ID: 612099
Sample Name: FFL 01 EXP 09-01-23.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 15:12:33
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

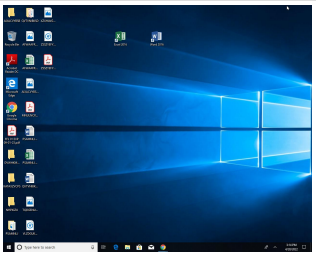
Windows Analysis Report

FFL 01 EXP 09-01-23.pdf

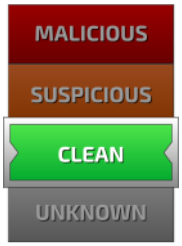
Overview

General Information

Sample Name:	FFL 01 EXP 09-01-23.pdf
Analysis ID:	612099
MD5:	1ab270f7ac3a8d..
SHA1:	892d8a649e2766.
SHA256:	1452bc811a129b..
Infos:	



Detection

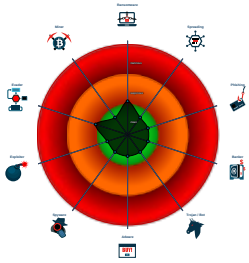


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

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\FFL 01 EXP 09-01-23.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\FFL 01 EXP 09-01-23.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6780 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7032 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1692,15095255467343264,15953424090873945641,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=7054524493282448139 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7052 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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3437087714133067519 --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=3437087714133067519 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 988 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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3988524340413199970 --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=3988524340413199970 --renderer-client-id=4 --mojo-platform-channel-handle=1820 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6116 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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10726486129092804403 --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=10726486129092804403 --renderer-client-id=5 --mojo-platform-channel-handle=1968 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6468 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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4353246954609320378 --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=4353246954609320378 --renderer-client-id=6 --mojo-platform-channel-handle=1964 --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

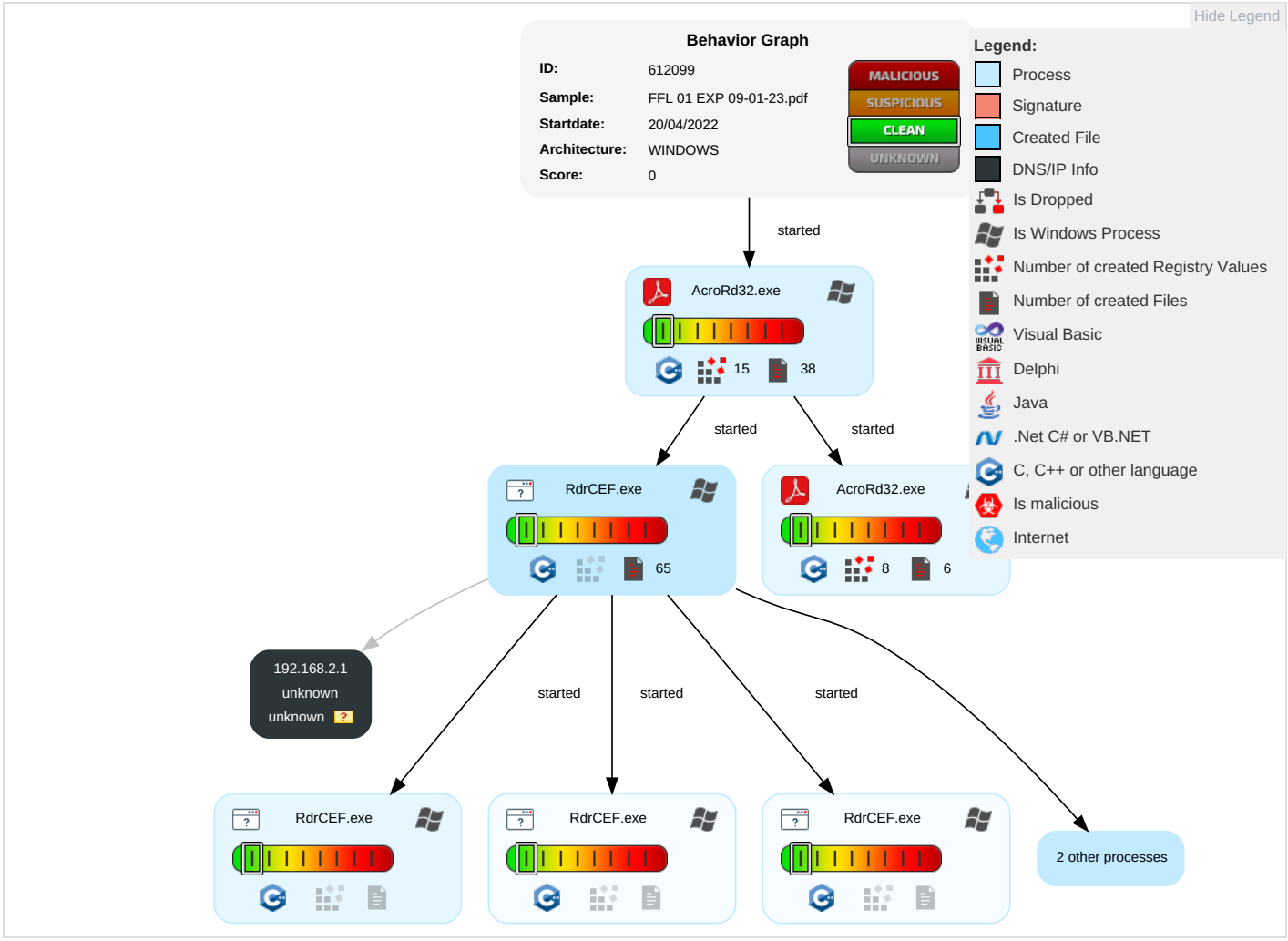
Joe Sandbox Signatures

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

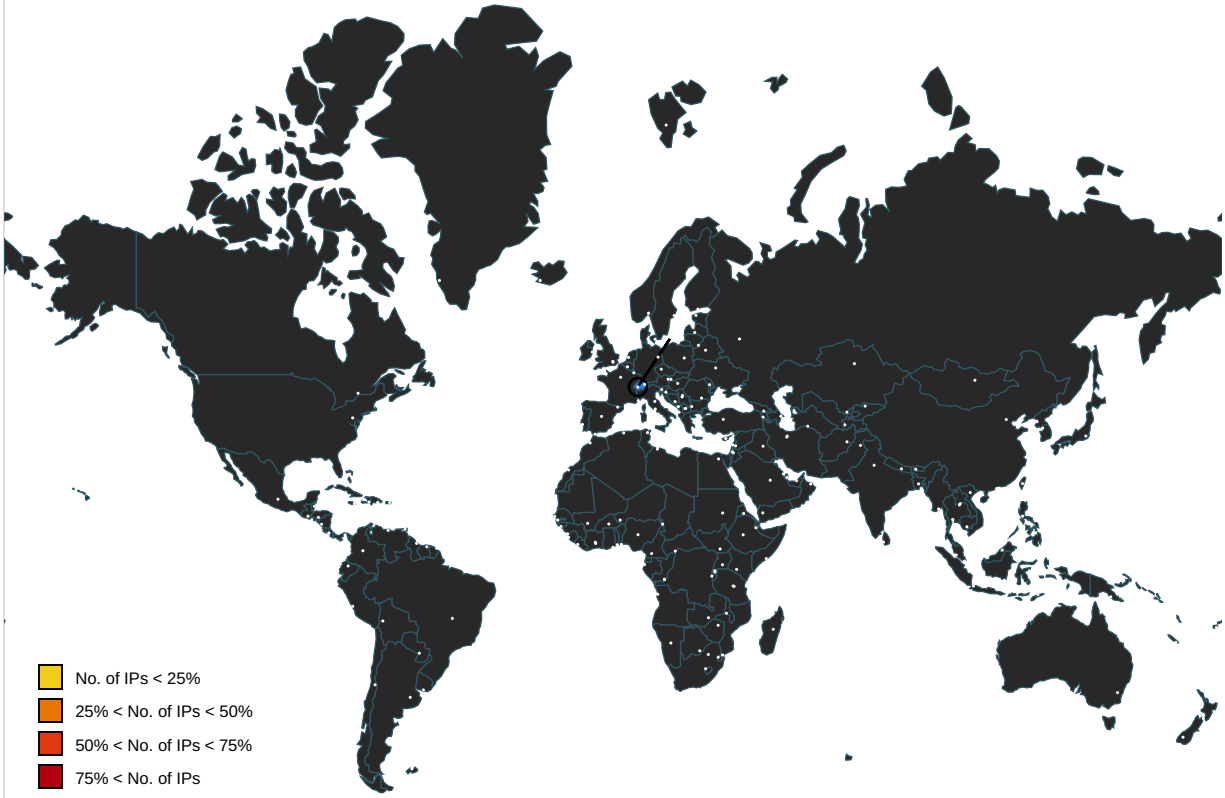
No Antivirus matches

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:	612099
Start date and time: 20/04/202215:12:33	2022-04-20 15:12:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FFL 01 EXP 09-01-23.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:	26
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@15/50@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, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 80.67.82.80, 80.67.82.97
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.com, acroipm2.adobe.com.edgesuite.net, a122.dscd.akamai.net, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, acroipm2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:14:01	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):	5.559642276835847
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVRWPllrtUGGvRktElXiTFJrqzOJkvP5y:men9YOFLvEWdM9QJeG9tElXi7Z+P41
MD5:	E7B713E118C37EB8B535A24B313232FA
SHA1:	FDFBE199FB0D8AD32DB8182BAFCCB86151FBD48C
SHA-256:	983570D5221E2A86D308926B401B2744131B6FFC156C4672B7D1848AAD7EBA4A
SHA-512:	9624C3A51BE993DCC1311C00D3F81F65D26BFCBEE5C4F3AAC005217FFC169C38A7F65A2A4EBB7D45D333CF9603DC12EEBF5C8EE6C7ABC9AA7160D4EB20CC7D86
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...M..;/....."#.D.}.p!..A.A..Eo.....Z.E.....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):	5.534692695322481
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVxSVtX199kGvRkt/lM98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEk6l9G9t/lQ8Be7Ywcr1
MD5:	92FDBFF85FCBC1F9A51D0F566CE4D395
SHA1:	CBA01C28C87947BD66840A68811CC5211004E9EB
SHA-256:	F0D3394506D5AD149FEFB34DF4EFC718FAAF29E445EDFE12F5851F4E043ACA8E
SHA-512:	E7F7B446268E54990FC46D225A877014C9CC2DA4AA7271054369B9890FEF700A8561EB42FEFB0A77BABD2B419884F72126909AFFC2DFFB006A59BDD083E68F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..!3..;/....."#.D. {p!..A.A..Eo.....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):	5.545352028124182
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuX64CUStXtot/RlUoSjGY1:DyeRVFAFjVFAFL64dSLotZlUo6
MD5:	F7D61A0E4E7D4DA14399DCB2948B48B6
SHA1:	E17C7DB9BF80BF787FF1D8CEB750BD7693267E62
SHA-256:	81CEC40B3506CDD0B82698D3CB97F729DC2CE676567EABAAF0A39DD364632F7D
SHA-512:	25BD95D9491110D5C680F06DAEE74B5EAE9C28EB911693F810334CD26C3F9B0B0CAEACD905804C1DF151F182B039AA64DB26360DAB744D455AF37F456F2DA0E1
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 ...J..;/....."#.D.].o!..A.A..Eo..... .....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):	5.546179540625291
Encrypted:	false

SSDEEP:	6:m+yiXYOFLvEWd7VlGXVuWl2AI9QtOVyh9PT41:pyixRuk2AIScV41T
MD5:	833E0A3A82D70D85E490E1967DD9522B
SHA1:	F66652F7D39C3197E50A2C6671DCA78CA810C5E6
SHA-256:	80CD515F6F83E1F4D9530256EB62F862A1F5FA85D09F5D8D9035FB29BF4A6680
SHA-512:	E8AE5D953599B4C90E649FF28F95E85668CC2D0784BC1C3142464EA7ED79A0625C94F90103CBB50101F2E0DB54C98D2E604A1A3FC9D35E1629AC7B5268AB441A
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..CL..;/....."#.D..p!..A.A..Eo.....~p.....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):	5.57046973842122
Encrypted:	false
SSDEEP:	3:m+lifIl08RzYOCGLvHkWBGKuKjXKoyNjXKLuVYHi0kRkt0ll3lYo2sZI8xeGvP5y:mvYOFLvEWdhwjQoQtclV3ZIl6P41
MD5:	AD5D5B460DC5E98DEB0135A0B7854F4C
SHA1:	9EE687A21F84FB50BCF6F4E675F9B113B4551736
SHA-256:	480485968452B00B6392CBFE526D69A81E75D6C38D23F1BCAD24B8C085084A32
SHA-512:	6F945D0C892C77BB4857B15CEF6EBC4A68254DD374A8F6727FC05B5051747C2C5ACC6EAE1D5DDECF36265B1AFACCE3A5137C5EE1A05B0874C742C859C145F1B
Malicious:	false
Preview:	0\r..m.....X.....V...._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ....;/....."#.D/n.q!..A.A..Eo.....].>....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):	5.500341624969354
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVLpHVlllntxUG6Rktu9cyxMtg:mJYOFLvEWdGQRQOdQM1TxUG9tqD6g1
MD5:	60A16133E8495523ACB38AA511DFACC5
SHA1:	0EA505E4009461B3F0860D82D29DA6C9012CF17A
SHA-256:	55434050B86EC693D237803F5C93F63D45555A3559CCEEE82C9FE94A789A9CE1
SHA-512:	5F4508250B7E549BA1D10DB53BE40130AA0A577926B33FA887A1BA2C78F5CA80537ADF8E889A82234C930A7835108D77337EC16463F024D34CDE2E9FA9C5967
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .XLL..;/....."#.D.H.o!..A.A..Eo.....8.....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):	5.561271057925279
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVD7Zuk8dvRktA9lXVQMWqg4nRb7om5m1:mOYOFLvECMLZ/8QtAHeuR/41
MD5:	53DF756972A42983ECB9C119FAF1D43E
SHA1:	38F126E1A5FB5DA738E7275D51727EA391F5F0B4
SHA-256:	DEE17A272ACD6DBCEBB36DAF6981A4013E2CC01D61C4341A83062C2C55B4D43F
SHA-512:	F0183612B0EFC586153B5E79A98C45E2A103EA527338F8ACE1AB5A683F04D6160DDD5F0ECFB73F6A71B83C5A675B6A2C7AC42481D7F72BD5944B3C076D1D521
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..*3..;/....."#.D..p!..A.A..Eo.....v.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.65099008157377
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAudilooO7tXOMGm0bbsIDMGH41:XfRM6lM7NOMVKsIZ
MD5:	AAA7789F22456CC1188E3231DABDDCA1
SHA1:	13BAA5B6A98E24420F7FC06B02C941C9E22FCC66
SHA-256:	4CB47B3995248EB5FE72B3E611693DD1DFD44E27245AA19B1FFFCCE339E69EEC
SHA-512:	AF5C0BCECBF2755A6F0EA5E3D83ADBA1CF8A272A879C181C9F91CA5827D605E5331E9D0BC49C1A5C7D7C0FC9EE2A37B2DEC616C1CED95CC28B8EA6CC2710A6A4
Malicious:	false
Preview:	0\r..m.....T.....,^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .....;/....."#.D...q!..A.A..Eo.....zZ.....`....^....L>..Xa./.....C.y.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):	5.519567742542207
Encrypted:	false
SSDEEP:	3:m+lS8FlC8RzYOCGLvHkWBGKuKjXKSO7p/KPWFvSI3v//fkGvRktpFYuuUy0tlBU1:m4fPYOFLvEWdtu9k9tdby0zBUKSAA1
MD5:	14D0FC581B48397E508E62B15F2D059D
SHA1:	CB2B39D4353B8ED77FF7435FF212CC774E248E68
SHA-256:	F52A36B10C467997ECAD632B4A06E5F71B6AF7AFA7D79492833C80C2DAA6A8CC
SHA-512:	434842D41F0C1B40AB2FB4C0EE88199F9A824C39033B530FD4BB1620CC3F68640F191299392DC1E54046EF724CE6D0721C26C740D04304BDD4B2ADD514D6765
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .7.R..;/....."#.D..7p!..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):	5.493547707420876
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvFZju1vRktjEd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvLhtjEjUdyP41
MD5:	B1B223DDF2521C143A174F6B384009CA
SHA1:	61230D1A5CAA4161F459FD4951AB4191E1F76DBE
SHA-256:	3ED6F6C00A6F5D5A8E2AA099758FFA76A4524E770D9F2A01D232ABC9A454832B
SHA-512:	D53A5D445B4C20CAB16FC12AC3E84284FD91EE03C69F5A61ADAF3A2AA8B9460804C474D74799B414E33D4DFC36E0A2F8AAF38D8AB62D1FA82937B213A3090071
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..%3..;/....."#.D.W.p!..A.A..Eo.....c.....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):	5.566678942250968
Encrypted:	false
SSDEEP:	3:m+lpSUllv8RzYOCGLvHkWBGKuK2fKVL0nVtfFUXRktuhUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOL0VdxtuCPqVyM+VY1
MD5:	1D7769221087AC3D4C4A11DA9748C1B3
SHA1:	FF799EA716A1A8770A94D00C99711B2DC286C27C
SHA-256:	313EC4E18B860F6B3394EDAE6C61994CC7D12FE3A6FA7C8273CA0A8251126722
SHA-512:	8B5DA48915074C556C2CA33111760FC647D17F9D846ACF11150415867082F1C5128DA2ECFD23719EB5BB38413713AA4DC790B1DE4C3614DA5E6897409C33F463

Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .(....;/....."#.D...q!..A.A..Eo.....Q.*>.....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):	5.602619933850661
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFly8WAG9tHtwSeKaT9pr1:URVFAFjVFAFLWn9twSeKaTL
MD5:	9F12FD941D9B035A28BF7FFCBA463C33
SHA1:	71440FB30442BA380E3294F29B5C2F5A9A7D6C67
SHA-256:	1CFB46412F07990D68D3E43F3C4FA122583D5297990CD273C0264ED449780B50
SHA-512:	D0AC814E228049DDF1BE7DD1E38D1C90C238B33DD86AF84C88E72D20792A65F8C0E5258CC480FA38AC28B586032CE349AB406124E57FAA40DA886201CC9713 4
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 ..GL..;/....."#.D.+.p!..A.A..Eo.....!..(.....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	210
Entropy (8bit):	5.565683448958373
Encrypted:	false
SSDEEP:	3:m+llys8RzYOCGLvHkWBGKuKjXKmbKPHJXKLuVZZK/ljvmRktXc6kV5t0FCV66zus:mq9YOFLvEWdzAHdQ+0ZtMt5GFCaa+41
MD5:	8E024E6D13D74A33745D979B21F825AD
SHA1:	7BBAEDEF7E59EE2A605A0423EC766400D7D24C57
SHA-256:	B18303F99B605FC64FC63B01CCF66AA8F28552D6DB22DFFDB8B81BD5E10A6F0D
SHA-512:	B3C8FBBA8201830BD83241E9356C402FA20C6C7046EF690C94893851E91164F2094CB8E68CC26C60A749EDAB4AB2142D8D5734ECADBA4963DC77E27F87E48D 9
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ..!..;/....."#.D...q!..A.A..Eo.....G.3D.....Q.g0...._.Q.....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):	5.48255735619504
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvs6nBRktRhyrpYFm1:ms2VYOFLvEWdvBIEGdeXuO64ti11
MD5:	2BFC8DFA0684D4F688703FFD3B15FA3C
SHA1:	E625C8415686DE9682F0F02541D6B3BBD0F9065F
SHA-256:	BDC594E8B2837AD06EF3315336D796D27CF5F782046E790F7298B4B3FB33E37D
SHA-512:	FFD2A59785EFC798FA8A80EE04A5A84B54027C1046BAA05108FC0435ACDC6791CDC87EC04CB17A3E1290B78A9088924D413044590E4231CE1229A8E6541C196
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .toK..;/....."#.D=C.o!..A.A..Eo.....).....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):	5.661499283555183

Encrypted:	false
SSDEEP:	3:m+lOy08RzYOCGLvHkWBGKuKjXKrAUWCKLuVpVtzkRktUdRx4Z/7Ov9PPKMkvg4m1:maVYOFLvEWdwAPCQgntUTxm7OhKlvA1
MD5:	8247E8767DD86DBB28AE4C35D32EC23E
SHA1:	29D736EDC5C18ECF331FF96B804225D3595BFDF4
SHA-256:	2673A96AA2EB42376FB86D347298B8E5A7DB71CD0BF1CF42F2851017B1D6ACEB
SHA-512:	DC4F0EF006E360ED76F587AE3FAB086C5B4951A79660AEBCBAAF80F5757B5A28D58EE09F820D797D2E0A83D54F88E57B99CE2CE4ACFC348985601036F97605 3
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .8...;/....."#.Dh .q!..A.A..Eo.....F.....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):	5.5325490457012805
Encrypted:	false
SSDEEP:	3:m+lx2gv8RzYOCGLvHkWBGKuKjXKX7KoQRA/KWEKPWFvL/CvRktKlVdF5YufMm1:ms2gEYOFLvEWdGQRQVuVht+VdFt1
MD5:	7A1E6E6BB8DAE88546285075F710B435
SHA1:	55680E878A2B894D42A27AA7652E6006D1F00625
SHA-256:	8A0FAAC4F19E5082ED41DB41CE051B8E69471FB6C0C0AC995D0E14EA78C480EB
SHA-512:	FAFB0BE289604E3B00BAD975929D3FEEB7AAF708BFC8341794C96A1A2EFF1FD51C3ED519ABC8D55F41D4991A5DDB23C2D5032B2F55D387E9313E57F2EBF28 B1
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .BmK...;/....."#.Dgc.p!..A.A..Eo.....2.....@..{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):	5.523299322246135
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVcP/K6Rkt84EnNWQ1SUm1:mzyEYOFLvEWdrIOQ1POtzEt1S/1
MD5:	D2A51127F813915F83EC490E7F3AAF9A
SHA1:	53B6F4D0975C7ECB266771DB4B272CCD7517F9E3
SHA-256:	B1597631B29D837C5EB934CD98B98D07089D9C9F998325D3EE42C67BC1F91E17
SHA-512:	3D7474F4F8BC338D7B0B13EE2E661BC38B4A1CA44AE0E47E9135D35D0C6FA662D6F06B9130AB56C57D8D0132BB1C46155D21FC03D07C0EA656051249246B9E 3
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..a...;/....."#.D.. q!..A.A..Eo.....`..A.....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):	5.572486249762836
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuziSHWKk9trlwrqwK+41:wRhEx2lNqGwK+
MD5:	A924F101CC67E2C523440C698EFB9EBE
SHA1:	C643022B3FCFC0EC0DFA1899C4929E6B82B74372
SHA-256:	B1FCCE3EFC5657DECE4DDBFB7EB68409A34E5FCA05B74DEECA10BE3E40433E5C
SHA-512:	92B93921BC9A9EB3DFCC8C61CE92CCFC42285E82AF481E2F53E9DA21433BA54AE3F459355B5D6A71CDFA8411E2A28D64EB410705A7DE71171731B7831BB5A0 AB
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .<....;/....."#.D..yq!..A.A..Eo.....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):	5.5470901353882835
Encrypted:	false
SSDEEP:	3:m+l26Xa8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKH/KPWFvK+t6+UG6RktQlbX8c:mYXYOFLvEWdrROk/RJbu1EY9t9fO441
MD5:	38034640001517C06E0200A6320C0660
SHA1:	C2F8A18BCBB1EDDC7168E4982629B28838257DC8
SHA-256:	0357FDA69E390FA43872088BFAA3D465A8F27A2F6C0EB3B365F2B76CE368C5D7
SHA-512:	826C02ABA523CC82D78282AB2B26700DDA9C8D0E3D80E565616AB50E811CC010C4E3E2509302EFEB33E0EAD520ED404A57F091D2912F603217521F88A2D2B15C
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..`...;/....."#.D..-q!..A.A..Eo.....wm.....~..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):	5.5780582990394
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVOgZKtIGUG6RktE+llllpzoIN1OFPL4m1:mmDEYOFLvEWXIOghg9tE+llllpzV1QP9
MD5:	08ADDDAD86A0DE9329C459123476DDC1
SHA1:	19A04DA3A7EB074B6E1497693CA3E24A2CF71846
SHA-256:	7A683C3D7807B951AD968800CB4E36EDB01CB68C01B1F12D7905C6C8936CDCF1
SHA-512:	FEB9961021D8B305ECC3215550FB6F85F3E0E849B18C4BD8348779403DDA64688A2BEE316FA69FDE7F6928228D3441442BB57B8C47C3E24A38BE7463126F1D94
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....;/....."#.D.y.q!..A.A..Eo.....W.....~]...%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):	5.568645886656855
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvfSWeu3VE9fvRkt0llu8D6EsEJeUy:m52YOFLvEWdMAu1le4yStcMEvsEJ41
MD5:	4B615F95B3280764FD65DB23FA8332FB
SHA1:	BDA895FBC269B4160CA7111FAEA21D14825F1D5F
SHA-256:	9E228912FF209DAB352806F483092407702834AEA940AF006AC8C6F0E2FD0E3C
SHA-512:	33ACE65C12CABF4A69CD90D72A91F6A57DE3F1E0431E34FA25E41EF4269536ACEA6751F6834FFDFF4E25F3710EF55E7B012A2FDB0B82F4C99EBA8A47D5CCA87E
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .:sK..;/....."#.DC7Op!..A.A..Eo.....Z.....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):	5.557086655175068
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFv4n6+ndvRktO2FoDb7T2/My:mYilPYOFLvEWd8CAdAuz+nQtHong1
MD5:	26BFE8B502990E8D6434685342955B43

SHA1:	70538E5E05753CF8F9024702F16BE42ACC5E6A93
SHA-256:	8DE766971557FF4B2CDAA24A86E28F8C3394AF78D69EC891933089A90E1687E7
SHA-512:	2EEC1322B32908FD04FA47148FC7253463BBE3F0536F93615DBF0D48FF4B4B2600C7FA1F9D6810AFD4AFB34782159741D1134FF3375D33C8097A04C784EC4F88
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..K..;/....."#.D..+p!..A.A..Eo.....Yc.z.....c}.H7M=M..-.....Ix..R.I...}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):	5.549300060589001
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVlJ/2oKPWFv2bBuURktPBflDOe28WlJLkB:mY8nYOFLvEWdrROk/luq+tPB1N16wG1
MD5:	CEB3941283A55F09EF3FBC354AB05559
SHA1:	580709D6CED19AE9E7B295E2E58E08F2A9A0140D
SHA-256:	9F45FC3E9E6A860522BB886C9D1DF10BF9B5B4C3E45130C5CBCC20715057F937
SHA-512:	481433EA1E3D1DA70D37B2B8E2B1CE517987BB286EE1543EE07F266CF16C2212BE63E9ED97E058CD1F6981578CE4729820E52CABC75571DF3F8B961087C3180
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..>...;/....."#.D..]q!..A.A..Eo.....A.....%.k.SZ..~W.....:)'B..a d.....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):	5.594225062757123
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVtWP/eUUXRktU9XlmPmJec:mLrnYOFLvEWdrIoJUQWWPWqtU2eJli1
MD5:	D4EBE1814C32F4C4EEE2895D33764AE9
SHA1:	24CF1A84B78A5BA88B36144052FE9478BC84AC4F
SHA-256:	17D42486E9186BD835D06600086C163E184DD4D2093659B4E37A199EAC2899A9
SHA-512:	AEA29FFE6875122357408AA02278AEC7CE808265E31D9DF46A3D1C682D12A4528F9E6003CF313527E730D8E89BCCCB6BAF647F50CB997D03D83A92C6F4E0423 3
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .;c...;/....."#.D..9q!..A.A..Eo.....n.....;"./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):	5.542006044434366
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvVkc/H+uE9G6RktoH/lx6mgmOZb:mOEYOFLvEWdrIhu/X0otoNxzgm2d/1
MD5:	15578233663F668625157B329E6EA2DD
SHA1:	ABB4304DA409C172B6AB8B2EE6FF1E792D907C7F
SHA-256:	2F615774B4D0C66FAEC5F194D0D5B5ECB5C681D9723D618331703A87219CD423
SHA-512:	F63FDF164DD805513B249422F99570420ACB4ADFEBCB675D0CE55FEFB4E2A55FA56345BD85396A1DD8F0E9BA1C61E8DCA8C60D1F77CA215420B897848BC6C 38
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .0=...;/....."#.D.[q!..A.A..Eo.....~.\.....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):	5.565621007510105
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvwZKl/JyG9kvRktOollleBiaQ562HvpMm1:mAElVYOFLvEW1K9+gqjtPllpx56uvp1
MD5:	B3E6AABD3EF08E2961FC001A7AEE3D9D
SHA1:	F358253DCD71AC9B78070F36FD6CC003582D3919
SHA-256:	BC54986DABCCE48FBC7FCAFD5336D1F462D30DF7CD65A73521F13572E312B871
SHA-512:	353ECFD43DC890B930C1F9C2ACB41A0F95E66ACCC6DEA7474BCE7782ADAC06207F5A753F1A8469777142CAEEBD4084CA4F5A81249661E265A15CCB4A79A18EB
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .(....;/....."#.Dj/.p!..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):	5.6038973797595855
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvucYmt9jtxjUDLYtmOZn1:xRBJfv7noDcFZ
MD5:	75C0B090F108D18C199BA0AE51C4C5CC
SHA1:	422CD096876906220BF2603249754D30A14147D5
SHA-256:	F6D4A3DDFCFA0A62587EF8CDBB1E6FBD75BC4455D162A7E8E296E16ECE88C5D4
SHA-512:	CEAC7927BD38BF0A6546A9E377EA0F8AEDFAAEEFD0563389F11EA7EA9C6E93985CD8B13A11ACFA018F235CBA2F8804766125671361344451E4BEF29077BBB673C
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .cqK..;/....."#.D...p!..A.A..Eo.....s.....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):	5.5557471860307555
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFve7WnXepkvRktUnpSKGoSSh:msRPYOFLvEWIa7zp7N7FjtK8VPu1
MD5:	B1E5846A137696F9ACBD4327ECBBD136
SHA1:	045091258D27967BEA9F82915B9A8370BF009342
SHA-256:	DC21E2D14989F3090CF7A56FE700AA7D743C2EEE9EE52D9C4CD70EAEE296BDE0
SHA-512:	2E734D8AD21C04AEBA09C9DBEA3C4281BF3CF789861805CA73AD860C21AE3A8DBB390633403AB7D8BF72320D86C53FAC14A34BA05E61BF931695E5E1A3BBFAB1
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .5.3..;/....."#.D.u.p!..A.A..Eo.....-C.....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):	5.590930277212668
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVSudl12Rktp196F4XVAZ+8cV3vA:mKPYOFLvEWdENU9Q5u3tAwiM3Y1
MD5:	13CB3B34C865F9880600972F6F5FEF43
SHA1:	BB6E5BF88A27AFAE4B11ABDF2FA3036BEDA6F2F1
SHA-256:	3F04C59B6B3DC94321E0156CCB0D3E5D38231CCAC80046542E06BF274B4622DD
SHA-512:	B2EC298BF1A743667171F871F3F2F1E29F2FB891E9605FC983C82F3FE36FE9E5E5065911487761664488 86A9B86D23F691E48BC58712C62F8CAF579C50331ECA
Malicious:	false

Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .`.7..;/....."#.D.X.o!..A.A..Eo.....O.....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):	5.6078041955027
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQFl9QtElwjBRCh/41:XRc9cQ3Di/
MD5:	20647C6995457871B6A466A333BB44E8
SHA1:	8DB187A0AB9DD386CA16A52A3D57AAD1B264765B
SHA-256:	CE944901058C34E1EE3C716FFFA2C926E5F140A2681B44B6E3B4C9B1ACE9FD54
SHA-512:	4A8D2E6C0D10474BC69E0B90EE2A7E5EF61C0A1BCBB417BB4A3B51F4904A245AC6AB23A74D4C90352F16D86C10D3CC977CAA5F261358256CCF3DF044267DB 94
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..IL..;/....."#.D...p!..A.A..Eo.....Y.....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):	5.491468295863016
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvIuRkVUGGvRktoNlECcu1isLK5m1:mhYOFLvEWd/aFu67tonEN941
MD5:	BC6E6B833F8CCCEC19835FA5DC05FA02
SHA1:	DAFC73F35F1D7C55416564AEDA8BFAC8D5C45632
SHA-256:	D21CC7670C5A92B6D756AE535B898305058FED9A98C54269C4B2FA72AD13B515
SHA-512:	0F7BDD7A57A59DB35C7001ABE83670A0588506FAFC78CF5ACA7DA09217D5F538A6AB4A0642AA4F39C33D5A46E00C30BEC173F88AF17B1A382A6213CB7CA29E 6F
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .I6S..;/....."#.D..lp!..A.A..Eo.....v.....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):	5.526236590580155
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ89jtHlBMqVd3G4K41:2DRuRx9jvB9Vd2
MD5:	E88CEF281EA20B166BDD1A5B6DE38CA5
SHA1:	5D327F8049F87029591C26D580E1D71226B8C94C
SHA-256:	7AD25155D39AFA5DD6CBF58CB101E39199845A5F350CB1A30C8DC62DAF813554
SHA-512:	355CE423D320DC27214FF40A1CA50D90D24E8EB8042E7A96170C79F81EAF9F9EF545E2511E1B95617BF4B0CA38E305D6175FE6D0FA57C28780AE9EF41DF9FD9 7
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .. M..;/....."#.D..Bp!..A.A..Eo.....^..h.....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):	5.56853717146886

Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVFhWV/l8M9kvRktunW4ThzJS:mkqYOFLvEWd8CAd9QFC8jtuNuA424r1
MD5:	7612800B28CA985FE92DCE777CED49C5
SHA1:	720F033F1C9066992360D04B4598119E66518075
SHA-256:	41A28FE82AD85F46C49D4F9943B3EF94847249CED7EE5149026FD0B714E26873
SHA-512:	9B9FBCF9DF8A624A3B893F65D41276575B636B5C255323448BAEBF1C7469E3DC278B84C50C76E7054CA4312263850250CCB543B59F9D4EE73C2F00B25E42BF0
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .t.M..;/....."#.D9..p!..A.A..Eo.....|.....#..@..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):	5.535049389271308
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvGA+upH9k6RktzDUrAg2iHio9:moXXYOFLvEWdENUAuNG9tzIkyC8n1
MD5:	C78DB27DB2030FC685324638CC149A0D
SHA1:	9E561E86444985273B414694722FB53E99250C8D
SHA-256:	CDF4890631844991507032755 7EAF5B5884CA4B7EB53BBA52CE0F31E3C64D182
SHA-512:	D8D4279860168FD25B7FCA65216EF90AB33783E16E27FF4FE1302D9C8ED75D5954939177D09AA7517C7560A24DB1CF642630A6DBF44DA72B3BF8D5465C2782E
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .#h...;/....."#.D.#.q!..A.A..Eo.....ff1.....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):	5.563570255509528
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVIJ/2kKLuVn8tjfRkt6y3XsYWmYk5m1:mQZYOFLvEWdrROk/VQrqtDHsLmB41
MD5:	20BA1175E0C49F013D37B9A75F9BE97D
SHA1:	75784CB0BF3CA56BE745AAE39854276550E06334
SHA-256:	39132D3D86FF02329DDB291B53445410B3765AFAF4B729E86C3FAAA2B9D635FB
SHA-512:	52AF1A41C5C4F59A71C0D12EB84CAF1536891A945D53AD00C5D77913E5B24E76B3AD7C7D5A6F3738073EA24A4C4789D30189AEC10C7FFBBDCBC34B22DC3D4 32
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....;/....."#.DAGEq!..A.A..Eo.....Ker..... ./.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):	5.526270138022635
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuhSHK7tytJdm9741:qxRc7SgkJdu7
MD5:	797486BD5CF8492F0FB8D9C347BF9669
SHA1:	34494BFF44BA8AB4E4376D8B8892C594076A12A1
SHA-256:	14E06A47BCE78C20A8BE9FB547283306FEE474AD3A823420797A595721CE0A1A
SHA-512:	7483E133B74815F3B1A4BBF5996D46B95F852B65B6F53B7F578C44E0A218FA3DA5985244F78CA9287648091AC1233284FCC1AF0BDE69A541DB9B2AB4BCBBC36 D
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..FK..;/....."#.D...o!..A.A..Eo.....U...I.>P...X...x..0U.~;m.x.k.A..E o.....

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):	5.509708896934059
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvHm8UlzXRkt0AEB6shoq+Nem1:mMOYOFLvEWdwAPVutL4StWB6Jn1
MD5:	A8E2764CB88EC98295B94DD59C83BC16
SHA1:	B6FD0A19D8C60134016F886EE8B61F1F14E89B45
SHA-256:	E5135695F6EC30D41DDC765D4AA2B3F5162582F13B479EEFBCE85100F1FD959B
SHA-512:	8C53C730203482DC091255FA46DFB4F1499E3C8C1B17A8DABF84271E3AEAF67021A0B873B0125F5CEFD82C4AE7FC19E3D581E3C11AA211C8339C21F92D1040E 9
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .".6..;/....."#.D...o!..A.A..Eo.....a#.....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):	5.607909560102804
Encrypted:	false
SSDEEP:	3:m+lUDfllla8RzYOCGLvHkWBGKuKjXKBRSJvBCvlKLuVNp80/ldE1vRktfllAN6:m3PXYOFLvEWdBJvYQ4tfl/qhcsBXIh1
MD5:	F4649F52F8DF4C16531F7AF2D6D5BD26
SHA1:	6D54658D27D573D889EE5C9BB5A873775B8D2916
SHA-256:	DDF603CBE76806ACEE2E6FCE34E6191F9C94754E07EACCDE6F45504E9FFAF018
SHA-512:	C5952AC0D137F8D3A9A391FEAC2E9831D52C3EBEFD9F5F7A083103C3A5B28D40C79516868CDA5E0C2C9F5E9D66A65A63367FFB86EEE6306AD93541D0DE7BF 5F
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..iL..;/....."#.D..]p!..A.A..Eo.....U\.....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):	5.5472542705847765
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQpvjotfkLc3Me/1:3RrROk/skoCL
MD5:	F89B2CC4EFE00EC714C94B29211E8518
SHA1:	8331D386217EEE9B7ABF6FD692CB0FE7DD57C032
SHA-256:	5DA9B06CE1BC23795190C789EDB9610FE30BD4A0F4AFF77BB64227AECAD9B2FE
SHA-512:	C001A92A7525A7667BE02563E29EC5208635820A6A4B4064A06B03501082B68E87E731BDE38726D9C77D2B3711E0815A7BFC0ECED886CC3831F68CA3A9C946E
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....;/....."#.D..Qq!..A.A..Eo.....#.py.....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:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
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:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
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):	5.268097042107263
Encrypted:	false
SSDEEP:	6:tJoq2PWXp+N2nKuAl9OmbnIFUtqVADZmwYVAZkwOWXp+N2nKuAl9OmbjLJ:tavaHAahFUtfD/1Z5fHAaSJ
MD5:	0EFA5FD57DCE06939345B459EADB80A3
SHA1:	C15C7FACFC2BE05DCE14B6C51F9622F62FF6BD65
SHA-256:	1C439D7D00DD1E33BD6C40550224B34E32F56534C5DB864290898F872DD65867
SHA-512:	BD68FA268C9DB11AA46D1D4AA0FA626C92EC5237B2D49E50AFA0BFDC74018769C4D31DB8E7AB120B9E5EC35223536224F4363FA1A3E5A6EE1656C44AB28A0867
Malicious:	false
Preview:	2022/04/20-15:14:13.677 1964 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/04/20-15:14:13.695 1964 Recovering log #3.2022/04/20-15:14:13.695 1964 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\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):	5.268097042107263
Encrypted:	false
SSDEEP:	6:tJoq2PWXp+N2nKuAl9OmbnIFUtqVADZmwYVAZkwOWXp+N2nKuAl9OmbjLJ:tavaHAahFUtfD/1Z5fHAaSJ
MD5:	0EFA5FD57DCE06939345B459EADB80A3
SHA1:	C15C7FACFC2BE05DCE14B6C51F9622F62FF6BD65
SHA-256:	1C439D7D00DD1E33BD6C40550224B34E32F56534C5DB864290898F872DD65867
SHA-512:	BD68FA268C9DB11AA46D1D4AA0FA626C92EC5237B2D49E50AFA0BFDC74018769C4D31DB8E7AB120B9E5EC35223536224F4363FA1A3E5A6EE1656C44AB28A0867
Malicious:	false

Preview:	2022/04/20-15:14:13.677 1964 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/04/20-15:14:13.695 1964 Recovering log #3.2022/04/20-15:14:13.695 1964 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.007705831707200586
Encrypted:	false
SSDEEP:	3:ImtV+Xb+jfyPll//zVrzlltD0lGQZ7XEZh:IiV+LgE//hFwl570Zh
MD5:	6ABF41DD4C73D60E4EE0BC302380FF61
SHA1:	98728D541712597763CBF6095060D35B40458E6C
SHA-256:	FA8AFA872E00F6E06A1ACE8A9B23124370BED970A87E4F97C78791A96D36FE32
SHA-512:	FFB9A0250FCAE05F2C8BBAA5DF0541E2D4E3552DB246EE8A20F32CFA689982B2E6DBDB0F0CEE03594D7EF4C914E6F9FE8EA37843BD9911178115F6A8C1AC0DC8
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2204202338172-213.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	4.314967755741964
Encrypted:	false
SSDEEP:	1536:lRImFqyRH5UZPvAhqGoV8D+c9bonKJPrtbj2:lRIanUlAQV8DrcSJbi
MD5:	B1800B3207FD260F85FB2C0F7DBD9AAC
SHA1:	B90FD8EF217FFFE79D0B74C2FA8D6E382FA8DE3F
SHA-256:	30787C8915BE24FCC466BA18BB713962BAB4A6A1FB73468C2D5B5F441E9141D2
SHA-512:	ECA64D2ADEC74E7F2948ECF8E2E9042EEE6CD8EF667CA9F347BEADFD16D013BD061DA3AF2484551C61C99D025F4C89847D1C4C573AC19255B2C7C9A382D881D
Malicious:	false
Preview:	BM.....6...(...u...h..... ....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	61440
Entropy (8bit):	3.5651685899976724
Encrypted:	false
SSDEEP:	384:3eI9dThntELJ8fwRRwZsLRGlKhsvXh+vSc:PkYZsLQhUSc
MD5:	911BB650E47850AADEF326826011CB88
SHA1:	D4727CA3F0D76295B1E3AB1E807EBF0301E11DAA
SHA-256:	D9726D6BE56F4F34CF3E404A37E2FB3B501EE0136CDE6B7DAA8530C079C3CFB2
SHA-512:	A996B8A8B2F06D027B82DC34AE5FF5D715D911414E715A9EE7154EC343038E72FFED03A3BB8B60CB90F99835C3A6A6C6BB1EDA19E32A5494B442C661A8B8E291
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):	3.2893472813648263
Encrypted:	false
SSDEEP:	48:7MHom1CYJiom0Jiom2om1Nom1Aiom1RROiom1oom1pom1HZiomVsiomgfqQlmFTs:7xKbOhrCsfN49IVXEBodRBkA
MD5:	FBEDE9693928B18FF80CA0DE1F45EF5C
SHA1:	15F257A390000B7DCF0F9FAC20AF8CF5AB0B08DB
SHA-256:	B1AD402F7020886D44634D6A06FAB5CDE3D4AB399256303266523FCF673D80AB
SHA-512:	36C51D4DB3196196CC23E7AFF4D6D04E98D0CC72F2D5CC9C994E70F0EF6AEEEF01B0D7E3991739D53783383769D54367381D5611E983E2D64F9A60D5F9F7038
Malicious:	false
Preview:	.... .c..... .....s..... L.s.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:Ar ial.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:Ro man.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:Ar ial.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:Ro man.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 1.6
Entropy (8bit):	7.8968139696396875
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	FFL 01 EXP 09-01-23.pdf
File size:	265785
MD5:	1ab270f7ac3a8d224acbced342aaa036
SHA1:	892d8a649e2766e828d5d199154742c470feb695
SHA256:	1452bc811a129bacb51f0161c982506f61b71ffb1880256ce32d43ee40af052b
SHA512:	41212f8d14a5592a2d88302445da59bf99c2579394e93737c70786fee5d91ea44d50d84f10bb5b99dd8f94076700974ba7402f2291a61c250ae2a066b7c48d95
SSDEEP:	6144:fu6tKQeTOi8bcUb7R6GrhSMij8rQuBQyFbi/y/mb/:fu6tKbTr8bRIG4jkRBQyFbEy/q/
TLSH:	4044E1362635E293513687485EB85E3DF03A6E42756FBB20B9DF4EFE6B62E530142304
File Content Preview:	%PDF-1.6.%.....31 0 obj.<</Filter/FlateDecode/First 5/Length 172/N 1/Type/ObjStm>>stream..h.d....0...W.on...4...4I(.2...t.H\.I._.....q....+M.ZN...h.Tc..A..G....B.9.1.....:n.u..>....<.1..^.....~..U?wB.....d.0.....r.c.^SC.[K3.R.;@....0....s...&.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

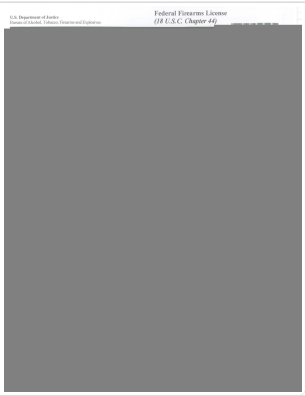
Header:	%PDF-1.6
Total Entropy:	7.896814
Total Bytes:	265785
Stream Entropy:	7.896357
Stream Bytes:	264536
Entropy outside Streams:	0.000000
Bytes outside Streams:	1249
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	11
endobj	11
stream	10
endstream	10
xref	0
trailer	0
startxref	1
/Page	0
/Encrypt	0
/ObjStm	4
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview

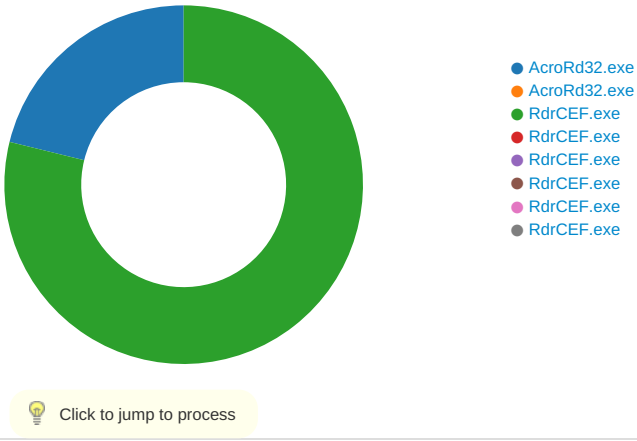
ID	DHASH	MD5	Preview
22	4323165f59912727	948645102d971cb52661f61415a8100d	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 6396, Parent PID: 2912

General

Target ID:	0
Start time:	15:13:52
Start date:	20/04/2022
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\FFL 01 EXP 09-01-23.pdf
Imagebase:	0x1290000
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:	15:13:53
Start date:	20/04/2022
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\FFL 01 EXP 09-01-23.pdf
Imagebase:	0x1290000
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: **6780**, Parent PID: **6396**

General

Target ID:	6
Start time:	15:13:59
Start date:	20/04/2022
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:	0x240000
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	4	3483E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	32	348447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	165	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	5	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	13	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1621	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	43	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	3359E2	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	3359E2	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	end of file	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	17	3359E2	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	3359E2	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	3359E2	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	3359E2	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	44	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	3359E2	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	3359E2	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	8	3359E2	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	3359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	5	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3	3359E2	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	3359E2	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	3359E2	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	3359E2	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	254	3359E2	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	3359E2	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	12	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	14	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	477	3359E2	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	3359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	40	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	3359E2	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	3	3359E2	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	3359E2	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	132	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	3359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	144	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	3359E2	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	3359E2	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	3359E2	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	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	4	3359E2	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	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	14	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	3359E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	3483E5	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	3	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	23	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	5	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	1	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	5	3359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	1	3359E2	ReadFile

Analysis Process: RdrCEF.exe PID: **7032**, Parent PID: **6780**

General

Target ID:	8
Start time:	15:14:01
Start date:	20/04/2022
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=1692,15095255467343264,15953424090873945641,131072 --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 =KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=7054524493282448139 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2
Imagebase:	0x240000
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: **7052**, Parent PID: **6780**

General

Target ID:	9
Start time:	15:14:02
Start date:	20/04/2022
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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3437087714133067519 --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=3437087714133067519 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x240000
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: **988**, Parent PID: **6780**

General

Target ID:	11
Start time:	15:14:03
Start date:	20/04/2022
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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3988524340413199970 --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=3988524340413199970 --renderer-client-id=4 --mojo-platform-channel-handle=1820 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x240000
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: **6116**, Parent PID: **6780**

General	
Target ID:	13
Start time:	15:14:03
Start date:	20/04/2022
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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10726486129092804403 --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=10726486129092804403 --renderer-client-id=5 --mojo-platform-channel-handle=1968 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x240000
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: **6468**, Parent PID: **6780**

General	
Target ID:	17
Start time:	15:14:30
Start date:	20/04/2022
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=1692,15095255467343264,15953424090873945641,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4353246954609320378 --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=4353246954609320378 --renderer-client-id=6 --mojo-platform-channel-handle=1964 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x240000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly