513886526 |
| Encrypted: | false |
| SSDEEP: | 12:T4RFQ8idRuMgxg6dxs3yBFTtDcSTAzidRuOPgxg601s3yBFDHpcSa:kNid8HxPs3yTTtPmid8OPgx4s3yTDHBa |
| MD5: | 4D5E3CD969F14362210F0473720C5528 |
| SHA1: | AFD90E9888759B809F78E87D5550B601A288A0A3 |
| SHA-256: | 79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE |
| SHA-512: | B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D64 |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont.. |

**C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt19.lst (copy)**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 9566 |
| Entropy (8bit): | 5.226610011802065 |
| Encrypted: | false |
| SSDEEP: | 192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMlzV |
| MD5: | 63B24EA3A13EAC476D6309BB202EF459 |

| | |
|---|---|
| SHA1: | 89502C393549C20C933E4553F51F74F3DBE085EF |
| SHA-256: | 2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA |
| SHA-512: | 2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std. |

**C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.4796**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | PostScript document text |
| Category: | dropped |
| Size (bytes): | 9566 |
| Entropy (8bit): | 5.226610011802065 |
| Encrypted: | false |
| SSDEEP: | 192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdflfsmtRZEtsuatG1gMlzV |
| MD5: | 63B24EA3A13EAC476D6309BB202EF459 |
| SHA1: | 89502C393549C20C933E4553F51F74F3DBE085EF |
| SHA-256: | 2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA |
| SHA-512: | 2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC |
| Malicious: | false |
| Preview: | %!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std. |

**C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 63598 |
| Entropy (8bit): | 5.4331110334817385 |
| Encrypted: | false |
| SSDEEP: | 768:PCbGNFYGpiyVFiC0ZWso1V09Qja1X0tAUaxlOKbwcrYyu:J0GpiyVFihWsMV09QjokSbprK |
| MD5: | CA607C33342C998F309E70ACE59E08B8 |
| SHA1: | AF0E7AFE863E5AEDC3ABB8337B0A6CB7F0DB468D |
| SHA-256: | F02CA5FC07B559B5714400386978FFE690866575DC2973B4ADB79428DF060A92 |
| SHA-512: | 8AAB438E7144BAEB9C4B8016849283BAED4B4A654D53EBC4EAA6DA762B09C18A55EDC72A1411014F6F70FA538EE9D907D134A7CC841D3B38530E2EF507B5C175 |
| Malicious: | false |
| Preview: | 4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B |

# Static File Info

## General

| | |
|---|---|
| File type: | PDF document, version 1.7, 1 pages |
| Entropy (8bit): | 7.805742545381868 |
| TrID: | • Adobe Portable Document Format (5005/1) 100.00% |
| File name: | Review Document.pdf |

| | |
|---|---|
| File size: | 138518 |
| MD5: | db3d4eea0b2f092a0e3e82d317a11548 |
| SHA1: | 9ef2e56b31af6330fc71f1582a30d5ea525b8ef6 |
| SHA256: | 96f73cb2b9fa43fbe95e3d5e659a15916114d751db674dec2c9383feea861105 |
| SHA512: | ff6996d5078f90b1b895720bf79c2f48a0b3a4277898e47961bad7c3fea5bcf86a5d40234e6678632dbeb27103cb51952dfe82935ff07fc1c0ba8bbb0f99e1f6 |
| SSDEEP: | 3072:gMJjMwca+epxqGyzMPESbbDSjJLkShwlVv36QG8ME1SK39Uw+SB:txuFGds4b+klu8MEYK3SRSB |
| TLSH: | 5CD38C078C049F87E52187E5BE071DAD5B1A374CE9C136FA756E8FCB2F245259C8E02A |
| File Content Preview: | %PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 17 0 R/MarkInfo<</Marked true>>/Metadata 43 0 R/ViewerPreferences 44 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[ 3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 |

## File Icon


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

## Static PDF Info

### General

| | |
|---|---|
| Header: | %PDF-1.7 |
| Total Entropy: | 7.805743 |
| Total Bytes: | 138518 |
| Stream Entropy: | 7.809895 |
| Stream Bytes: | 133508 |
| Entropy outside Streams: | 5.252002 |
| Bytes outside Streams: | 5010 |
| Number of EOF found: | 2 |
| Bytes after EOF: | |

