ID: 635346
Sample Name:
CA14522283_5480736289593760083_label.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 19:40:17
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

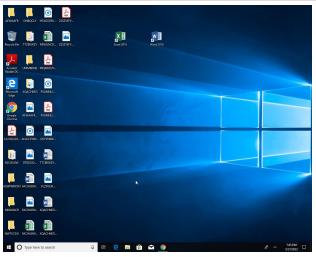
Windows Analysis Report

CA14522283_5480736289593760083_label.pdf

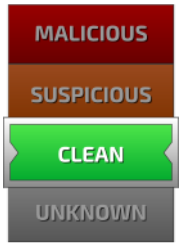
Overview

General Information

Sample Name:	CA14522283_5480736289593760083_label.pdf
Analysis ID:	635346
MD5:	cf69fb260a2a8d0..
SHA1:	ac040fbf4f22c86…
SHA256:	f61fdf68eec2a84..
Infos:	



Detection

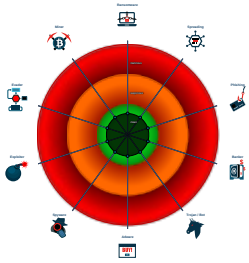


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 6396 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\CA14522283_5480736289593760083_label.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6460 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\CA14522283_5480736289593760083_label.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6572 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6780 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9883313947327340566 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9883313947327340566 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6804 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=1896595982516621214 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6868 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11556664242557579988 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=11556664242557579988 --renderer-client-id=4 --mojo-platform-channel-handle=1772 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6984 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6513707815498450385 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=6513707815498450385 --renderer-client-id=5 --mojo-platform-channel-handle=2092 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

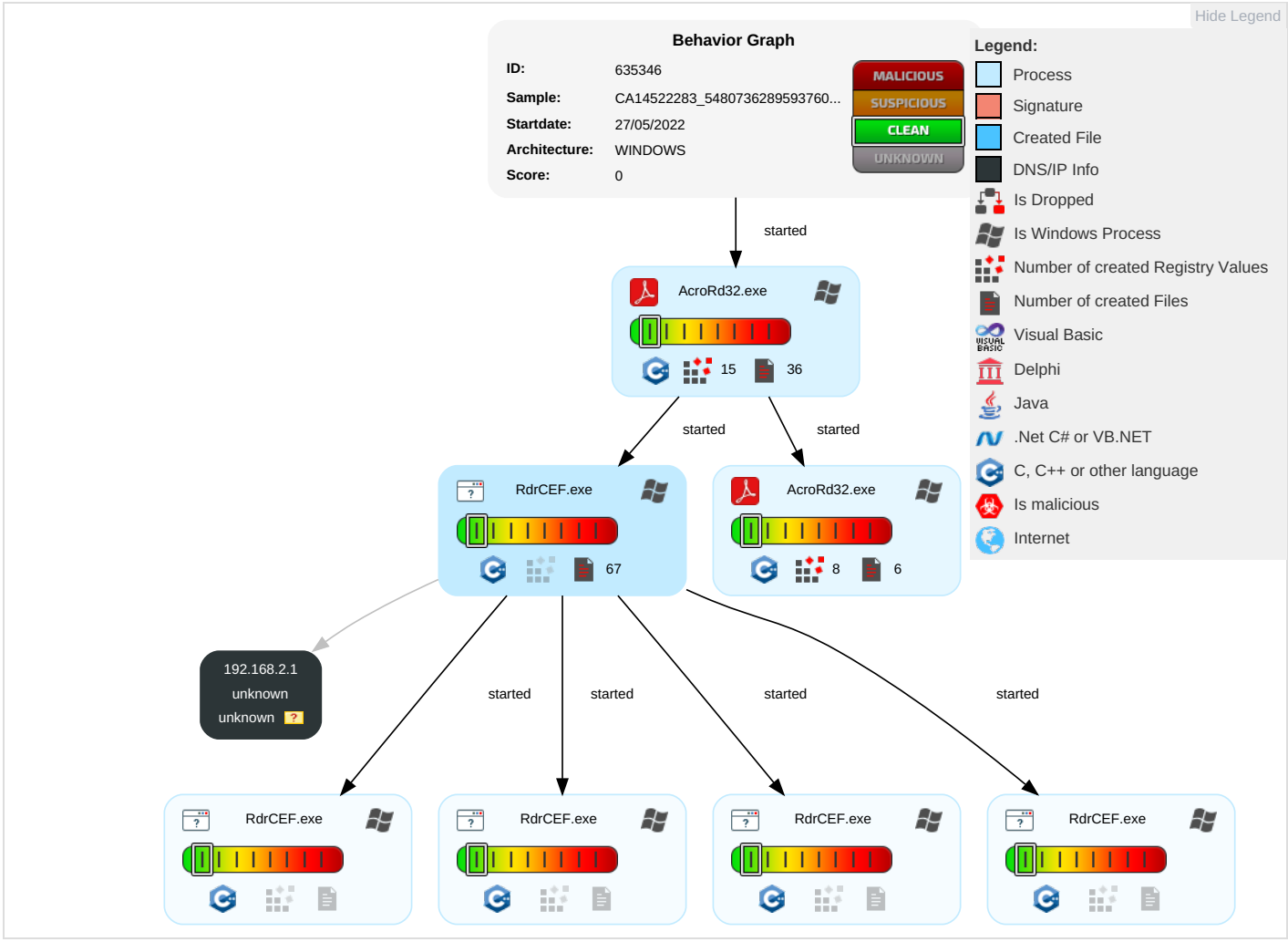
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

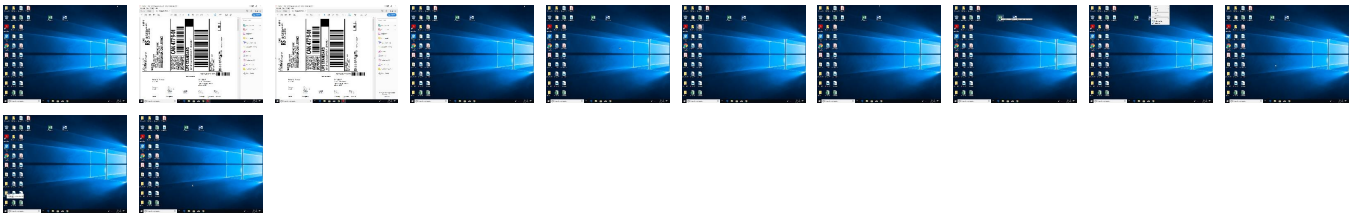
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

