ID: 534014
Sample Name: 404.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 00:29:36
Date: 05/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

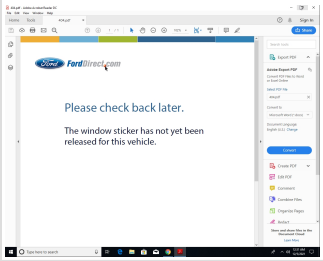
Windows Analysis Report 404.pdf

Overview

General Information

Sample Name:	404.pdf
Analysis ID:	534014
MD5:	d838d040fd7877c.
SHA1:	6f520b71773361a.
SHA256:	21979c27f520821.
Infos:	

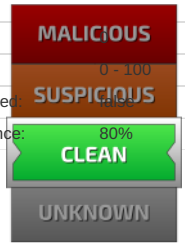
Most interesting Screenshot:



Errors

- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database
- Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service
- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP
- Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog
- Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell Script Exfil
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Detection

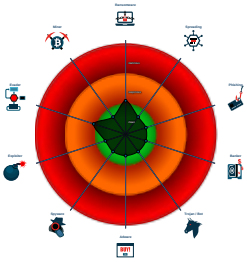


Score:	
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 7136 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\404.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5076 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\404.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 2248 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5376 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,17932346825100363335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10825893705877279914 --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=10825893705877279914 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6792 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1700,17932346825100363335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=2127389532984776761 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6880 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,17932346825100363335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15934386517068702169 --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=15934386517068702169 --renderer-client-id=4 --mojo-platform-channel-handle=1820 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 1244 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,17932346825100363335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5360389963267492183 --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=5360389963267492183 --renderer-client-id=5 --mojo-platform-channel-handle=1968 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 3396 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,17932346825100363335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4148878045607610064 --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=4148878045607610064 --renderer-client-id=6 --mojo-platform-channel-handle=2976 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

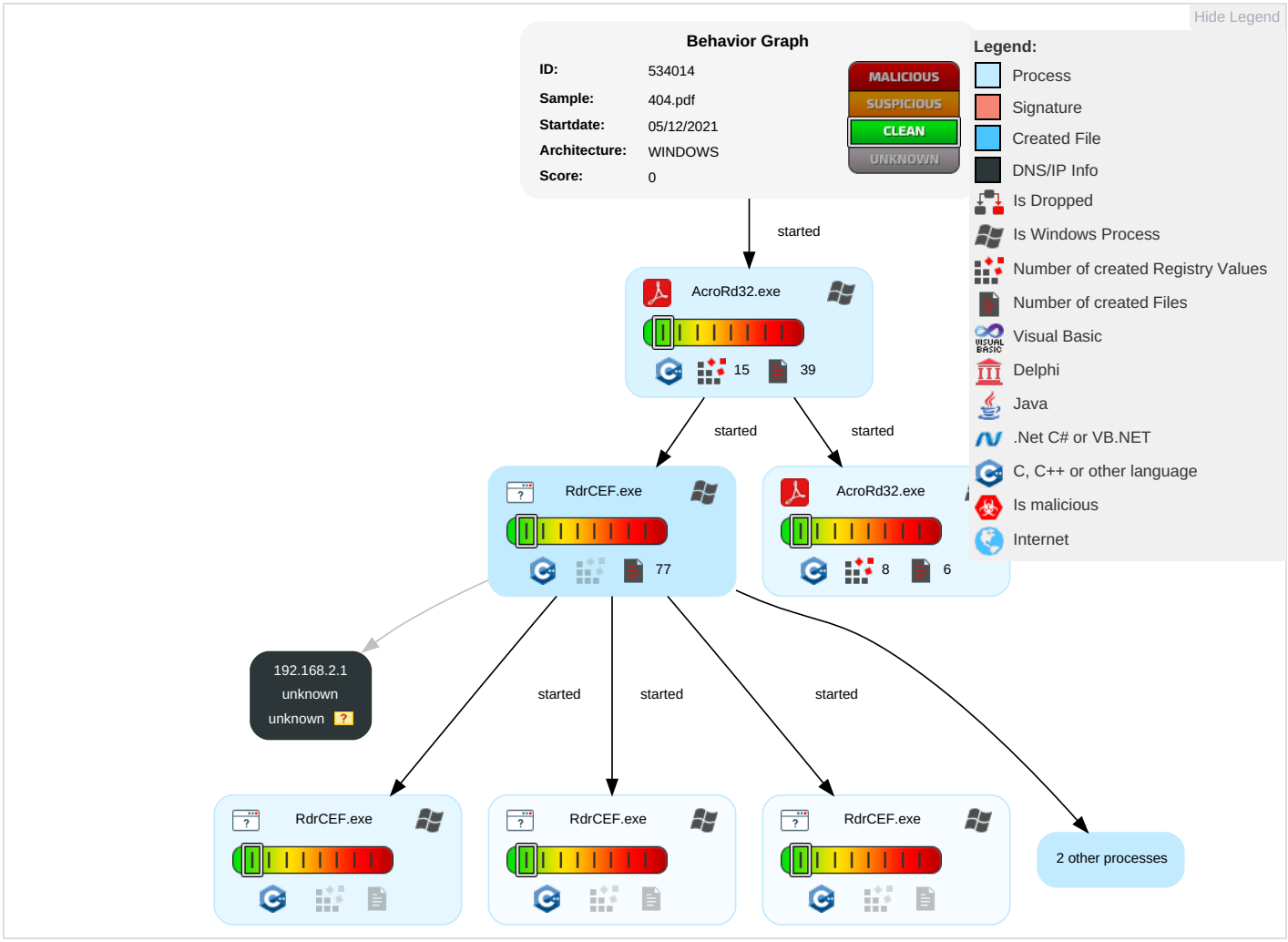
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	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