### Keywords Statistics

| Name | Count |
|---|---|
| obj | 24 |
| endobj | 24 |
| stream | 9 |
| endstream | 9 |
| xref | 2 |
| trailer | 2 |
| startxref | 2 |
| /Page | 1 |
| /Encrypt | 0 |
| /ObjStm | 1 |
| /URI | 4 |
| /JS | 0 |
| /JavaScript | 0 |
| /AA | 0 |
| /OpenAction | 0 |
| /AcroForm | 0 |
| /JBIG2Decode | 0 |
| /RichMedia | 0 |
| /Launch | 0 |
| /EmbeddedFile | 0 |

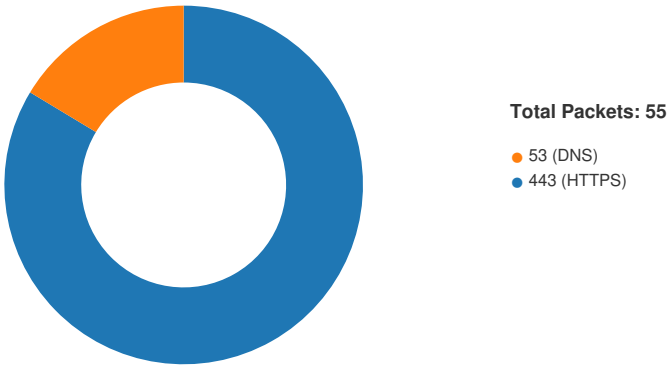
### Image Streams

| ID | DHASH | MD5 | Preview |
|---|---|---|---|
| 5 | 607070707878fcfc | 201df49e8e1f21dbcd45d435a1926a41 |  |

| ID | DHASH | MD5 | Preview |
|---|---|---|---|
| 6 | 808c8c8c8488c4c4 | d53f459021666add9032d6be0f7f398d | |
| 15 | 40d9d95d454d6540 | 01be0f5eac2196274ef01bf799bbf3e6 | Office 365 |

# Network Behavior

## Network Port Distribution




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2022 17:42:32.187824011 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.187896967 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.188015938 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.188457966 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.188488960 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.188559055 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.188716888 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.188750029 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.188819885 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.189529896 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.189564943 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.190026999 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.190057039 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.190582991 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.190604925 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.256422997 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.257113934 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.257148027 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.260226965 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.260333061 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.347170115 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.347207069 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.347759962 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.347816944 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.348031998 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.348081112 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2022 17:42:32.348334074 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.348423958 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.349189997 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.349335909 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.349400043 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.349499941 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.654258013 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.654333115 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.654541969 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.654591084 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.654613018 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.654767036 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.654799938 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.655286074 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.655317068 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.655338049 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.655452967 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.655473948 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.655627012 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.656105042 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.656141996 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.690279007 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.690432072 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.690496922 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.690551043 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.692306042 CET | 49698 | 443 | 192.168.2.4 | 142.250.203.110 |
| Nov 29, 2022 17:42:32.692346096 CET | 443 | 49698 | 142.250.203.110 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.710189104 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.710257053 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.710351944 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.710383892 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.710414886 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.710447073 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.710489988 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.711119890 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.711271048 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.711321115 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.711847067 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.711952925 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.715202093 CET | 49696 | 443 | 192.168.2.4 | 172.217.168.45 |
| Nov 29, 2022 17:42:32.715240955 CET | 443 | 49696 | 172.217.168.45 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.926748037 CET | 49699 | 443 | 192.168.2.4 | 199.36.158.100 |
| Nov 29, 2022 17:42:32.926801920 CET | 443 | 49699 | 199.36.158.100 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.266411066 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.266496897 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.266586065 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.266946077 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.266993999 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.267064095 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.267311096 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.267349005 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.267677069 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.267699957 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.368726969 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.380167961 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.380206108 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.382639885 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.382735014 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.385416985 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2022 17:42:33.386077881 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.386099100 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.386495113 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.386516094 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.386744976 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.386812925 CET | 49701 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.386821985 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.388058901 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.388179064 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.391441107 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.391457081 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.391581059 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.391701937 CET | 49702 | 443 | 192.168.2.4 | 152.199.23.37 |
| Nov 29, 2022 17:42:33.391715050 CET | 443 | 49702 | 152.199.23.37 | 192.168.2.4 |
| Nov 29, 2022 17:42:33.405064106 CET | 443 | 49701 | 152.199.23.37 | 192.168.2.4 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 29, 2022 17:42:32.069503069 CET | 56807 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:32.077249050 CET | 60686 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:32.088759899 CET | 61124 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:32.097070932 CET | 53 | 60686 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.114919901 CET | 53 | 61124 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.140862942 CET | 53 | 56807 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:32.972089052 CET | 55570 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:32.996231079 CET | 53 | 55570 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:34.660171986 CET | 61088 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:34.679291964 CET | 53 | 61088 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:35.126368046 CET | 58729 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:35.144424915 CET | 53 | 58729 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:42:35.153969049 CET | 64700 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:42:35.173648119 CET | 53 | 64700 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:43:35.195314884 CET | 52437 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:43:35.213175058 CET | 53 | 52437 | 8.8.8.8 | 192.168.2.4 |
| Nov 29, 2022 17:43:35.216938019 CET | 52825 | 53 | 192.168.2.4 | 8.8.8.8 |
| Nov 29, 2022 17:43:35.234961987 CET | 53 | 52825 | 8.8.8.8 | 192.168.2.4 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Nov 29, 2022 17:42:32.069503069 CET | 192.168.2.4 | 8.8.8.8 | 0x8f2f | Standard query (0) | passatuhen verify.web.app | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.077249050 CET | 192.168.2.4 | 8.8.8.8 | 0x22a0 | Standard query (0) | clients2.g oogle.com | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.088759899 CET | 192.168.2.4 | 8.8.8.8 | 0x50e3 | Standard query (0) | accounts.g oogle.com | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.972089052 CET | 192.168.2.4 | 8.8.8.8 | 0x2022 | Standard query (0) | aadcdn.msf tauth.net | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:34.660171986 CET | 192.168.2.4 | 8.8.8.8 | 0x8779 | Standard query (0) | aadcdn.msf tauth.net | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:35.126368046 CET | 192.168.2.4 | 8.8.8.8 | 0xaba5 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:35.153969049 CET | 192.168.2.4 | 8.8.8.8 | 0xe9a6 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:43:35.195314884 CET | 192.168.2.4 | 8.8.8.8 | 0xe87c | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:43:35.216938019 CET | 192.168.2.4 | 8.8.8.8 | 0x3875 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) | false |

## DNS Answers

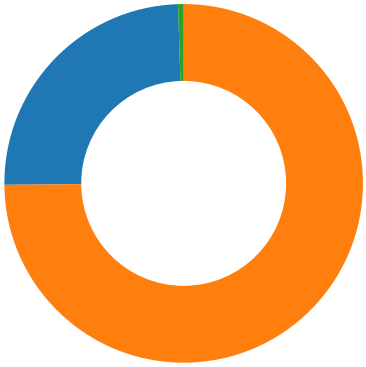
| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 29, 2022 17:42:32.097070932 CET | 8.8.8.8 | 192.168.2.4 | 0x22a0 | No error (0) | clients2.google.com | clients.l.google.com | | CNAME (Canonical name) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.097070932 CET | 8.8.8.8 | 192.168.2.4 | 0x22a0 | No error (0) | clients.l.google.com | | 142.250.203.110 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.114919901 CET | 8.8.8.8 | 192.168.2.4 | 0x50e3 | No error (0) | accounts.google.com | | 172.217.168.45 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.140862942 CET | 8.8.8.8 | 192.168.2.4 | 0x8f2f | No error (0) | passatuhenverify.web.app | | 199.36.158.100 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.996231079 CET | 8.8.8.8 | 192.168.2.4 | 0x2022 | No error (0) | aadcdn.msftauth.net | cs1100.wpc.omegacdn.net | | CNAME (Canonical name) | IN (0x0001) | false |
| Nov 29, 2022 17:42:32.996231079 CET | 8.8.8.8 | 192.168.2.4 | 0x2022 | No error (0) | cs1100.wpc.omegacdn.net | | 152.199.23.37 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:34.679291964 CET | 8.8.8.8 | 192.168.2.4 | 0x8779 | No error (0) | aadcdn.msftauth.net | cs1100.wpc.omegacdn.net | | CNAME (Canonical name) | IN (0x0001) | false |
| Nov 29, 2022 17:42:34.679291964 CET | 8.8.8.8 | 192.168.2.4 | 0x8779 | No error (0) | cs1100.wpc.omegacdn.net | | 152.199.23.37 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:35.144424915 CET | 8.8.8.8 | 192.168.2.4 | 0xaba5 | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:42:35.173648119 CET | 8.8.8.8 | 192.168.2.4 | 0xe9a6 | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:43:35.213175058 CET | 8.8.8.8 | 192.168.2.4 | 0xe87c | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) | false |
| Nov 29, 2022 17:43:35.234961987 CET | 8.8.8.8 | 192.168.2.4 | 0x3875 | No error (0) | www.google.com | | 172.217.168.36 | A (IP address) | IN (0x0001) | false |

### HTTP Request Dependency Graph

- clients2.google.com
- passatuhenverify.web.app
- accounts.google.com
- https:
  - aadcdn.msftauth.net

## Statistics

### Behavior



Click to jump to process

# System Behavior

## Analysis Process: AcroRd32.exe PID: **5016**, Parent PID: **3528**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 17:41:01 |
| Start date: | 29/11/2022 |
| 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\Review Document.pdf |
| Imagebase: | 0xc30000 |
| 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

### Registry Activities

#### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789 | success or wait | 1 | C7CF19 | RegCreateKeyW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 | success or wait | 1 | C7D41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0 | success or wait | 1 | C7D41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo | success or wait | 1 | C7D41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut | success or wait | 1 | C7D41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles | success or wait | 1 | C3EA55 | RegCreateKeyExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | success or wait | 1 | C3EA55 | RegCreateKeyExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | success or wait | 1 | C3EA55 | RegCreateKeyExW |
| \Device\HarddiskVolume4\Users\user\Desktop\Software\Adobe\Acrobat Reader\DC\TrustManager | success or wait | 1 | C7D41D | NtCreateKey |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms | success or wait | 1 | C7D41D | NtCreateKey |

#### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | aFS | unicode | DOS | success or wait | 1 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tDIText | unicode | /C/Users/user/Desktop/Review Document.pdf | success or wait | 1 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tFileName | unicode | Review Document.pdf | success or wait | 1 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | tFileSource | unicode | local | success or wait | 1 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sFileAncestors | binary | 5B 5D 00 | success or wait | 1 | C8DF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sDI | binary | 2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 52 65 76 69 65 77 20 44 6F 63 75 6D 65 6E 74 2E 70 64 66 00 | success or wait | 1 | C8DF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | sDate | binary | 44 3A 32 30 32 32 31 31 32 39 31 37 34 31 30 38 2B 30 31 27 30 30 27 00 | success or wait | 1 | C8DF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | uFileSize | dword | 138518 | success or wait | 1 | C8DF89 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1 | uPageCount | dword | 1 | success or wait | 1 | C8DF89 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | aFS | unicode | CHTTP | success or wait | 1 | C8DF47 | 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 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | tFileName | unicode | Welcome.pdf | success or wait | 1 | C8DF47 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | sFileAncestors | binary | 5B 5D 00 | success or wait | 1 | C8DF69 | 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 | C8DF69 | RegSetValueExW |
| HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2 | sDate | binary | 44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00 | success or wait | 1 | C8DF69 | RegSetValueExW |

## Analysis Process: RdrCEF.exe PID: **476**, Parent PID: **5016**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 17:41:07 |
| Start date: | 29/11/2022 |
| 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: | 0xd90000 |
| 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 |
|---|---|---|---|---|---|---|
| \pipe\com.adobe.reader.rna.user.DC.0 | unknown | 4 | success or wait | 11 | E983E5 | ReadFile |
| \pipe\com.adobe.reader.rna.user.DC.0 | unknown | 57 | success or wait | 71 | E98447 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html | unknown | 4096 | end of file | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css | unknown | 4096 | success or wait | 163 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js | unknown | 4096 | success or wait | 6 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js | unknown | 4096 | success or wait | 18 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js | unknown | 4096 | success or wait | 5 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | 12 | E859E2 | 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 | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js | unknown | 4096 | success or wait | 1622 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css | unknown | 4096 | success or wait | 43 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css | unknown | 4096 | success or wait | 8 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css | unknown | 4096 | success or wait | 5 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js | unknown | 4096 | success or wait | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js | unknown | 4096 | success or wait | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css | unknown | 4096 | success or wait | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css | unknown | 4096 | success or wait | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css | unknown | 4096 | end of file | 3 | E859E2 | 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 | 6 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js | unknown | 4096 | success or wait | 2 | E859E2 | 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 | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | 13 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js | unknown | 4096 | success or wait | 18 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | 41 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | 43 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css | unknown | 4096 | end of file | 2 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css | unknown | 4096 | success or wait | 5 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js | unknown | 4096 | success or wait | 1 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js | unknown | 4096 | success or wait | 7 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css | unknown | 4096 | end of file | 3 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css | unknown | 4096 | success or wait | 2 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css | unknown | 4096 | end of file | 2 | E859E2 | 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 | 15 | E859E2 | 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 | E859E2 | 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 | 15 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css | unknown | 4096 | success or wait | 42 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css | unknown | 4096 | success or wait | 43 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css | unknown | 4096 | end of file | 3 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | 14 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js | unknown | 4096 | success or wait | 2 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js | unknown | 4096 | end of file | 2 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js | unknown | 4096 | success or wait | 15 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js | unknown | 4096 | success or wait | 15 | E859E2 | 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 | E859E2 | 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 | 88 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js | unknown | 4096 | success or wait | 200 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | 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 | 148 | E859E2 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js | unknown | 4096 | success or wait | 178 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js | unknown | 4096 | success or wait | 215 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js | unknown | 4096 | end of file | 3 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js | unknown | 4096 | success or wait | 10 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js | unknown | 4096 | success or wait | 2 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png | unknown | 4096 | success or wait | 24 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png | unknown | 4096 | end of file | 3 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | 190 | E859E2 | 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 | E859E2 | 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 | E859E2 | 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 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg | unknown | 4096 | success or wait | 5 | E859E2 | ReadFile |
| C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg | unknown | 4096 | end of file | 2 | E859E2 | ReadFile |
| \pipe\com.adobe.reader.rna.user.DC.0 | unknown | 4 | pipe broken | 1 | E983E5 | ReadFile |

## Analysis Process: chrome.exe PID: **6948**, Parent PID: **5016**

### General

| | |
|---|---|
| Target ID: | 9 |
| Start time: | 17:42:28 |
| Start date: | 29/11/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://passatuhenverify.web.app/ |
| Imagebase: | 0x7ff683680000 |
| File size: | 2851656 bytes |
| MD5 hash: | 0FEC2748F363150DC54C1CAFFB1A9408 |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| 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 |
|---|---|---|---|---|---|---|---|---|

### Registry Activities

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

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

**Key Value Modified**

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96} | dr | unicode | 0 | 1 | success or wait | 1 | 7FF6836DA143 | RegSetValueExW |

## Analysis Process: chrome.exe PID: **7120**, Parent PID: **6948**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 17:42:29 |
| Start date: | 29/11/2022 |
| Path: | C:\Program Files\Google\Chrome\Application\chrome.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1784,i,7271988810475612612,8623558977825433660,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 |
| Imagebase: | 0x7ff683680000 |
| File size: | 2851656 bytes |
| MD5 hash: | 0FEC2748F363150DC54C1CAFFB1A9408 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| 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 |
|---|---|---|---|---|---|---|---|---|

## Disassembly

No disassembly