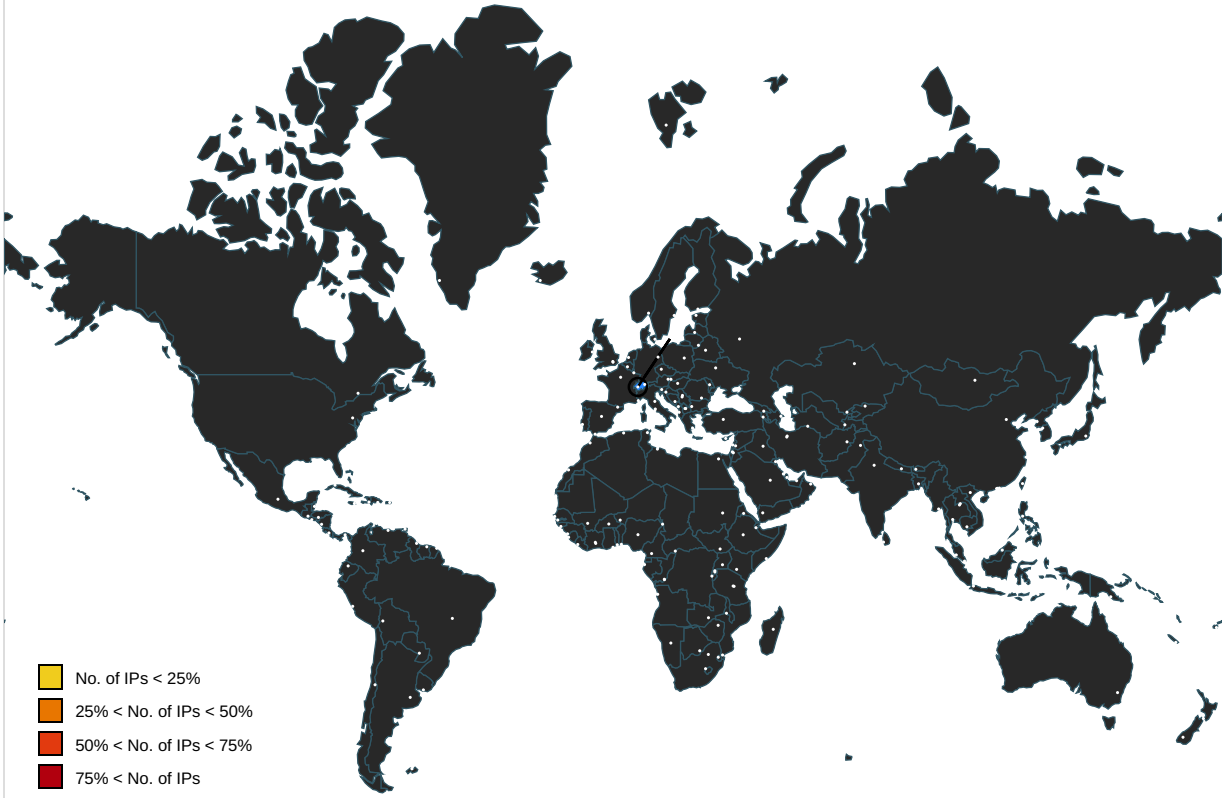
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635346
Start date and time: 27/05/202219:40:17	2022-05-27 19:40:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CA14522283_5480736289593760083_label.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winPDF@13/48@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .pdf • Adjust boot time • Enable AMSI • Found PDF document • Adobe Acrobat Reader window no longer existing • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 80.67.82.80, 80.67.82.97, 23.211.4.250
- Excluded domains from analysis (whitelisted): fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, ctldl.windowsupdate.com, arc.msn.com, acroipm2.adobe.com, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, store-images.s-microsoft.com, login.live.com, a122.dscd.akamai.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: CA14522283_5480736289593760083_label.pdf

Simulations

Behavior and APIs

Time	Type	Description
19:41:39	API Interceptor	4x 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):	5.594497140385733
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVvmbKtR290hyRktvc9xiTFJrqzOJkvPo:men9YOFLvEWdM9QkhltE9xi7Z+P41
MD5:	D955DF17BE56D8272E6FDB988195D404
SHA1:	D2386733C99109A893DA270EEB67653B3D7542AB
SHA-256:	16527786B4DAE560E46398501D8DBB386A88BF37561E1A32C838953D9CDCC056
SHA-512:	401E0CCD49F89C4DB7D712DD8AB417AC4162EB4E434038A314A26E8E2D52D9BF3670B2FB5B1454E37D08A3FE6AA0C541929DBEBB96707F4E0A4AD923F9528646
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..S..>/....."#.D....c..A.A..Eo.....Z..y.....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):	5.527536876369398
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVba6bKtaRPBG9kRktEO98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkxdBu9jtz8Be7Ywcr1
MD5:	AD25413CFDAA8060AE3F962326B6F884
SHA1:	1D66F62ADD1E6AE9B366AC4708DD4CFB219C9438
SHA-256:	BDC36A64CFC844734BEAE7AAC8D60B372C743E4B38DE514EA899939EDA5BCDEE
SHA-512:	2584C5C3C422468980AECBDBB2FC70C99DAE58A31CE9CE8F3CBFE844DFE92DB30FBD798E7DFD78CA59DE52DC6110BADC392F1BF52C6FACA6ED7024A98E6AD256
Malicious:	false
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ..q(..>/....."#.D.4>.b..A.A..Eo.....|..y.....1.x.'.vI..*|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):	5.5453520281241815
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhut/atFJFgt/RlUoSjGY1:DyeRVFAFjVFAF9aFFgtZlUo6
MD5:	AE969FA754A8015A91BF1F6CBD3F8B8A
SHA1:	9969338BC0098377A9D9B5590AAB8F393256F2FD
SHA-256:	994C94381C09D51387070F352FAB50C65CBADABCFD5F2C9C1D76FF037964646F
SHA-512:	A7E5A93209104DDDEB75B3F6870DECF4035599AC9C4D095CB9CDB8942A58215CB62AB220B35DCAF4D236F9B6B4BBE9C37580AFDC52D3F4AE853836942C4265A
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .w}..>/....."#.D..o.b..A.A..Eo.....E[$ l.....hvDO.N.t@.....n.*..... ....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):	5.4727774318653095

Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu9zK/ltnWVyh9PT41:pyixRuu/lFWV41T
MD5:	C2FCC27D20C0E01CF9904A708C11130C
SHA1:	877DDF120E243953CD77D979F60E6B6AD83FD017
SHA-256:	99566A5D1E70F1E2A7FBF431632C90E910ACFF25FB34B42545702EFD5F0FB41C
SHA-512:	82D2A8BBB876DBCE85507155FB118A451A4176026742B47D3E4A950E577A15DE8238336672FC515B908193D738BBB6A8FDC9CC2F27ED2492BBDB44FD1557177
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .AW..>/....."#.D..).c..A.A..Eo.....E.m0.....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):	5.599172196477792
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQBT+mBfathtV3ZII6P41:0Rhkyffa/tBZ
MD5:	51F85BA9D3CBACAE22F8CDB5A97F06AB
SHA1:	9DDD8946ACEF7608C6489AA9C3574EABDCB3FC7A
SHA-256:	C5649CCBB16E83607AF8D1D418DC57ED8E905E691130927C1E7B92DAF62E76C8
SHA-512:	CD7BBD7E18E252C2C450B28B497EA5C09550F144F6CC0231311095DDC77D766B845A595D6944540D80F99EC4D5F7BD7CCD23B0054406ECD5C5D51D105CBF2I 9
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .)n..>/....."#.D..H.b..A.A..Eo.....6.;.....].>....uUf..N...k.....c..l.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):	5.500209467592879
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVvucTwG/yRktuHXVcyxMtv9Ej:mJYOFLvEWdGQRQOdQ0vltuFD6g1
MD5:	F2088A2F5169E2812E8FAB530B7C73C5
SHA1:	2E7BF873FCD5AED0AAEFB347D69981F32EADD243
SHA-256:	546205F443E3F65BE42E0090E017680DE6E75FD163D8A19497CA1120E880EF32
SHA-512:	B24C5A7E2DA82A2F4FDA886ABF960A60E9AA3E947BD5F65038A253769C8E8651B781FF33530469B56CBFF4EAFF819EB89AA5FF47176D4D1F4E4D2E67B2CC93 99
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .~O..>/....."#.D.Gv.c..A.A..Eo.....!7.....c..y/L....|y.n..C/I.....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):	5.54258403017139
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVw66LJRktYu9zQMWqg4nRb7om5m1:mOYOFLvECMLKLQtYuR/41
MD5:	9D3863190E6225865662D51245294E77
SHA1:	67CB7631BD99D26B9F3908517031798F6D47F395
SHA-256:	54F32CE2FD8E2B1F8AE23AD59B6B31019C8844039F2A98DBB6C786AC67369C80
SHA-512:	3CBB4AD746E85E0750FCEF7E6A499F0AD1FDD586A48F839ED2ABAACF663CA857F57BD6BFED09E4E1876B3DA151A6EC57E3E73D739874CC2C93221539BAD6I 093
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .e.(..>/....."#.Dc.`.b..A.A..Eo.....S.....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:	modified
Size (bytes):	214
Entropy (8bit):	5.467901507912481
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuCqBG2lt+l3by0zBUKSAA1:pRWBG2lkl3b
MD5:	EFEFA232AFDE23D4CE0BB59193AC8D9E
SHA1:	A1EFB17617C71B426D9626ECA3117E2C4E543352
SHA-256:	925BF0D399260803C9AE5C5F8004E4F70113B83517CE62474088F32150D7A5DC
SHA-512:	CB8F8D986697B458B2413226F6BDAE9B25C967C67FF86576C4B0CEBB23EDDCC5B48EF9118690032CE9FA6980BCA9F7D3A2E6D669C0E9FAD2A2F55A3A49505(68
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .....>/....."#.Dpz..c..A.A..Eo.....M.....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):	5.475777950202081
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvxND/l/JBqkRktnTlWd1dn76KohyP5m1:md4HXXYOFLvEjMSWFv3Zqjtn4jUdyP41
MD5:	09FB3094ED7E7BEC90A2E5FFCB2A753D
SHA1:	328932B8C1455886C4CE9BCC6169CD69A408EE05
SHA-256:	4E7AA8F9B24329B4229BD700144569DF8431B71A5D2F90B282976FBB7A072CCD
SHA-512:	F6A16F36E0F6A9D1327060C00ECA1AF48317EDCC71B92F0AFC2FB4EF817027D54236EE31842CC553EE6033FA37C91C544515ECBD3D04F0D7A3E59F5AC2F0F6 C3
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..u(..>/....."#.D1(J.b..A.A..Eo.....ZJr.....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):	5.545288567919417
Encrypted:	false
SSDEEP:	3:m+lpSUllv8RzYOCGLvHkWBGKuK2fKVL7ow+/t9JRktdGMzUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLH+nQtdGM4PqVyM+Vl
MD5:	8D8014FD12FF0EE968C4F6AFF4A0CA80
SHA1:	4BB0B1D8D8EB4ECB0FC75A38F9AA5651D2644555
SHA-256:	D830D118BEBBED1D081E2A4B688EF5A19AFD7AC16D637A3A20805C2F1AB9E1FD
SHA-512:	3B9B9D68D921C4E48256F4FFFC9130B56C28F2300B6CC5A839682C40906A4E71A6354A93E4B7CA1E5D8493870053A30464AE2C20CD5AC7F9BE9D7714F0F56F3
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....>/....."#.D@...b..A.A..Eo.....L.....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):	5.541455106621468
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyx2xhltjqtqtwSeKaT9pr1:URVFAFjVFAFW2xhlNqItwSeKaTL
MD5:	C01AD31078D95AB65D8A1B0C3371CFEA
SHA1:	82FF1E995089B1EA32AD372CD338A4D744CDCFEC
SHA-256:	EB6DE9E7F0F434FD3CA2B5F47D4A5ECC2BC8C3A9546D30268167DBACDB9D04C2

SHA-512:	2C059DC1ED68F8933770149318B87E7C26E604C500B9F44EACF8642E5B8961ABF9AD737FE52361AFBADEBA408B1A54A856B80591C41AC0223B724B0A7D34FEB
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 .F...>/....."#.D..j.c..A.A..Eo.....1.... .....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:ms2VYOFLvEWdvBIEGdeXueReEIatBAl11:BsR2EseNbIa0
MD5:	7218C16A6C18709658FFE447D7740BBD
SHA1:	15F6DF54EA942582052E1B252CAB496E5B120E7B
SHA-256:	2AC16B77A60C7360D81AA2B7E90B19A51678712C9A70A25C26943CFB7080571A
SHA-512:	E3A3BBCB13F645317D768B2C7C44002AD11C1C61CE0EAEFE61232D03C1B013AF66F340C0532F517BD30C814D8B7F95340B68C163358AB2E151420AC082B86D6 5
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..%..>/....."#.D.;..b..A.A..Eo.....~@.U.....A.o]@r..Q.....<w.....].n\ ....A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.60825726621774
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQhONwGatPQ1xm7OhKlvA1:RbR16FaNQ1xmJ
MD5:	7FA948AFE1FEB7E2CEE98E560DB110C7
SHA1:	FE92458AB544B446CC2B626FCAC14D97712E31E6
SHA-256:	9FE8FB47A139611109575024303 4D888DCC65C5407301B4DF18CE636EF82AAF6
SHA-512:	1FB7972A9A727013A97B13969095AD736F69AD274304979FA87911FB518FF87B0F9ADD52474D04123B34E5F48400A2DE2DA9F27BCDE570E75CF718FFBBFD194A
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..j..>/....."#.D.0.b..A.A..Eo.....]].....4T].....Tw.....(..b...EO....9.A..Eo.....

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):	5.543172623522068
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVudWkHLdatHT/PdFt1:B2geRHRQ2HLda
MD5:	18A673603FAB819540C47E0DE36CDE3D
SHA1:	4E11351DE3EE98222ABBCD54F020C4B16F50A8EA
SHA-256:	B245C228092AE5A880A801655B4C2F4380B93C955F674F229F74C6DDBECB4E7B
SHA-512:	E3F699FE22D7B602CCD439DA024D08DB109CDCDDB9C201199D5218970BA6DE5D81D37BB733019D40A5B8261176BD8C118A05353C94856C130494F5642CC536
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .....>/....."#.D.z..b..A.A..Eo.....@..{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):	5.580379055643289
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVWD1tw6RktO9eEnNWQ1SUm1:mzyEYOFLvEWdrlOQQtO9eEt1S/1
MD5:	1EB8776FCF2BA9ED28ADCB2E4AFD57F2
SHA1:	FF68BF648389AD64F9E2D46D8BA4938B9EF90BA4
SHA-256:	9C26E3980B85DC5861A6DB88B5B08AE2921BD37B50D1A4F3313EF4080C7B64AB
SHA-512:	B282A6D0AADFDB0E3DA5EEC26649801D7CDA8F873F97DD2197A1E89F9ECD7C354FF8803D858EC15BB02119397367A480CEBD7ADE8519726A5A3213DE76080E EF
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .t...>/....."#.D_...b..A.A..Eo.....n.....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):	5.561063199323969
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvxtRAfvRkt+/tglwJNqww6U+5m1:mnYOFLvEWdhwyuPAfat+/KlwrqwK+41
MD5:	BE072802200ACE8C6E7573520775FD6E
SHA1:	A3433770B4E10D609B2FFCCAB704F6BB4F7E6E9A
SHA-256:	6F9195A803812469B2910F4480C95580A0A6234CA90268D1C48CFAF9FFD0FC3A
SHA-512:	2CCB176F267E6037DC68BF3EEF8D298DBD45B4FAEFCD7668A3D07D962CBA3D859C14ECCAAF842EAA3B1F25D6B950853DE4015DBE624DEA1B92E7A2975A92 D41C
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..?..>/....."#.DA.T.b..A.A..Eo.....N.....7...o..a=.98I.....(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):	5.566066343982197
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuS+p0jt7+fO441:/RrROk/xSQAfL
MD5:	5286F3CB9FFA9BDD60EBBCEB65E1D6A9
SHA1:	90697B6B88AABF1918FEBA1117358D6DDFB5C3CB
SHA-256:	4ADF2DCD153F70ECFF1733A83E6719190EDDB52F5AC0EFA99FAF64F2BA459301
SHA-512:	3CAB76B064D2D5DE55C1C957227EA3D2CA02803D645897C9D156BA3D1A12637A129D2C096386C2850A02CC66921F38B2B9A3DD95DE44D4A16BAAF33B43ABD BA
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ......>/....."#.D....b..A.A..Eo....."..]..........~..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):	5.5503956806107615
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVFUDwu9phRktAh5zoIN1OFPL4m1:mmDEYOFLvEWXIMNYt8zV1QPLr1
MD5:	598E5F002F6F167EC17BE0CFFBB18882
SHA1:	89791BAF716839E8C752F6DC3DB0A04EFF74D110
SHA-256:	DE5E238CE050E4F6AA6E0F494074714D5BAACE9A6B362E54F0769FAC375A953E
SHA-512:	47B080004E925C870BCCE9DEE0AF4CBC2DF36E68661A5119F8EF292DE9829A3B014CD6A21B7016DD484EEAA7BEBB77579EED207684FB83A8424349513FB6CB 06
Malicious:	false

Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .@....>/....."#.D....b..A.A..Eo.....c.....~]...%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):	5.626303222085497
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvKl6elHIvRkt1bY28D6EsEJeUm1:m52YOFLvEWdMAuNat1tEvsEJ41
MD5:	2BB1B9D14B38A1DB8C472B3CC40A17C6
SHA1:	0FC8119CA9A139179AB63A14D94C5CD3315D9BDA
SHA-256:	8B0EE55698790308534DB10F16560628A91D25ACFC09EA5A9602FE7B26EBCC7A
SHA-512:	6574D3027115C1F1C442993C4A98EA76964B874920A15E6AAD19BD7311D03287BF063E492C637C4A22BA34B29A2E86A28D60274BA5B672D82A0BA80177456F6E
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..S..>/....."#.D....b..A.A..Eo.....^T.....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):	5.538713843032575
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvNzelyk9kvRktBDXGFoDb7M:mYilPYOFLvEWd8CAdAudkGatBcong1
MD5:	59EB4AE4B8D5EF454609D0EB6EE69808
SHA1:	7E3620FBC6B1C9A723486072901A3FB0460EC49D
SHA-256:	ACD97180073593AB6D2633188BA070406EF1F3DADF9A16E208D604B2D19A2951
SHA-512:	1D14F8D57A55B9AEC461BBABE3058EFCE063F80FD4060A3C0366300E59506DE73E35C0B888840AC25C7A2505E0E15AF9ED2F18F8922B1EAE11E9CD1092EA91 6D
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..U..>/....."#.DS>..b..A.A..Eo.....Y.....c}.H7M=M..-.....Ix..R.l...}R l.$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):	5.57840420855166
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVlJ/2oKPWFvQ68Kt3XRktbFOe28WlJLkxb:mY8nYOFLvEWdrROk/IuXSt5N16wG1
MD5:	345CF2FF47CF04C36B0C0AB5A7C7349B
SHA1:	9704FD782225C6063A9A8CE59BAB3F6B953897CB
SHA-256:	3B8454750C93E50A200385F06155FCDC8DEDE9BDBFBAB5412911C10C93A40938
SHA-512:	6E18A84027B4A06BD5CAF318C16226FFAE0D0C93E50B2A480960BBE15C1E7EEDFA543ED77AED727E72AD27860E1994682B26CA1CDD38FE97F91BB909CD058 23
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .5....>/....."#.DL...b..A.A..Eo.....%.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):	5.6442486403724015
Encrypted:	false

SSDEEP:	6:mLrnYOFLvEWdrIoJUQ5bFiyBqjtZeJIi1:ehRccbFuj7eJI
MD5:	E81E0FF18659D71B75B088AEB5A2F156
SHA1:	CF4D924B14F861267591A13DB78E02106CCD8724
SHA-256:	8C035B8C80FCAE69ABB35DBC4FA3A813DE0A1AAA2E60EB663761E3F069AE2B9A
SHA-512:	361F53EC2600A4885F3B5F59DA971CD88F3CCB3608177318914A7B3ED52D945CB0D7DDC7916359194B379B04BE539B29D7BA81E793C821695DE36FEAFF3FC7C
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .F..>/....."#.D....b..A.A..Eo.....j,.....;".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):	5.580467582895903
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvx0Xm6MIRktidltx6mgmOZLhT79:mOEYOFLvEWdrIhub0Utin/zgm2d/1
MD5:	92B1CB6EED15E18794542B2C71769131
SHA1:	814B3150A5C1F1BCF94D0499DCB41CEF304C9FB2
SHA-256:	5BAC637EA57CF493016DD9E271D0467E6BE676FCFD7BFE7DA4A372CFB8F5C035
SHA-512:	667FFA71E2DC65D8D17AC8C9BBFC1C35468DEBAE0AF84CD963AEDCD68663D2348E49D030F4405369E75A0B4C6C19E2D84397CD966E274163D8952E6613987D9
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....>/....."#.D._..b..A.A..Eo.....v..b.....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):	5.627596988650549
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvgbuaLJRktiFleBiaQ562HvpMm1:mAElVYOFLvEW1Ktb6tiFlrx56uvp1
MD5:	3762D00EE6BC10141A14CB98A53D6AF7
SHA1:	A52B9D7AB625CCE958C41A1FF74C9361B794AE0B
SHA-256:	B2F4AAB306565E2C4D1C94651A361938A2D609B95B91DAF4936F2258107FF349
SHA-512:	19C566976C23AA9ADE924A019DBB0DC1083ECC10AC36E12F74B4D639604E1E983845C92579FA5F17D58458A69488281056D8F571B7DE756E48BE931FBFDDFDD4
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....>/....."#.D(.~.b..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):	5.653762026783217
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuK30atC9jUDLYtmOZn1:xRBJQaRDcFZ
MD5:	E3CDD1A3CF10D28E0E0AECDBDD6ECD72
SHA1:	588AA9FC7D7EA65CA3F59D2FB48E27590D156AEC
SHA-256:	D0C94487899EE53904411A7F16099A9161949E11CA58F71F7AC868659F9A10F6
SHA-512:	BDADFA79538C9A00C0B3B88385B87B80125CFE2B414B2518D6E9539A5210CE5195DBA9516D31416DF2EDB10A178447F9FDEA88D38C449E825F48C7F9C2468EDF
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..'..>/....."#.D...b..A.A..Eo.....L.=.....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.60613550093952
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFv+cq/ZLJRkt9f/npSKGoSSh:msRPYOFLvEWIa7zp7NcKLQt18VPu1
MD5:	8991E98D42524B490B83C36ED03E1C2E
SHA1:	9F563B0B9E2397EA167CC334AFA3E12F5AD94D5D
SHA-256:	B7C819593B92AB557BDC95DD99CDEE1A1BAB0839EB5B8A4AA4AD964714629104
SHA-512:	43AF11BD19ED5AD7D4AE00230B84C06BE785A2A6A71B755DD816E6BBE7A890463182C4CF761DDEEA5057FB5A96F42A562C7CA5CA785C9B63CB35C44D6276F EFF
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...(..>/....."#.Dx.`.b..A.A..Eo.....(.Z.....L...Im.@.....E.nW...IP..A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.594559544049992
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Q5bKtr5ath/CwiM3Y1:bJRT96Ktr5aH/3r
MD5:	ADDDE0E34FC888DBE5FB941CA5F4E074
SHA1:	60A6EF6DCAAF189C56D51EDED95E6E82FE07327E
SHA-256:	A3128396F27B309CD7A546167650FF4A0D6FD0BD12D8ABF1831441829623C0B3
SHA-512:	79282D3803D46300D46F8A9BE7B923FA40F6635400157C6334882DDC6E13A7F468D0CC73952D828F0FAB5358F2A33FC70334B8698DA467BCB6345493A9DF525C
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..I..>/....."#.D.Va.b..A.A..Eo.....$].....M....m+lS..e.....<7.U.P8*. 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):	5.545557534780453
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQz6qN3lt/ljBRCh/41:XRc9E3lJIDi/
MD5:	5300BB89AFDAAC58F806BDB125427F94
SHA1:	84E1C5E46F30450DD730E4329BC8F893E19387BD
SHA-256:	3AF9CD093FE376246F64A5C87E1B1435A885DB20EA008FF60B995AC56DDDD181
SHA-512:	C4CDEFE2CD68851372D44B4CF2E4B53CC8B5EB626D6F19D73198147E7F103AA5ACEA9B8FCBE2BC0C6C3F017EA5F59A41753DF9017F3DA5CB9321DB8AF4A2 78C
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....>/....."#.D-|P.c..A.A..Eo.....!.J.....PJm...0x.x..RD...BB!@5..<..]. ...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):	5.467170288774952
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvlOtllqIqyRktzzXlECcu1isLK5y:mhYOFLvEWd/aFuANqltn1EN941
MD5:	6F1A8C6BD0B977C0A33FC884A6624737
SHA1:	0F204C02D019BE6B980A669372F46387C789C99B
SHA-256:	83D23273243FBBD58701CFA635CC616C990B5F7C5D83000DE4EAEEA86EEA2A38