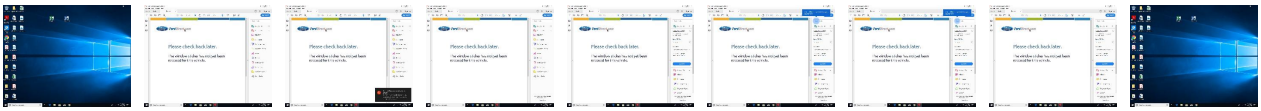
Behavior Graph

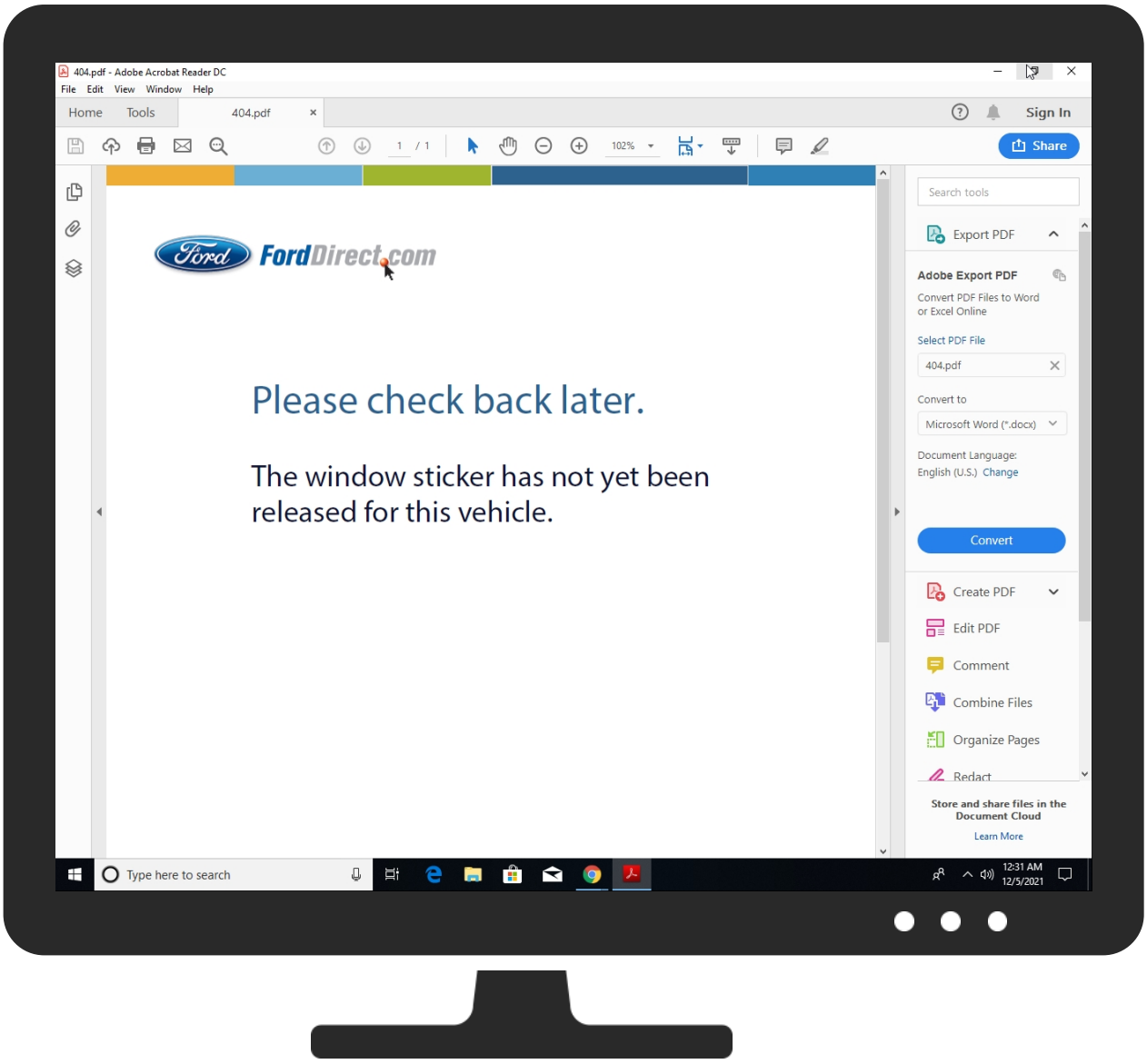


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
404.pdf	0%	Virustotal		Browse
404.pdf	0%	ReversingLabs		

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

Contacted IPs

Public

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:	534014
Start date:	05.12.2021
Start time:	00:29:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	404.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:	31
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@15/54@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:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Close Viewer
Warnings:	Show All
Errors:	• Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database • Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service • Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP • Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog • Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell SAM Copy • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Simulations

Behavior and APIs

Time	Type	Description
00:30:34	API Interceptor	12x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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):	5.631752073879002
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVYsbdgwsF9hMktFlXiTFJrqzOJkvP5m1:men9YOFLvEWdM9QHasHjtfXi7Z+P41
MD5:	5197B742C579186C905045B441D8CD41
SHA1:	F19F4ED8CE69166241A733BE8335B70FC8DAD0B1
SHA-256:	67A434E3E6CADFA6C1280567F5C790832DDF56B568E5A3F615891B7452D9E418
SHA-512:	954324718D7EBE62C5D906A6955342EAEDE360EAFE98722EE78346BDCC429BB83A1A56DEE7580E2B9D4D7B12887D15F313D4FAABE278D7D6CBDF47C99BB7C97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..z.>.0/....."#.D..C3.k.A.A..Eo.....=.....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):	5.539031129242961
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVZ+/1yXxhMktpH/lle98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEk2yX5tRy8Be7Ywcr1
MD5:	E4DAD6CBA5A47F97426C3ED8C537362A
SHA1:	97C3EBA6EB89A1328F0B5FBCD6339752025303AD
SHA-256:	13B1A9E80FCF7615F4109286CA307CC6A22E4BED4CAA064A221D8FFCD956A561
SHA-512:	20C72B489FB0EC8791660DAD757D12A7E7782E46B36E2DD0E306BA0DFB1F533510172BC7A329CCCE7D2F19621A118F6F1AC25DA492AE813EBDAA46D5FCB13A42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .<.>.0/....."#.DB..2.k.A.A..Eo.....A.S*.....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):	5.543359243588924
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuBUjtret/RlUoSjGY1:DyeRVFAFjVFAFlUjUtZlUo6
MD5:	AE4BED58C20783954FD9EF397281BC16
SHA1:	1BA7C6FCBB419CA8B39943F128123F1133683C10
SHA-256:	1D6AE5B418AC40492F58E7857016FC2C171AAE9CA21C4D069B5538CF9218C178
SHA-512:	F404D8475622D39A8BF86416DF3E668BB00AAE87B533F6ACCD81023A0F7611247AF5EF089189035BF29343DD8FCC198CBF09B7F57F6C961A37334546110A63C6
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 ....>.0/....."#.D.^<3.k.A.A..Eo.....n .....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.611503383286171
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsB0FOG9tiVuiWulHyA1:IbRkiDtFOG90jWus
MD5:	C8B7C338861DDA6B3979E8CDA466CFA7
SHA1:	123FC61D7C1B304C3DF66E75646D86DB38BB4CA9
SHA-256:	327BFB9508753B4CAA383B5A615ADA3AA8DAF15277173665DA34071A7DABCD3E
SHA-512:	F7BF34B1834ADD7A71237BFBC231961D8B8C5D764F4A6196E1EEE41D5626C513696BC9425D5CDBAC7863E2A4170E04D110415D32CF17B5C30B3E212685AC120
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .$p.>.0/....."#.D.o,2.k.A.A..Eo.....8 P..a...R.. Y....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5474398382752454
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuv/t2Vyh9PT41:pyixRu1cV41T
MD5:	2DE00A9F34A90A00EC8D8F7489CD4862
SHA1:	8031B306046DDC323058CD33793DD10D5CD63AC0
SHA-256:	B16303124195CF6DA243440F95A4179E88F1FB7EFD28FBF888075B936F714CF0
SHA-512:	BA272E7685EA366D68EB9A5E816B5595487F8E9FC4D1D2A63729D08AE384F8B323A59712538D81E752C0B0321ADB18995506C9EE85A3109F23099BCDB77939A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .^..>.0/....."#.D..;3.k.A.A..Eo.....}.%.....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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.539272006976839
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuV9sdg/SmvMktFlxlYo2sZI8xeGvA:mvYOFLvEWdhwjQd3mNtFV3ZIl6P41
MD5:	AB62A5236C3CC2C31069BDCB39754049
SHA1:	8B234CCB4D7D3B7252BA4FC60E2B1BA76F1D1388
SHA-256:	B67F0BB152FA2CCFFDFC328DD24DEE8861266B8F34D22737C72771BB650D2FD5
SHA-512:	F9164386B5DCF4550E4DB7237452C7A1D19D6C1FEE4A36CD01C019247558A390D05E7D75D03F25F89A0CCC33F2DF4EF04ABF42C79C0315C215DEEF9C70262C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .t>.>.0/....."#.D.b.3.k.A.A..Eo.....rq.....].>....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):	5.544776823427742
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuV5tqcWT/MktrA9/jcyxMtv9Ej:mJYOFLvEWdGQRQOdQP5tAD6g1
MD5:	042C6F95B2A2622E9561DF44ED0624A3
SHA1:	0583CB86CA151259095005CF146BD2D04694E3B9
SHA-256:	3CF8BEAD336F056FEAC87C1CD0DCAE215E75D1C0CC5502DD987483EFDEB2E4F7
SHA-512:	83DBCFA25C7177E501ECD7B195CEBFCE4923D1F190FF1F9DCEF97D1B0AC2B7C0057B0986BB7627B0219169DF3AD4944103D9A30FE87A709FF4C388CD26E5962
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..u.>.0/....."#.D..=3.k.A.A..Eo.....$.....c..y/L....|y.n..C/l.....X7-ne.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.511803164225429
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVZXK//XAMktjNlVQMWqg4nRb7om5m1:mOYOFLvECMLZXLtREuR/41
MD5:	5D8AE3A433BDE7C96AA7E8D970325AD9
SHA1:	7D571A327FCB3D63177D9F03F4B1D5A307B38D1A
SHA-256:	AA89F710C56ACC31FB693E5A59EDA4B5FAED57A9508BDFC7D75FF025D80F2128
SHA-512:	8F3EE6A02A73D1D6C1BC1D41568F3A452CE0D137FD69CA24C3BCAC0521BD444D76872E4ECA6950F3B030F5778F382F1F1645B70829C60907C982F9D05D5C366
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .u.>.0/....."#.DA..2.k.A.A..Eo.....(.....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):	5.581207121576264
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu4nKjt7UGm0bbsIDMGH41:XfRMqKjuVKsIZ
MD5:	E1DCFFDA0DCE3D9231CC2642A80E1D6F
SHA1:	B2A14BEA2DE9235DA9FAB70A9489FB6E8F511857
SHA-256:	6C3F0FF66905C964E165EDB6B1EC34E9CC6973D148868299FA3C28ADB105FA2A
SHA-512:	24BDB654253B18387D765E1816F718CF6796C76D1DF8539FE1DDD3F522973B07689EBEE8968A03B39B97E195F8FBF0992F1E953EE27B6E8536A805A715E56845
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js ...i=.0/....."#.D4Js-.k.A.A..Eo.....;.....`.....^....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):	5.46702048787942
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuMYOqjtAHby0zBUKSAA1:pRnjqj0b
MD5:	DB8F594B78A3F2BF31DCB5BC023FD243
SHA1:	542A04834D0A8CE326E71B3C388AABC741C88298
SHA-256:	BC7F222C37C9CED8501FC027050F2C91256C003DABF449E68F6D3E543E3A56F1
SHA-512:	D7FEC33A4A75AE705069A7E6C8752302D173A9478CD4C6064CD8AE5F73F839F267DA8072725404425BE1ACA5903CD21CC41EAF156934C3E117A2A52B28D1046
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .D..>.0/....."#.Dnj>3.k.A.A..Eo.....y.....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):	5.475923891156674
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvsa/+Mkt9Md1dn76KohyP5m1:md4HXXYOFLvEjMSWFvsxtujUdyP41
MD5:	A16BDAC8F238B629EB72DD7C40595F7F
SHA1:	60B2E9BFF07028308472A02D7E6833B41D65289A
SHA-256:	2FC6F6AF27902240098E9ABA988188A7945BF56F042005B4E953D6D2DEDC52CA
SHA-512:	2DA8CAE907C21B6589C115AF8E58C92692CBAB6CDB4B3C84A31CADF58510DAFB17E60A87BDF8E086AEBC0B6BBB50DA627AB797A331292A6BF81299E89C622 FBD
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .E.>.0/....."#.DX..2.k.A.A..Eo.....6.....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):	5.535265557326223
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLhIV+tFG/Mkt39zUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLhlG9tN4PqVyM+VY1
MD5:	8DE727FB2F0307D2928E920926252531
SHA1:	2FBDC3DEF13C1E9DD095381138543C5A4D6AC3F3
SHA-256:	D36ED88208595255D18CC50FABAF11942667161B89E10B897F41184AF8EC12CE
SHA-512:	F3190FFBF9A217529DA06CDD730748B9B8EAE8144B7F41B600082B4ED2BDEFE6833580139E76444575BA62361353C57C8E75B2909FEF4285275FF3B9236CF00A
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .QV.>.0/....."#.DT..3.k.A.A..Eo.....\c.....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):	5.57543987464677
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFly6iStWtwSeKaT9pr1:URVFAFjVFAFL4twSeKaTL
MD5:	F7DC0683D7CC2FC4AF1F1EBE5AB0AFE6
SHA1:	B34F8C273012EFC7E9B753DD7A9628372B59663A
SHA-256:	865883754F170EEE6C0AB1B0FD0BA18F4665E39652E6C5865FE79816AA21275C
SHA-512:	29798C6FC49981D769DEE7A41644BD14115D87CA2F1EAD09D6F3B3AB56FF91A5178295ECE880F2BCED87A3D3D045BF056A60D92CE319F3C63A81160E527DE5 E
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 .c..>.0/....."#.D&.@3.k.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:	dropped
Size (bytes):	210
Entropy (8bit):	5.503010784869182
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQ3K9KStZyyt5GFCaa+41:NRMHdQKX7Jt5Gda+
MD5:	4713CD09CA7F32B2C113A73FFF822744
SHA1:	F2462EC4C181424D7E1062570DEF6B0536E23874
SHA-256:	1F1D85AE72D72F8EBA971217A10AD8D434D3EB9A4FAC257370D087DA27CC9AED
SHA-512:	1DC41548A535883A18FC4541B64DC19682C45057F3C9BEC81E3EFB6816735EEB79AFD90F9121CB633F78E1608AFD010D1FEEDA8E15FF9F652291BA4F4C3AB9AC
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .Q.j=.0/....."#.DN.t-.k.A.A..Eo.....E.....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):	5.527902363277839
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvnt+tlYmk/Mkt7yrpYFm1:ms2VYOFLvEWdvBIEGdeXuNtxmQt+11
MD5:	9483676F78C69D07C54047629A9E86E9
SHA1:	45FF6767FDF14826439CF429E60ABFE08CF8B02A
SHA-256:	97DEEA6C3CDA97BA9B400868A18A53D4F0EC3CD618AC4551D9E038AC12C085E2
SHA-512:	35015D74A8029E6579B6067BC1559AB24E45EE70F459B1D4EA042E7726C0295A05EB2C9E7A8A1876A1F1D224464225B51020648ED42AFD3852D4DA60A48278B5
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ....>.0/....."#.D..=3.k.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):	5.608257266217741
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQrG49tKdxm7OhKlvA1:RbR16N49UxmJ
MD5:	8D430543936D2EE647981D91F37EA024
SHA1:	6C00774132406FD04B2C644C18C8C345373B7846
SHA-256:	3C853B20A50013B77839B0DF0AC41D115A56386B1A6EBA3D6E198FC8FC50841D
SHA-512:	7E1E830D4A9E8997289B96837841134C2326DB0AD40A16CE7C918B99735C6E48873424131BCDCA034621F2BD51F8E9CD3DAA46EC3C109D6397946D724C9781A
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .k-.>.0/....."#.D.#.3.k.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):	5.587571038471125
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuLGibft1QtddFt1:B2geRHRQ21bfj
MD5:	28E4F9F05F6CA9803F98A3E4E98735E0
SHA1:	07AC46242D6C50028D311C9650057B03504765D9
SHA-256:	5AD8C31B55B133FD265390F602097C2A5F84E201FB47226255880D413C7F485F
SHA-512:	D6538C1FA22CDDAB323E5FE4FDD6C5CF82A8E04F4803558FC8611A49728E8377796CA9D003C203CADF7922F0334838BAF9ADA97E13D110EE7F8615E5D24B745
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ....>.0/....."#.De.=3.k.A.A..Eo.....@..{o]...9o|..qY....T....{..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.5845416621235415
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVn8TG/Mkt0sl/uEnNWQ1SUm1:mzyEYOFLvEWdrIOQo9t0sl/uEt1S/1
MD5:	B300BDD6F0E7423960EBE38C34A68998
SHA1:	C75AC1C4F828B7D79482199BF98F4ED99C618BC2
SHA-256:	70DDB26CF0C9234D5942C9EF4C4F95F4B5BC712BDC2A099B605B162D203EF167
SHA-512:	778ADFDE7020B5C784F873F2CEC47BAE89590A8675368235DB4D4DB5C949486F71E513DC22B70E1672C28F83307E090C3F174DC19FB992CDB42144CEA8875C4
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .H..>.0/....."#.D#..3.k.A.A..Eo.....s.....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):	5.508563917498022
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuq05td9l/olwrqwK+41:wRhMzH/oqGwK+
MD5:	AFDAC319626A75297446AAF72517D958
SHA1:	29B533C581DE483DD294CBB85B21E1F3BE906958
SHA-256:	2A2F8529E6DC8BB6CB4374EEDE8EF9BBF1594BD89742912DC648F89D058DDF03
SHA-512:	F17C9067B5272EBD853227E90939731CD15637705B142579425F15EE50A835B333F834B1B58EFD08241BC020A5DFF928D8811F8ED017A72C5B504A6AC64B3A58
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .-,.>.0/....."#.D...3.k.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):	5.580175528755398
Encrypted:	false
SSDEEP:	3:m+l26Xa8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKH/KPWFv+qq2SqMktErX8AL2U:mYXYOFLvEWdrROk/RJbuAf2NtRfO441
MD5:	E0A416C0932CFA9E62F223EB627AB783
SHA1:	7B16DD71DE3E983DD3A53ADCB65846BF808A32E5
SHA-256:	A3FC5F8E38C0B19A5E4F8ACC49497D51C2CA1BE99FD6024ACB0D0849502C84A8
SHA-512:	471983EDA9B573838DDA5592C8AA9CCDBA55D951D3E1839E8E706247007D4DB479BEF5D71B4FCCCB6AAEE1734FF96B4622EB3913D27B7BEF4B9E5A3E9E90F 2A
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...>.0/....."#.D...3.k.A.A..Eo.....\.....~..rw.+[....!.) ?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.531525922522983
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVd+tKWT/Mkt1HzoIN1OFPL4m1:mmDEYOFLvEWXIRWT9t5zV1QPLr1
MD5:	0F5D21BA167549C5D9680851B68AC3BB
SHA1:	BA82E59298E35B40A145F2DA9FD4F094914D2231
SHA-256:	F0B659BDABEFFE45B7F04F45E9AFD5BBF03E2B1E53E09BC0619BA0292F3DD5F1
SHA-512:	9AAA533700835FCA0CA7B5699015F759AFD4FE58E876A8654AB769C990F0C073BEA17BBBF853B02CC8B932D82D543B24D7AC377DEA281199FFDC4166A016EB3 B
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..T.>.0/....."#.Dt..3.k.A.A..Eo.....Z.....~]...%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):	5.584009079562968
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvzt5g//e4Mktzl9t/m8D6EsEJeUm1:m52YOFLvEWdMAuLYrtzntuEvsEJ41
MD5:	7B7D41CD9542ED280F0C61D7EE1C38FE
SHA1:	A61E9874129A11028DAFF8D51746BAD04CBCBE51
SHA-256:	884E721DA48A913C0427EBF3C0522E2D76A48F11986E168D7A2EE923CA5CDD4A
SHA-512:	86E6ADFD254CCFEF5CF5D26097C53DCC1799C0084C09FF96F5A927E1EE360F3B8F65D4C746F1F29737E1C2419B38D1A3E29FD89C6519EB6B8D651025B5BD75
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..,.>.0/....."#.D.B;3.k.A.A..Eo.....nb.....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):	5.555427057338893
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFv7Ull/OSG/MktF/OFoDb7Tg:mYilPYOFLvEWd8CAdAualYBtF/4ong1
MD5:	18104583136E708E62BC7A909FC379C3
SHA1:	FC222C1F8A6838BBE9861E66B2F7F2D513170EAB
SHA-256:	86B192C9FD61B53096CA58D9409047E5829C03AC3F8A99C44F4E0183E4A71DEA
SHA-512:	AD7C34F5DF5BF15E5058E120FEB4F22550B425226381BFBED82DBC16A3B013E7B9BFF15FF7B318EC95149D0BD275DB1B02BE45B375DC714906FDDEC66F3B31A
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .x..>.0/....."#.D.;3.k.A.A..Eo.....B3i.....c}.H7M=M..-.....Ix..R.I...}RI.$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):	5.5822371815214975
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/Iuu29fStkVN16wG1:F8hRrROk/E29fSK
MD5:	7AE32FC1290DB08160CD649E77B3282C
SHA1:	3B139E83BDBD559D4C506821B065D166C41B1870
SHA-256:	FFF3898541931DA207C66D0210476A7E90EE9A55DE079D97BF21A84E57C61EC5
SHA-512:	5E165680F675277BDC4F41A5F3903B16E16500789FFFD390C967B23369572773BE58C791D11A5ABC26B2472ADE6A96FD532CD722253050FBED3147793E351B71
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..;.>.0/....."#.D...3.k.A.A..Eo.....a.[.....%.k.SZ..~W.....:)'B..ad.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.631314896230787
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQM/40V0jtItoeJIi1:ehRcR4uQ9eJI
MD5:	0093A34DA8CD4A1B40B56C98E8BCFFAF
SHA1:	713CA1A5EB2D6D042E2878729AA217FC441C9713
SHA-256:	BEEBA705E22A18C6546EC5233CEE3F992E53BF5C2D51A79ABDD744AE61DCBBA1
SHA-512:	25C2CA29F492E751BF3E8CBCF2B0D458D2B5755BC58075B4036FFB2E7E2BBE7B2AE144F2FABE1D165319BDA9A05C56F2671DC283155EC0A010C575A3F303B8E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....>.0/....."#.D...3.k.A.A..Eo.....;"./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):	5.5479921622124255
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvRlbdgY1O/Mkt2j//lP6mgmOZLP:mOEYOFLvEWdrIhu5Q9t2lzgm2d/1
MD5:	A4ACD4F9F1FF3C63FE0B2219CE83582B
SHA1:	DC0D07386F597058FF968F4E4D5102FB74D32AEC
SHA-256:	636216360CAD4E5F6E9B7F25663FD62498B99055037029607308B49F2013C233
SHA-512:	486A25C2936EC30A18A54774B2AAE190CDA8E9C49D496FC54E8AC4F097E3027E274B23AFBDC16E17FF1ADE59B68F04C18BDC2541A1A3EA6A08F2E4E0147155C
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..&.>.0/....."#.D...3.k.A.A..Eo.....Q.....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):	5.591666735979466
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvT6YxrMktT//lGBiaQ562HvpMm1:mAElVYOFLvEW1KA9ztT/px56uvp1
MD5:	ED0B32F1E0D69FDA05DADCBDCD1B3B7E
SHA1:	FFF3E44708198BC78C6FDA2034CD6AB98BEA7F1C
SHA-256:	E266C586F4AEB78AEFD521C066A47F0884BEE7590432576302E7E4A368395D1C
SHA-512:	6967FC8EC69140BA6CE89B1A98B27CA60EF076BD21D63680F4A52D67CF8CDD0D1F60C76E672BBF59C5D8D533C1B2756ABC3AEF119711173EA2A8F873D0376EA
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....>.0/....."#.D...2.k.A.A..Eo.....Y.....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):	5.6572895384755695
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuBnXLKtZUUDLYtmOZn1:xRBJXvNDcFZ
MD5:	25F76B6040807109B779674BB47E9D60
SHA1:	97F5EB316C1D844B7561708ED9D2B58D90A2AD18
SHA-256:	123DF10A09D97B3F994BC07046B8CB459DBB1E906A652B34E7EB191B32A78830
SHA-512:	1973D9AA621F7CA2DA3FC62E259CF356B5858BC4E47E52472792B168F1645E74EFF5A5403292E604A7A02332F56C038359C523D40CEE8C997E3D1A01B35B0ACF
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ....>.0/....."#.D..=3.k.A.A..Eo.....w.....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):	5.535909436639206
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvu//vP9k/Mktt9pSKGoSSlf:msRPYOFLvEWIa7zp7v29tH8VPu1
MD5:	BBF344DFFED62697F3F1BAA94DB8E840
SHA1:	2062C2CAEE73F973EF62F1E4380E727A2D5B53BE
SHA-256:	03C2C3E621F00DE71262602EBA394AFEE3BA2A09C0F2289787243094FB273359

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
SHA-512:	0C4F531F7A63282807E1FEDD9E703C2FECEDA52C1FBBF0D5EBEC0F04CC3AA2730C722DD02E8704F89BC541033F8324B5590FCD3780BCCF31F8D38EBF3785E5C6
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .R.>.0/....."#.D.I.2.k.A.A..Eo.....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):	5.583503792077253
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVPdg//BlI0hMktj9lll96F4XVAn:mKPYOFLvEWdENU9QgdODjtjH0wiM3Y1
MD5:	C5E1928A16A6314F2BF960435C8E40DE
SHA1:	2CA3B5C1580AA0791DB2A03B5EF63396EB55297D
SHA-256:	F51A4E4376141B43F1861719974E1BCBE11C469F935830252124DC36EDF4DB00
SHA-512:	27253CD102C746A673CF41E853FA05E6D6A65B55B545070EDF70F9404D41BAA1C83BA8DC12435AC0ABB3E7A9C2D40D0B57EC912FA638F5033332E0C42A1C805
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ../.>.0/....."#.D..3.k.A.A..Eo.....?Z.....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):	5.600545661828052
Encrypted:	false
SSDEEP:	3:m+lQWt6v8RzYOCGLvHkWBGKuKjXKjcAW6KLuVvt+//chMktYu///4MY3jBMQ7GRE:mQt6EYOFLvEWdccAHQqjtTmjBRCh/41
MD5:	3A737E340C098738BC676662C0C901FA
SHA1:	C434DB52A02F8FE5D08DB905E5A652B6716BAC10
SHA-256:	6D4C78C0DFE47320C330F6C612F4CDA0825F95EAE914037DEEA9A248797A3FFD
SHA-512:	58DED436804ACADFA5EC4F3C5F5624159A62E50E4D8F63D9186603A80C4F4E369AC2623DD5ED846BBF622653CA92B8343F0CCC19402AE74CD1E8070CA311CFE
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .!..>.0/....."#.D..C3.k.A.A..Eo.....PJm...0x.x..RD...BB!@5..<..] ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.594119604100184
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuoktA3kULlF4r1:bs6xRki6k27LlF4
MD5:	A7A13CB4FA42DD8F74BAD789AAB3D335
SHA1:	A46D0FEB6AA8A978671FFDB953672FD309469522
SHA-256:	87869FDA6259F77F3084061C328EC4A368073F105F4332517F4A377ABCCD9031
SHA-512:	46B837115EB248CB3683BE4E210DE6AD2270D7C622FC1B280DD1F3B024695DD035C35B1E90A187D7800113CC940521A49FC6FD208BAC47CBF415DE3C251724E
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...>.0/....."#.D..$2.k.A.A..Eo.....B.....P...#4..l....5. ..5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.485677074942846
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvACl/GsOqhMktzllPECcu1isLK5y:mhYOFLvEWd/aFuiCQsOqjt7EN941

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
MD5:	FAB0F6D7A5ED5D7CCC5288C5576675E5
SHA1:	C98021901D3C0613D9EC5B26CD4A6CE78FD8CF2F
SHA-256:	280CFAE115809A183AEB0263F952BE998CAF7455A9894EF87C5977C4E44590A1
SHA-512:	4719774150C630E15A77D1EF1B0BFA87957F07FD99FF42442BBEEA60BCD6F27A68124D80340AF14C846A339CF1A67793D53D491B55242F44B791476ADED60F7E
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .Z-.>.0/....."#.D.v>3.k.A.A..Eo.....l.....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):	5.532904003791274
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQPjtPBMqVd3G4K41:2DRuRKjRB9Vd2
MD5:	C09AF002BF2AA2BA3311E6017BCF95DA
SHA1:	236F0E85DF26A66A7F67F7C87B114D7E46B0384C
SHA-256:	A787EB776CA0504BBA2621247F95FF0291E7706B199B5073131C095BE553DD39
SHA-512:	48A2F5058DCE471108AF046607BC220B120354105FBB859EF3E01D9DE5B4EDFDB9BE485A40ABE8B77569E1C447685BFADCED9094530BB7C14A50D0FE0D7CB2 C1
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....>.0/....."#.D~R>3.k.A.A..Eo.....G.....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):	5.610036856304193
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QuklxjtrGuA424r1:+RQ/kwjbr
MD5:	7DF2BC99079044DFBDBC85F89F8A7A50
SHA1:	43FB440CCFA84A7523E1FCA981892D4E1D7BAEBA
SHA-256:	E4B6AF4627CBECA8E3A24E40967A0721955B800B857B7B5F8043D0365E42819E
SHA-512:	B0E14558EC210B95B4AE80ACC6491A4192F01BF62D2AA98D68829637026062364A55D4868D70CE6D584DF5FBFA24958F644C12642DF1836E8075061194BE509A
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .<..>.0/....."#.D..H3.k.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):	5.515326963318564
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvl5V+l/z6KAMkt9aLFlTAg2iV:moXXYOFLvEWdENUAuNKSt9Yl8yC8n1
MD5:	08455AA0404A59A44AB9B137BA78B75E
SHA1:	3F9AEB7F526092A8EECE9DF70BD06EDE73872EF2
SHA-256:	5A2425C5812059EE2EB5D969C92D58385453F881CB76FBE10AA874DD771DE7ED
SHA-512:	721BC4CC0AD58A2EDF2381A6F53E122325ED156523BAB8556BEB909BE38E86349F7A8561B2E9BAAA4C9AF570D5DF11DCF3BFB123D0447996E38E2ED8EF06EA 69
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..*.>.0/....."#.D...3.k.A.A..Eo.....e..n.....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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Entropy (8bit):	5.591740221523928
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQpiqjtk/l/sLmB41:nRrROk/VWqtN
MD5:	ED8A76440188D20FC6063329C24965B0
SHA1:	4CD89144ACA02B30641566B8E036BEAE09BAFF11
SHA-256:	7E96A3A90A731A7306EB91A6DFECAF9AF7168D0991CDBFF0D0E2C006DE765FD7
SHA-512:	5CC0836367E40AD5872C0090FCF2D1E96442450A6D6D90EDD06730463469894960 63CBC882B72DCB269FB0C4B839F18EB8085BC264AD528FAD19BD02134E35D
Malicious:	false
Preview:	0\r..m.....]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....>.0/....."#.Dg,.3.k.A.A..Eo.....Q..... ./.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):	5.570969290155554
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuBWBlWKqjtirdm9741:qxRcWlfqjIdu7
MD5:	11D88A1A3E9470684DEDB8E6376189A5
SHA1:	33A7412399DB5C81550BEC074B851C66A1C99849
SHA-256:	B5DF656943F14AB1DD2FD380DF62326C589AEE1CB8EDC42EECF5FFB9ADE822F8
SHA-512:	11BB9B8B5EB662D59743099C0BFD726E8C3F9A96E979CE8D56208FF7DC649C581F6697A045E7DC98E0A48E91C12D8609190FC81753E7856C0FEC7BB8C0632E5
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....>.0/....."#.D.F<3.k.A.A..Eo.....Q{$).....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):	5.538915544091086
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvhgtmkpLMktB/OB6shoq+Nem1:mMOYOFLvEWdwAPVukwkLtB/OB6Jn1
MD5:	F1167195846582B5C9A6253BF5C7BB59
SHA1:	549B11FF1264E755EBFC961226DB736FB4FCDD8D
SHA-256:	58A4AFA4AEF8F4C036CFDF508E6101C4CFF5FD55E45558F60C63394A924D9E06
SHA-512:	1A8C1BC13E97A0660F88E14079260C98674F43E94111DFC82E837C739693048203C6CEEAEB6EDC55E39EF9F17D12E92406EC0DCF3BEFA9D0DAEFDAA37956D4 6
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .F..>.0/....."#.D...3.k.A.A..Eo.....\.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	212
Entropy (8bit):	5.600623197328436
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQfT9jtElAhcsBXIh1:mxRBJQ8T9jSSB
MD5:	4CFBF2A8FA9212DC3EA522BF6BA628DB
SHA1:	B550122E573DA6C8CFC689D3C3E964B5166AC59E
SHA-256:	579AE38FE0F0B5CC29A626E4E3B59E53A37236E7D636D333EA9D95065B11E86B
SHA-512:	75B1923C461A751D6BDBCF012678B4F80B143A1842161C0535DFD1741D99C3ED4C5B065CC2E0B99B2AD7FFCEF20D4F2C30A06F8A1A9C321FF7DB923536E9E4 2
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..z.>.0/....."#.Dh.>3.k.A.A..Eo.....N/.....k..`..N3.... ..d..$[.....{.A..E o.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.577318976603521
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQkg9jtcc3Me/1:3RrROk/s3yK
MD5:	748B268FA219D127CB23DCF56D31AFB9
SHA1:	ED897357B29FC2D1EFA2D06C61FA961C843C1989
SHA-256:	05DA71664947C64FF901059F210091FCB0A5E461E3DB80DC1A8812BD36C4A33E
SHA-512:	2D5DB112B5BB0519AD1024A25A24CB377311A48DACAAE659DFE4481D50E559C1F4E4F326ACBCE270A4A5C28A29AEC6A48B8F1933FFF1852D2C4C2CFAA3131 91
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....>.0/....."#.D...3.k.A.A..Eo.....'.....9Q].8O.z....= ..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.126171681913686
Encrypted:	false
SSDEEP:	12:HX6dlra+/l/CC5tALImjYDTtYh2Mzl3RMjUnhfi+/l/FLGNb3YIYmabzLPAgWd3V:qWAvmjYDZ9MXpXKbLIkx3V
MD5:	83885128F010B8581A8B150101FE486F
SHA1:	57BA809A5548CDCF17E60B1C8D8D3A29168FA57C
SHA-256:	F36781EE22ABA254A2A77E7E2334DCA6CBE71AF07C82CCF6CAE4E01CF204E7FF
SHA-512:	22FCFB58FC138B9CE4C6C53FEB46FA5D9B99B5E92B9640C0E65798812591F1945FF678EAC1A4F6BF546F11903F704EF58497C2CBB80E0AD56DF20660792D527
Malicious:	false
Preview:	0...@<H.oy retne....+.....V.....*.....>.0/.....;.y~A....>.0/.....oB*..>.0/.....#...(...A_./.....D.4.@M.>.0/.....[.i..%.@M.>.0/.....k7A....>.0/.....]...I ....>.0/.....,+...._.#...>.0/.....<...W..J..>.0/.....J..j.....>.0/.....6<|.....>.0/.....2q.....>.0/.....P....V...>.0/.....!...0.o@M.>.0/.....P[. q...>.0/.....3.....>.0/. .....v...q....>.0/.....a.....>.0/.....C..M.....A_./.....qi.K.L.9@.^=.0/.....K..JM.gb@.^=.0/.....>.0/.....F..=z;....>.0/.....o....>.0/.....Gy.'.h....>.0/.....:..N. A.....>.0/.....;/.....>.0/.....>.0/.....*....@M.>.0/.....o..k..@M.>.0/.....^.~..z.@M.>.0/.....q.@M.>.0/.....A?.2:..@M.>.0/.....u\]..q@M.>.0/.....+. {..'@M.>.0/.....MV3..@M.>.0/.....@..x.@M.>.0/.....*)....J:@M.>.0/.....&.S....@M.>.0/.....

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):	1080
Entropy (8bit):	5.126171681913686
Encrypted:	false
SSDEEP:	12:HX6dlra+/l/CC5tALImjYDTtYh2Mzl3RMjUnhfi+/l/FLGNb3YIYmabzLPAgWd3V:qWAvmjYDZ9MXpXKbLIkx3V
MD5:	83885128F010B8581A8B150101FE486F
SHA1:	57BA809A5548CDCF17E60B1C8D8D3A29168FA57C
SHA-256:	F36781EE22ABA254A2A77E7E2334DCA6CBE71AF07C82CCF6CAE4E01CF204E7FF
SHA-512:	22FCFB58FC138B9CE4C6C53FEB46FA5D9B99B5E92B9640C0E65798812591F1945FF678EAC1A4F6BF546F11903F704EF58497C2CBB80E0AD56DF20660792D527
Malicious:	false
Preview:	0...@<H.oy retne....+.....V.....*.....>.0/.....;.y~A....>.0/.....oB*..>.0/.....#...(...A_./.....D.4.@M.>.0/.....[.i..%.@M.>.0/.....k7A....>.0/.....]...I ....>.0/.....,+...._.#...>.0/.....<...W..J..>.0/.....J..j.....>.0/.....6<|.....>.0/.....2q.....>.0/.....P....V...>.0/.....!...0.o@M.>.0/.....P[. q...>.0/.....3.....>.0/. .....v...q....>.0/.....a.....>.0/.....C..M.....A_./.....qi.K.L.9@.^=.0/.....K..JM.gb@.^=.0/.....>.0/.....F..=z;....>.0/.....o....>.0/.....Gy.'.h....>.0/.....:..N. A.....>.0/.....;/.....>.0/.....>.0/.....*....@M.>.0/.....o..k..@M.>.0/.....^.~..z.@M.>.0/.....q.@M.>.0/.....A?.2:..@M.>.0/.....u\]..q@M.>.0/.....+. {..'@M.>.0/.....MV3..@M.>.0/.....@..x.@M.>.0/.....*)....J:@M.>.0/.....&.S....@M.>.0/.....

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):	5.16626899413451
Encrypted:	false
SSDEEP:	6:mzjWM+q2PWXp+N2nKuAl9OmbnIFUtlb1ZmwTNWMVkwOWXp+N2nKuAl9OmbjLJ:WjL+vaHAahFUtlR/TNLV5fHAaSJ
MD5:	CD26F3152D31B2B9B5F9FD272F8BC913
SHA1:	5422E1641A468C59E118698E17A75A1A7A6A3581
SHA-256:	47F8CCE93ACB02EF6ED8464F14B09BCBE16DF5997485059AC109DB46245EF2E7
SHA-512:	1FF9DF7594C13BF3C299B265111FCA5718EC4F7BCD08A37E741594CFDF77A89CFA3408DF14A8B3A49CB582F5DF71C85312F5A738938FCC4651E7F94866DB287

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Malicious:	false
Preview:	2021/12/05-00:30:39.180 14ac Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/12/05-00:30:39.181 14ac Recovering log #3.2021/12/05-00:30:39.181 14ac 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):	5.16626899413451
Encrypted:	false
SSDEEP:	6:mzjWM+q2PWXp+N2nKuAl9OmbnIFUtlb1ZmwTNWMVkwOWXp+N2nKuAl9OmbjLJ:WjL+vaHAahFUtlR/TNLV5fHAaSJ
MD5:	CD26F3152D31B2B9B5F9FD272F8BC913
SHA1:	5422E1641A468C59E118698E17A75A1A7A6A3581
SHA-256:	47F8CCE93ACB02EF6ED8464F14B09BCBE16DF5997485059AC109DB46245EF2E7
SHA-512:	1FF9DF7594C13BF3C299B265111FCA5718EC4F7BCD08A37E741594CFDF77A89CFA3408DF14A8B3A49CB582F5DF71C85312F5A738938FCC4651E7F94866DB287
Malicious:	false
Preview:	2021/12/05-00:30:39.180 14ac Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/12/05-00:30:39.181 14ac Recovering log #3.2021/12/05-00:30:39.181 14ac 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):	0.010978819626460943
Encrypted:	false
SSDEEP:	3:ImtVdXb+j4x9pPlXlpyPll//zVrzlltD0lGQZ7XEZhGIelHdP4/X:IiVtg4x9pdM//hFwl570ZhdelG/
MD5:	E36F8F81D3C03F6AAF7D768706B7673F
SHA1:	EECE93F9E417717892E50F6A159516DD76C255B0
SHA-256:	C6E687FF9677244574F37AD2877726DF64E5BAADDA2ABE8C4759BDE8344E44F2
SHA-512:	0582ADCFA1A09095D4482C9A61475C8B77FF444BF2655DE4F6583BBB2699A054BBB2292DE2741FEEB27AFE0835B0B48F476418EE1A666DE20CA146D1EB4390A4
Malicious:	false
Preview:	VLnk.....?.......Tq.>..j...

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-211205100402Z-190.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):	0.5870422524031753
Encrypted:	false
SSDEEP:	48:8cScSEriqJVSwEHxvXySJTQKhLYpSSaFucoyBnUFSREHy9l843hvCqFq:FTLXEXbh8ESaFJUak5
MD5:	C76EFEB122456696DEA738A2FCB8D91C
SHA1:	EDF5FE85CF54AE7070E7A2F437E36F3AA3BD441D
SHA-256:	6C8CF31E089BBA8B99D94143B3552E6CCC3E0D34542DD38A91015859A77D83AA
SHA-512:	439C62273B77CFEEA8FDE3BB5444BC83FE2B89FBEF0141E755B535555D7CE0FACF098E158ED7CABA564A3A516509156CF7650EB1CE3BFB22A0A3BC14DCA763A4
Malicious:	false
Preview:	BM........6...(...u...h..... ....5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5....k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k./.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../...P....b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5...5....k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k..k./.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../...P....b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-..b-.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.../.5...5...5.

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:	dropped
Size (bytes):	61440
Entropy (8bit):	3.564628524252542

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Encrypted:	false
SSDEEP:	384:3eI9dTh2tELJ8fwRRwZsLRGlKhsvXh+vSc:ekYZsLQhUSc
MD5:	52D0C9862F6046F2D3F67D6C7AF36CDE
SHA1:	0F23BE8A35D5B216A8D853FC3172C1E3C4ED2E51
SHA-256:	6CDCBAF96DD484A8E8A22817EC7DF0EA39EC266227080C8833E2E07ECD2FD6AB
SHA-512:	9DA4034E3DA231D856AB2139B30C76B59D82A226888CFA1C43AF72A7BF0DDBDEDC671C992780974673603B2C4F6C3DA7EB7CE4B06778F720E7E6893278FE8C E
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):	3.285995596096166
Encrypted:	false
SSDEEP:	48:7Msom1C5iom+iom2om1Nom1Aiom1RROiom1oom1pom1FZiomVsiomgzqQlmFTIFb:7U5NOh1CszN49IVXEBodRBk8
MD5:	255610EE3E6065529910EBD141F0C093
SHA1:	884F4E9514F1593DDD07705F1BEEDC6BC047A865
SHA-256:	1A51554DB44C27B83A97368EA863BA18E29B33A51FEC89418E59D95417E45478
SHA-512:	BB9CE1BCC1860A1674469D856783A956744E6EFB0EEBD3682890E7F1EA8B3E9B9C6495D46A1CFEB5C6BDE655BC648576E4FC0E7BA296562124EACC80B1933F 0A
Malicious:	false
Preview:	.... .c.....wy|..... .....s..... .L.s.y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5076	
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.Na meArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleN ame:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.N ameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-Bold MT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)	
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	0.6750050738677021
Encrypted:	false
SSDEEP:	12:BZ2vX7vz+YXnTlHLjJ9wkI4c6/oCyitQBOIP0xg5/fLM:BZeXTz++IvJ9wkI4c6QbiuBOI2gxLM
MD5:	C38DB0F968872CB3B1FBF6AE9A0EF9DC
SHA1:	F33A6E1368267704758D324C3170FFEC35A64886
SHA-256:	6B804B2E7E3F3F270A809298758697B12697A26846FF9D20E0FBFDC9F64EED8A
SHA-512:	55BC7AE2ABAF607B7B4F6804390ED8FC796EDC0D778728DDF84E62B97BE74C1BD9547CA1EEAF3646BADD30C8AB1A7E20D534249DD976E07BA83B718DF6A39AD8
Malicious:	false
Preview:	...Q.....{W.C..$;..U....b.T}..k..... .....g$#..q.....i>....[}l.... .....M^.....A.....W >.D...{.... .d...h.g.U7.Z..!.....j.&...Q,9.....M4..mN.1...CB&....$.....,1!.f_?.1..&.....a....t. ...]U.hQ.?.*#1....r|..0c...=.....]..J.....LfhI.<.....].5...P.5.9..{`b.GB.....$.....r.&"8..2..x5.n.j.{.S}..l..[..4..K._.*....Q..A..L..YY..vg..M...x..d|0...k..I..~...-Cih.KW...._".i._.!..X.r..... .&.Q`....90....L... .bz.s-Z.}..;v..>...%.|.^.....}.qm..:.....Pf....`.&.L.....ny.....)I.M..Q..xZ...$.I.....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	24152
Entropy (8bit):	0.7519410049126055
Encrypted:	false
SSDEEP:	24:DM9iGGEWwXc9BeayznQAY3vFVV5jDBJej5JVzesSSUeolpgdXcdSqx2DX95:oVXG9BCWZ857zctlawz
MD5:	48B99ACAEC7BCFBDB7F0B4B96B2453B1
SHA1:	BE8AF0C8AF83D943747928B45EBBF44ACDCB374F
SHA-256:	D92FEC879C4EAF4D3B887C7FDD0FC602F9C97C0BBA66024E4F280C27DDDFD0A9
SHA-512:	429D4DB90913FA07F2402BBF3802A4DF6DFCB1E367E4B41D8629B85F463FAAF38F5A6EC51D0551C4CA845FDE856C2203875DB5F87DBA6388B0A4A648363DF32E
Malicious:	false
Preview:	...s..K.....j+...%...X...Ba.....zzd~.....#B..0_...\..=.u.!!..+@.f...Y.)mg..;...Ab.....a3..k.....MU.Jq.$*.jnG..*.WY..W.~...:.D.M....n.L.....d..''b..]n.....bj....p...d..cN.s..+P8. {z:x.P$:..n.L.X.....co[v"Y....^...59.32.tn/Ce0.*\..i.N.N.}A\.e.U..7$zf_x..j*.buOq.N...P=0'.....e..#.....I..;Aq...\|.el.78..g.#.....k...#2>.....G....% ..K..=W.!..@..[..7_>PI..(.$. .%..`'.kglw.....UC.4.....^.M...!....4y..O..~.|...vpY.8\H..z..Kb..j.....7G]D.9$.7.rRu..,t!^..0.e...\|.X.]..k.KVnb.B;.n..P.....q....P.....:mg.jH..R..3m..x.$...zR.b$..QR.M...`.....U{....(.a ..Z..EZ.6+.BM.Fq....Wgn...=..k\|.. ..>....q...T?6zSB.....1..6.....s...l^k.Lt..f..c`..V.qz@.+..e$.....

Static File Info

General

File type:	PDF document, version 1.6
Entropy (8bit):	7.981995550292027
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	404.pdf
File size:	1650766
MD5:	d838d040fd7877c106b9800d3df0c3a6
SHA1:	6f520b71773361a887a3cdbe3f8745d1ed3a57be
SHA256:	21979c27f520821587157e7dd3af9af3872998d527834f141cd7dc0535aab5b5
SHA512:	fbd65fb3365706b84528d240e3a27443ba725545408f499f72a648ac48cd4349982d44767f147518204cd6bedf47fd40fcb6d8d1c4f2ff2c506a2b122dc49408

General

SSDEEP:	49152:tBDAZhJMZdjaGb92cUW0BgEaO5fBOBE4VL:tBEZXux19vCWET/Oi4VL
File Content Preview:	%PDF-1.6.%.....109 0 obj.<</Filter/FlateDecode/First 12/Length 330/N 2/Type/ObjStm>>stream..h.t.]k.0...J...f>.v....S.&+.....hMIRp.~I.../.N.s...74F.Q.x..l._.....L.... F.e....i....7.....k..;.....5.1...T..f..0v.jy.P.-...!....s..@....=^C-.MF.....r..d..r

File Icon

Icon Hash:	74ecccdcd4ccccf0

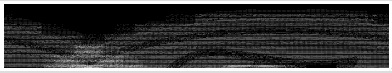
Static PDF Info

General

Header:	%PDF-1.6
Total Entropy:	7.981996
Total Bytes:	1650766
Stream Entropy:	7.983466
Stream Bytes:	1639483
Entropy outside Streams:	0.000000
Bytes outside Streams:	11283
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
29	0000000000000040	0fa841a99d93cd8796561c79b13f0b3e	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 7136 Parent PID: 4940

General

Start time:	00:30:28
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\404.pdf
Imagebase:	0x1360000
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

Show Windows behavior

File Created

File Moved

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 5076 Parent PID: 7136

General

Start time:	00:30:29
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\404.pdf
Imagebase:	0x1360000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: RdrCEF.exe PID: 2248 Parent PID: 7136

General

Start time:	00:30:34
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0x1100000
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 Show Windows behavior

File Read

Analysis Process: RdrCEF.exe PID: 5376 Parent PID: 2248

General

Start time:	00:30:35
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,179323468251003 6335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=10825893705877279914 --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=10825893705877279914 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1100000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6792 Parent PID: 2248

General

Start time:	00:30:35
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1700,1793234682510036335,8651460955286290735, 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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAA AAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAQ AAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUA AAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=2127389532984776761 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2
Imagebase:	0x1100000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 6880 Parent PID: 2248

General

Start time:	00:30:36
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,179323468251003 6335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15934386517068702169 --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=15934386517068702169 --renderer-client-id=4 --mojo-platform-channel-handle=1820 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1100000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 1244 Parent PID: 2248

General

Start time:	00:30:37
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,179323468251003 6335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=5360389963267492183 --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=5360389963267492183 --renderer-client-id=5 --mojo-platform-channel-handle=1968 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1100000
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 Show Windows behavior

Analysis Process: RdrCEF.exe PID: 3396 Parent PID: 2248

General

Start time:	00:31:04
Start date:	05/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1700,179323468251003 6335,8651460955286290735,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4148878045607610064 --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=4148878045607610064 --renderer-client-id=6 --mojo-platform-channel-handle=2976 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1100000
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

Show Windows behavior

Disassembly

Code Analysis