SHA-512:	5050AF74018489EE708EB994D4BEE5A171A8837D5658262C7DCB4F759B8FF40A98605D7429C4B77741F6976614B80BEDBA3B3A7F6E4333E0A06A42E21781B467
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .]...>/....."#.D..\.c..A.A..Eo.....u.....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):	5.504716113767317
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQl6p2lthljBMqVd3G4K41:2DRuRlolnljB9Vd2
MD5:	1F32DCA70BD38B092B48EA01EF73FAD1
SHA1:	D3544956966D346273B69347447B67E2FC4F40F4
SHA-256:	00E428E36BF379B0EDD78AFF18BB73C154B67D3123C3B6E6021360D5992F3CBB
SHA-512:	58940BE8D10BA451BFE0033F059E507DC4D40E50760CDA774EF22FF7BF3333BBBEA55CBC46FB28D2D40665056EBE39F50947DED4BE4FD5173E1F80243D008C D0
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .}...>/....."#.D..B.c..A.A..Eo.....a..=.....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):	5.554088484351692
Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVOAbusIqyRktQPW4ThzJuA4N:mkqYOFLvEWd8CAd9QpALltKuA424r1
MD5:	B45DF86F158731F8FAAACD387BFD500F
SHA1:	E9907FD5816AA28EDB7EE8E09926708AE964F5E6
SHA-256:	AC3D8505126D3DCE4E4DECDDB0F4A9218C4C380737567C64046D12B16DF88523
SHA-512:	321E5235B9AF14262DE38A65C23796E6CB7E535FAC20DF2BDD283F26A9816E198EF67030C76FF0891906EEEF082BD51A85673395F9721C4318FA6F3C4F96D35D
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....>/....."#.DF...c..A.A..Eo.....06.U.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.555357305968881
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvOIuyhqkvRktt1Ag2iHio/Mm1:moXXYOFLvEWdENUAu8IBfatt+yC8n1
MD5:	0EF7271AFD975FBA9B76839B83315528
SHA1:	4C8872D7A6DD60F3CE0EDD656AF04E7EAB1BB06F
SHA-256:	B8E99CD17CBFA649DF01493A2FDA32F7459D11DCFACA8245A63C334BF1FEEC74
SHA-512:	91E03DA58354C2D52C0B40A7B2257D40EB93901CAFA104B770E0A317E439971FE8618A22F782A7C21BA97C6C83B40B7527D869DEF13018F1A5F3080CA10ABF8
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..7..>/....."#.Dg...b..A.A..Eo.....1.....8.../...;.\\o....1.....+..A..Eo..... .....

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):	5.622305323343672
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVIJ/2kKLuV21YVRktB1sYWmYk5m1:mQZYOFLvEWdrROk/VQoctB1sLmB41
MD5:	72E1080586004D208A9D07CED16D3E48
SHA1:	F0E34FA5F01E41D2C86A25F9BF5A313B0FB3B2A0
SHA-256:	7CAB1B5112FD6BC618DDF72D5D0FCC74B4F2DAFB9B61ABEAFF1CA8D0DA476777
SHA-512:	C158D41F6529161E60FEE884D711C1C6B972353DF6A6DB3C3D6CDE54F9D0EB3BDA7B47ED473417725C8C1D775700E387131B8C6E25719EE9273727CB9039A6 E
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .....>/....."#.DL...b..A.A..Eo.....8.J..... ./.ev.....N~..6.b.....$ .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):	5.584087802070617
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWus3Dr5atABdm9741:qxRcS3Za2Bdu7
MD5:	33F2B1E3A7790A2EDE6236F24E569B61
SHA1:	FDF7E32E1002B861F679C8B16F0D331143F90CAA
SHA-256:	9DF462CB0FD69102EC8C6EA6066E01301377B2FDE3501CD5662095F172A195F4
SHA-512:	7F639603589B9B8B47D4A5E63470C1040A3E9B6330964B476118DA6B325F49B357955A634F7050B3EA6EBDAB3FADD432502C6D2FCC2DF9C39921DBE6C30A41A D
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....>/....."#.DbN|.b..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):	5.5818316592977695
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFv4F/wuiL9kvRkthJ32B6shoq+Nem1:mMOYOFLvEWdwAPVu2/EqatOB6Jn1
MD5:	E99DC97C07BBE68099B5604DD1179551
SHA1:	E808A50045B20DDAB1FCAE1B231D0E951D171227
SHA-256:	E8084F3ED0030E84BC4D05D32E78892B306AD485EA2A455F93792478E005328A
SHA-512:	1B911E1069467A56C85108E7EE031B56E0935B5498C103796524C03355D7C35AFA1B863AF4320AB94C305E0DA74D445C8CBEFE42D80709C54DB7FA775A0A190I
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .. ..>/....."#.D..%.b..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):	5.613324405878832
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQB+fQ/lt5qhcsBXIh1:mxRBJQy+fQ/lLaB
MD5:	03C2A2E92797F564B82D0D42D01EC448
SHA1:	AD4DFB905329FD1542363162EC2F8D50366FED31
SHA-256:	F26171C66D890B069E11E0CF0F005754DCA2A4295E65DE030007E59FBE463D04
SHA-512:	D2AC14FC7BE0439389DF085BB00D83486E503FA5B284B067C983CB079E6A5430C2517963429B9CA22736ECA72DCA2413380E7CEA7603AC2365EAB2B9C5C44C C
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..Q..>/....."#.D2.5.c..A.A..Eo.....NM.....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):	5.582341989883022
Encrypted:	false
SSDEEP:	3:m+l4kC8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKjXKLuVq6utdMMQGvRkt3lc3OK:msPYOFLvEWdrROk/RJUQEGat1c3Me/1
MD5:	DC9391D439392DD4258C4A53DD939CF4
SHA1:	A4D556FF6D63B75BBFC77CACDA23928104777FDE
SHA-256:	837A1D7B2F98C50E4D4E2939BAE48170204BFB3E5ED53EAB4479910807843922
SHA-512:	816717D6E8A3706F90B4A176F00D07F6DCD909FE95245B3BA33CC35032A7B6B6F38AA925A18ABB0D8E607359144BCC1834A03686DCC2351CBA8F62AC1B03224 8
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .K'...>/...."#.D.i..b..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:	dropped
Size (bytes):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/I:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F 6
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q.....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

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):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/I:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F 6
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q.....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

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):	5.264131873066937
Encrypted:	false
SSDEEP:	6:AXQL57b+q2PWXp+N2nKuAl9OmbnIFUtqVfXQL5+5ZmwYVfXQL5+tVkwOWXp+N2nC:AXQLNCvaHAahFUtiXQLQ5/IXQLQT5fHi
MD5:	542EE29EF0AB690EF85051B799148B08
SHA1:	A4BDF429F4879C2AC3613C8BB25C2BA356E18E10
SHA-256:	AC95E9A5E5C05412CEDE0AE6AFCBF7C09897EBE09A435A7CC24251C3D81CD879
SHA-512:	909F0CA1C22E59BEEA62A6E80B42D6EAD38E2338D247E8FD5478F610C7B8B21241F3E68C157B1721EA9FDB2300A781977E65CBE5242D577C193166DDDC3E7ED
Malicious:	false
Preview:	2022/05/27-19:41:45.422 19e8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/05/27-19:41:45.432 19e8 Recovering log #3.2022/05/27-19:41:45.432 19e8 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):	5.264131873066937
Encrypted:	false
SSDEEP:	6:AXQL57b+q2PWXp+N2nKuAl9OmbnIFUtqVfXQL5+5ZmwYVfXQL5+tVkwOWXp+N2nC:AXQLNCvaHAahFUtiXQLQ5/IXQLQT5fHi
MD5:	542EE29EF0AB690EF85051B799148B08
SHA1:	A4BDF429F4879C2AC3613C8BB25C2BA356E18E10
SHA-256:	AC95E9A5E5C05412CEDE0AE6AFCBF7C09897EBE09A435A7CC24251C3D81CD879
SHA-512:	909F0CA1C22E59BEEA62A6E80B42D6EAD38E2338D247E8FD5478F610C7B8B21241F3E68C157B1721EA9FDB2300A781977E65CBE5242D577C193166DDDC3E7ED
Malicious:	false
Preview:	2022/05/27-19:41:45.422 19e8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/05/27-19:41:45.432 19e8 Recovering log #3.2022/05/27-19:41:45.432 19e8 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):	0.006631749576398164
Encrypted:	false
SSDEEP:	3:ImtVz3xzb+jfyPll//F0lGQZ7XEZh:IiVzVgE//il570Zh
MD5:	978DDE022228B368660F550F28305DE2
SHA1:	805EF21B306DE8A5D245AD55812D812B187BDB4F
SHA-256:	20B4A965BAB76237F6A393347C19A6276DA04EE71C65B71447066A136D8A419B
SHA-512:	1970FBA514FEDC666E621869BE8919DB53E8BAC1BBEEECDE099D44B6FA474D9EE3E42A894C0177099D566E556858B2E6172CA8DF88FDAA8C9C9606804197D2F4
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2205280415102-237.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.8214600940282861
Encrypted:	false
SSDEEP:	96:493vrnh5mqSi/DboUagoM7fKR9vLdn1b7YnSNTlYXfdQmR+UhsUW4ySLtGIjuKWE:u/rnh5fTUCTcvL7b7GSxmyP4yxjTa5h
MD5:	4FB5D42D505B4355A2C84ABEBDBB598A
SHA1:	C0FE746E0318BEFDC432C6A4EEE01A1043575A35
SHA-256:	1904EFB0CF767AB5E2E25F63FD94D3A19DD1E08615ECA1F5F3582AEC3D7A657C

SHA-512:	6655B89C900D6E12AAF4ACA51EC3467697368391DDDF616BDFF217E84655E831F590CA40EDC1B216C027F758FD6D13EF0D61D7CF2013FA2B38E21856813AEC3E
Malicious:	false
Preview:	BMV.....6...(...k...h..... ....GGG..... .....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	61440
Entropy (8bit):	3.5634194284755845
Encrypted:	false
SSDEEP:	384:XeI9dThKBtELJ8fwRRwZsLRGlKhsvXh+vSc:iBkYZsLQhUSc
MD5:	48BD3DE75B1BC8C102BF7C5B5FA2F240
SHA1:	4910BEE3135A5D8F919A2534E39F930DAB86E2EF
SHA-256:	144DF0EA778F8749B4043AF300BD026F1490E164DB89217EC564068FD2A82AD3
SHA-512:	018B31044097746649C8EDC97F20B6211C4689FB12B1721ADE38E044B56DBDE186E0F7F1E557CE1A341C00251B9329E07605670487C018F5A9C28B93E50A0AAA
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):	3.1729666391613414
Encrypted:	false
SSDEEP:	48:7MoiomHPiom2om1Nom1Aiom1RROiom1jom1C/om1BZiomVsiomguq2RlmFTIF3Xa:7HMPOhFVCsuLR49IVXEBodRBkB
MD5:	6F6A01F1E74CDAF284C68EF9F8C56897
SHA1:	E8D4BEE74C54E43C2CA1DB58A2A0494D21D65481
SHA-256:	D5B702F633476181BD31D6074E5A73A5AE987B19C8FA192081973F570F435375
SHA-512:	AA8A18FE07EC42650C951A1CDCE8BFF7A1F8B449938AF3E4DDA396C34AAD2573000E999E9203A7D44D26052BDEC8AA98E023CC87740015274D8D1492F7810A9
Malicious:	false
Preview:	.... .c.....q..... .....X..... .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6460

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false

Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

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):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

Static File Info

General

File type:	PDF document, version 1.4
Entropy (8bit):	7.965068719987818
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	CA14522283_5480736289593760083_label.pdf
File size:	76094
MD5:	cf69fb260a2a8d06c50930a3e2dd1811
SHA1:	ac040fbf4f22c867fbada6dd6931c23b9a85fe57
SHA256:	f61fdf68eec2a84e386631c1927b1cbdcd185936a4e8d9a844a3b270dec07071
SHA512:	637a97e63ba295719ae73af3bb1645eeab3d0b75a40f5eb4039b065ca3f2e996405fbf59e5b8afda9b07453d0d06d3af8855294391b1684533f99501f3bacdf2
SSDEEP:	1536:22LcWPXujdruCUPn5NkmNlbymW1LxIdxHgvCUc7yy8:lvfHNQIvKz3y8
TLSH:	C273E0FDEB39C138FD654808EE12B974C0AA3A609BD53D4BB1650DC592C2E197C1EB74
File Content Preview:	%PDF-1.4.%.....2 0 obj.<</Filter/FlateDecode/Length 52>>stream.x.+.r..26S.00S.I.r....*T0T0.B.ij.....f.....8.'.endstream.endobj.4 0 obj.<</Contents 2 0 R/Type/Page/Resources<</ProcSet [/PDF /Text /ImageB /ImageC /ImageI]/XObject<</Xf1 1 0 R>>>>/Paren

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.965069
Total Bytes:	76094
Stream Entropy:	7.973659
Stream Bytes:	70650
Entropy outside Streams:	0.000000
Bytes outside Streams:	5444

General	
Number of EOF found:	1
Bytes after EOF:	

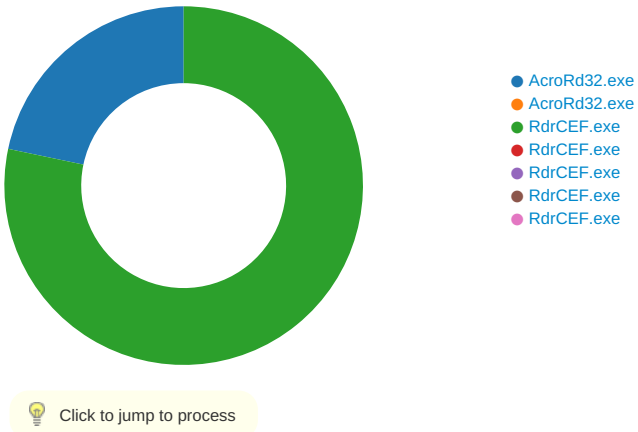
Keywords Statistics	
Name	**Count**
obj	23
endobj	23
stream	12
endstream	12
xref	1
trailer	1
startxref	1
/Page	4
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: **6396**, Parent PID: **4000**

General

Target ID:	0
Start time:	19:41:31
Start date:	27/05/2022
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\CA14522283_5480736289593760083_label.pdf
Imagebase:	0xd0000
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

Analysis Process: AcroRd32.exe PID: **6460**, Parent PID: **6396**

General

Target ID:	1
Start time:	19:41:32
Start date:	27/05/2022
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" --type=renderer /prefetch:1 "C:\Users\user\Desktop\CA14522283_5480736289593760083_label.pdf
Imagebase:	0xd0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: **6572**, Parent PID: **6396**

General

Target ID:	2
Start time:	19:41:38
Start date:	27/05/2022
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:	0x1b0000
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	3	2B83E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	14	2B8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	165	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	6	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	16	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	2	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	11	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1636	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	2A59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	5	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	2A59E2	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	2A59E2	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	3	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	17	2A59E2	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	2A59E2	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	16	2A59E2	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	2A59E2	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	40	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	45	2A59E2	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	2A59E2	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	3	2A59E2	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	3	2A59E2	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-selector.css	unknown	4096	success or wait	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	9	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	6	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	2A59E2	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	3	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	12	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	2A59E2	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	253	2A59E2	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	3	2A59E2	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	11	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	3	2A59E2	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	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	2A59E2	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	3	2A59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	2A59E2	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	2A59E2	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	23	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	488	2A59E2	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	3	2A59E2	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	2A59E2	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	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	2A59E2	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	2A59E2	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	3	2A59E2	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	3	2A59E2	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	15	2A59E2	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	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	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	5	2A59E2	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	3	2A59E2	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	198	2A59E2	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	2A59E2	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	224	2A59E2	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	3	2A59E2	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	18	2A59E2	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	3	2A59E2	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	48	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	177	2A59E2	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	2A59E2	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	2A59E2	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	2A59E2	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	15	2A59E2	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	3	2A59E2	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	3	2A59E2	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	3	2A59E2	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	6	2A59E2	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	3	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	2A59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	2A59E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	2B83E5	ReadFile

Analysis Process: RdrCEF.exe PID: **6780**, Parent PID: **6572**

General

Target ID:	4
Start time:	19:41:40
Start date:	27/05/2022
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" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9883313947327340566 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9883313947327340566 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6804, Parent PID: 6572

General

Target ID:	5
Start time:	19:41:40
Start date:	27/05/2022
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" --type=gpu-process --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=1896595982516621214 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2
Imagebase:	0x1b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6868, Parent PID: 6572

General

Target ID:	7
Start time:	19:41:41
Start date:	27/05/2022
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" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11556664242557579988 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=11556664242557579988 --renderer-client-id=4 --mojo-platform-channel-handle=1772 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6984, Parent PID: 6572

General	
Target ID:	8
Start time:	19:41:42
Start date:	27/05/2022
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" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,2511582042625791843,3130822291093567199,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6513707815498450385 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=6513707815498450385 --renderer-client-id=5 --mojo-platform-channel-handle=2092 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly