ID: 438549
Sample Name: 46.896.524.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 18:28:23
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 46.896.524.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 5
Sigma Overview 5
Signature Overview 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 22
General 22
File Icon 22
Static PDF Info 22
General 23
Keywords Statistics 23
Image Streams 23
Network Behavior 24
Network Port Distribution 24
UDP Packets 24
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: AcroRd32.exe PID: 5724 Parent PID: 5972 24
General 24
File Activities 24
File Created 24
Registry Activities 25
Key Created 25
Key Value Created 25
Analysis Process: AcroRd32.exe PID: 5712 Parent PID: 5724 25
General 25
File Activities 25
Registry Activities 25
Analysis Process: RdrCEF.exe PID: 1836 Parent PID: 5724 25
General 25
File Activities 25
File Read 25
Analysis Process: RdrCEF.exe PID: 4180 Parent PID: 1836 25
General 25
File Activities 26
Analysis Process: RdrCEF.exe PID: 6116 Parent PID: 1836 26
General 26
File Activities 26
Analysis Process: RdrCEF.exe PID: 4560 Parent PID: 1836 26
General 26
File Activities 27
Analysis Process: RdrCEF.exe PID: 5636 Parent PID: 1836 27

General 27
File Activities 27
Disassembly 27

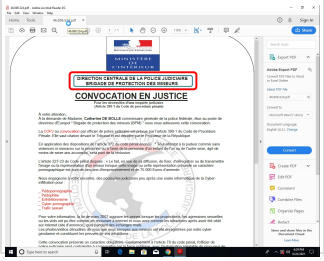
Windows Analysis Report 46.896.524.pdf

Overview

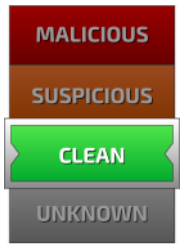
General Information

Sample Name:	46.896.524.pdf
Analysis ID:	438549
MD5:	62b935b490a6b1..
SHA1:	09161204aa313c..
SHA256:	83b25d7d8ab99c..
Infos:	

Most interesting Screenshot:



Detection

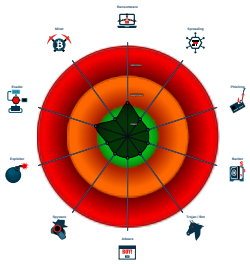


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 5724 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\46.896.524.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5712 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\46.896.524.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 1836 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4180 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=1748,247041772033505157,388763858971282016 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=18154713270360583040 --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=18154713270360583040 --renderer-client-id=2 --mojo-platform-channel-handle=1744 --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=gpu-process --field-trial-handle=1748,247041772033505157,388763858971282016 1,131072 --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=KAAAAAAAA ACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAA AAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5327604125794324983 --mojo-platform-channel-handle=1696 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 4560 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=1748,247041772033505157,388763858971282016 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11484347080584688627 --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=11484347080584688627 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5636 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=1748,247041772033505157,388763858971282016 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9495211575289344956 --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=9495211575289344956 --renderer-client-id=5 --mojo-platform-channel-handle=2140 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

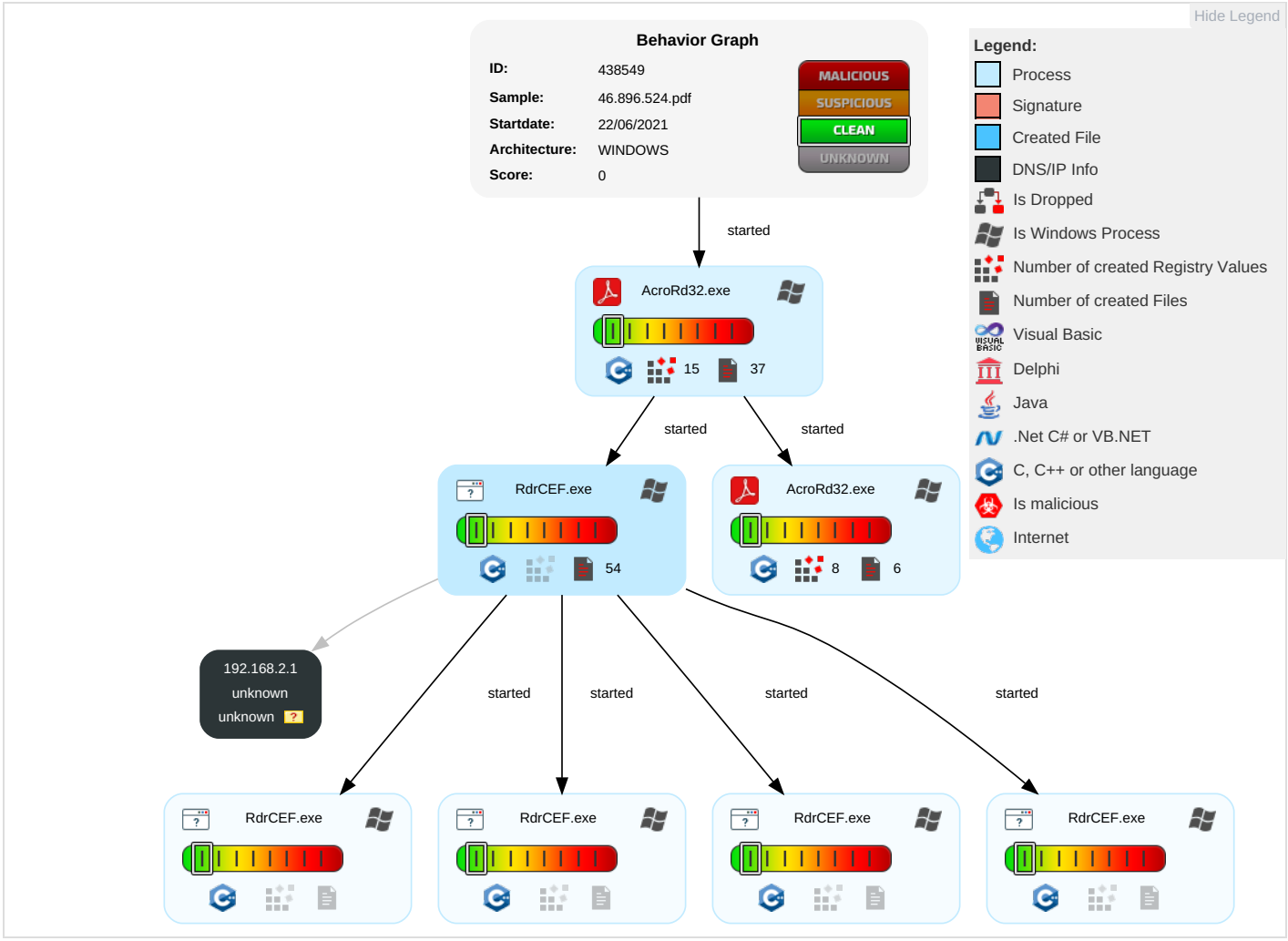
Click to jump to signature section

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

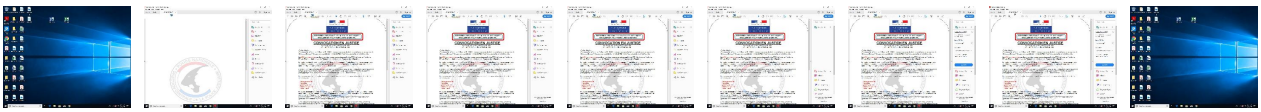
Behavior Graph

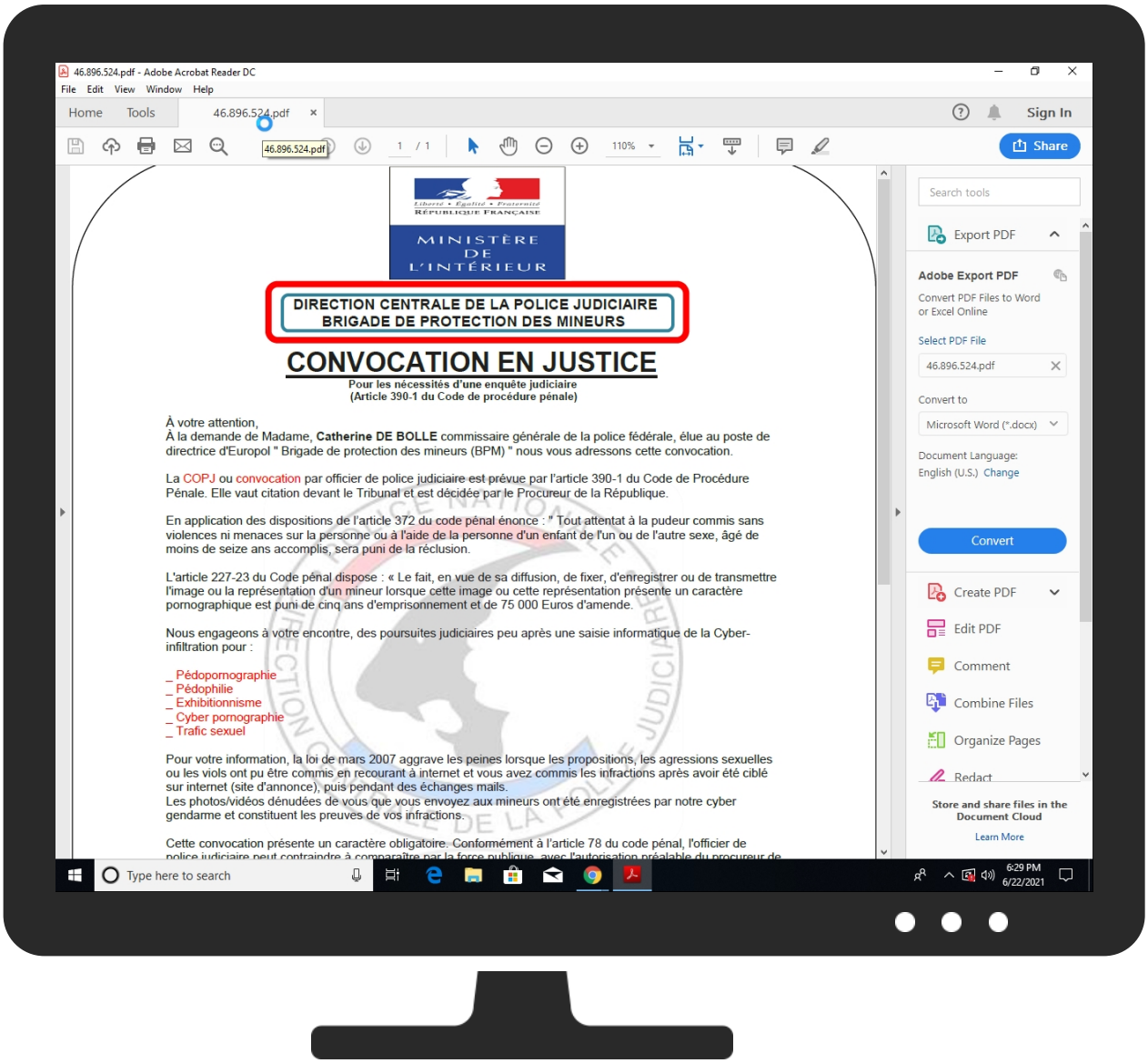


Screenshots

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
46.896.524.pdf	0%	Virustotal		Browse
46.896.524.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:	32.0.0 Black Diamond
Analysis ID:	438549
Start date:	22.06.2021
Start time:	18:28:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	46.896.524.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:	8
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winPDF@13/48@0/1
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

Simulations

Behavior and APIs

Time	Type	Description
18:29:21	API Interceptor	8x 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):	410
Entropy (8bit):	5.644311880495737
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Q1xWGqv0i7Z+P41TK6tNf2en9YOFLvEWdM9QZiS/i7Z+P41TK1:vDRM9cxBqv3ZiE7fDRM90wZiEny
MD5:	72F74A80A78AB35FBCAA6A790AAD8E3B
SHA1:	386AF0D85F0E736D776F972C7AE6F2C53FD615CD
SHA-256:	882875E32FAAB192713567EC4C80E2E8134D26B5D486691BC89C6DDD4F84B9E5
SHA-512:	54F22C99BF8B5793694CCE3F07D275A69669493637BBD6E48E58411BC4DF1FF0033F3B52D0A9C7981F71C9D99FADA51916059EC8A1CF529629428FB2A0A6ADA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .{.*..#/....."#.Dn....4.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... ..+D.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .oFY..#/....."#.D.....4.A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....m.S.....

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):	522
Entropy (8bit):	5.599873748458714
Encrypted:	false
SSDEEP:	12:V9zofYtF9PQK59zDAtcXF9PQt39zEtw7F9PQx:Xz/9PQKjzk29PQPzH9PQx
MD5:	6B59700391DE1CC3AB48333E40C784F5
SHA1:	1E8DC495ABB5101C3BFD4CE5E88FFE8A424927BB
SHA-256:	2C6E8DAA8CBBB98424B67AF3CFB09CA56554488A5893ACF025700D2A5C9D3F64
SHA-512:	48C60C0EEAC6566C7BA4E22D56B926E596984EA3BE909C941088E7D7E2A9327745D932A273BCAF69069AAB587F6D6407E3CE294B85D1BA032F3107E58E6002E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....#/....."#.D.N...4.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....x.....0\r..m.....,....._keyht tps://rna-resource.acrobat.com/init.js .....#/....."#.D....4.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/ init.js ...C..#/....."#.D.9..4.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....2N~~.....

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):	492
Entropy (8bit):	5.610530565945525
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFaVG0lUo6jh7yeRVFAFjVFAFj7qM/jYlUo6j:tB4v40SBbB4v4/YSB
MD5:	DD24B9C252C154115ECBD347F97FC2A1
SHA1:	8882ADFAFDA1FFC6FF86B477859194A6D32B1443
SHA-256:	391E400690A06DB8F7643E76F5FDC486AAFE0D2A327485B1F93F42FF337ED3E0
SHA-512:	977C9F2673D09A14030A8FF4356712FBBCD91CB9DBE86D62B6263F52EE7F35F91A259EFF86B65C74B65F33E7531EC881E06D08348C7257C4364F74CB8577E3E1
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 ..(*..#/....."#.D_....4.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....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.W..#/....."#.D.G...4.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....L.).....

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):	5.622107347775726
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsK/qwKe0iWulHyA1TK6tzl:IbRkiDj/nWussZl
MD5:	E648BDDAD2A86367F73CEF200459E75F
SHA1:	C6F17D033DA78DB23C7A3781AF57F459FAEE1FEF
SHA-256:	0CCD1991264840B6419CD57EE2E35DC0D4A5DBAE9D66F3CA17B959A084924E22
SHA-512:	37F9B07F318B74C5B3B4A282CF11EDEFD2C98B8709663937B2D89E565F4072860E832862409D25B53F7AB31940D3C9BDF642F0C387F3E7F2FE5A6953DE463256
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/..#/....."#.D.0...4.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....U.....

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):	5.556963647799055
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVumRVyh9PT41TK6tJ+n:pyixRugRV41TE
MD5:	2F590CDC7A1F1D9A130CBA708DF33952
SHA1:	25A203E5150B62AFCCF49263DB33BA9029A29EEC
SHA-256:	A94F1578F19CCB1C176C87ECFB4D8D9E7855059BD2085A9E613BFCB28318B6C7
SHA-512:	D21D1610347DC5960F2BD395711078FA469E965130D42B2E70E0773C7DA5E62AF641B7DBB372A5EFEC410B237EA17A63CD6A72224D0C16EDB653B98F0D3B337
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .k.X..#/....."#.D.....4.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....*T[B.....

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):	5.61011908525835
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQm/ZVNLZIl6P41TK6trl/:0Rhk//1LZCd
MD5:	A26FBB263E2408EAFDE096D9F79C9A68
SHA1:	7454CB2660F45633A310923F12972ED8BDBD8161
SHA-256:	397665BBC74F3823F95969E1B15CB26A13EB89A44C231A8DFA83EC1D43D75D12
SHA-512:	60B3E020DF4EE9FC7EC4AF5A40F6E084480249BA93488DBFEF48BB7608F9B2BEFB73D0C0F52B51DF47C0A548CE973AE10F47BE6D369241A0A2EB00C6D4F540 C

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .1.S..#/....."#.D..}..4.A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo..... ..g.....

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):	5.487706223324518
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVEGKltYwcyxMtv9EWm1TK5ktW:mJYOFLvEWdGQRQOdQVntB6g1TK6tbut
MD5:	4238028DD42A7B3C7F5125B7CC5880BB
SHA1:	A458223F0623C87A0C2EBCF3291D481445286B85
SHA-256:	26F872BF6487E1BDB51CCC9DEC51EC02A65C32E161187AB98BCAE36178D79E84
SHA-512:	FCA99261FC66B353DD4E1D6CCE9A8CAB8A668638C810665396E870414F642F890E1DF0A113DE009A2C9134E8514C6799213629D73ABC997F1AAD8C02B8C3F40
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..@Y..#/....."#.D|+...4.A..c..y/L....|y.n..C/l.....X7-ne.A..Eo.....A..Eo.....kQ.....

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):	537
Entropy (8bit):	5.627762932115294
Encrypted:	false
SSDEEP:	12:Z5MWnMuR/EEz5M0AMuR/EZ5MyXUOMuR/E:ZS5uR/EEzSOuR/EZSyE/uR/E
MD5:	FF7E853057D1198EF3058B564AAAB35D
SHA1:	94CE80CB1730D76398585FE183D1F6DD982F81B9
SHA-256:	6B12B4FFCA1B7C8E2669DAEFB51CF1B59827CE329A89BF10547DBBE952BC0005
SHA-512:	9EA9333154E5D3250355A1C336443BFBAA89D2440DED64342D5931236815BB0D6EB6A5959D368F44391E950F250F371D07042A661B66C7095E8E77463134757E
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....#/....."#.D....4.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....A..q.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .?....#/....."#.D@....4.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....d..l.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .P.C..#/....."#.D..9..4.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....e.....

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):	5.467891807841453
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtucziVMby0zBUKSAA1TK6tRH:pR1Zbe
MD5:	792E44C3EB9CB1928E6DDF017F01EC96
SHA1:	B98F1C741CDF01F71F9674B580F253466E5AA893
SHA-256:	C90FF7E4F7BA20FA4FED4750CA186AD3D2543593333178B85A4FC23DF577BFFC
SHA-512:	D70CDB8E09CAD632C663B9416D2332EDC4CFDB057586F8B3F14D3CF011B00C7F577A5AC98D6AC8050C12AFA41759571FC3DF07E48B1D80328DC5CAB49D7B8AC
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...Y..#/....."#.D.r...4.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....t.....

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):	531
Entropy (8bit):	5.566543156268537
Encrypted:	false
SSDEEP:	12:KkXxKMSCvqpXFvtUlQkXxKMSCvuJRvtUlekXxKMSCvROvtUl:KkXxiCivWQkXxiCeZWekXxiCwW

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
MD5:	E681DA8264211D404BCA91658ABA0E70
SHA1:	30571FB06993EA66E62F6CC55891D8028280AF8C
SHA-256:	19CC12F597C682F46E92E83AE0F3E28CA6F6D1E14D765AE3F0005621F972C4BB
SHA-512:	0FA81F7EDDC142AFCFF0AE843E08EF66D12D3B2BB793B25B8F9A53418E279738D0A2F5553150CD0D10244E2BBEFE6EB8BB8D7268B68740435BD5D2F67979C18E
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ....#/....."#.D....4.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo..... .....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .G....#/....."#.D....4.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....L.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .;.C..#/....."#.D0.9..4.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....uCu.....

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):	374
Entropy (8bit):	5.6060259676115445
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLj85PGJyM+VY1TK6tLCekl9YOFLvEWsfOLP2/3Uc7yM+VY1TK2:5h6OLj85PGEkmh6OLPm/ak
MD5:	E79394EAD84AAE464EB27827449531E9
SHA1:	5ACB45C79C06D5B8C4F790F789A9E96E2E9BBDFD
SHA-256:	AD62E50113139D5029E596F93BA92E47A198CFE4CE671EA5FAE32A3F3609544F
SHA-512:	8B412CCAD91B87263D1262975B663D89D7E9CE4FA02B69D02643F2BE36E6047594CCACAA2F20CE44DB67FB48C6F422A94DD304F63C0A07FF9FA0FC4546BA4F7
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...$..#/....."#.Dw....4.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....[Q.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..P..#/....."#.DC.n..4.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....>g.....

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):	488
Entropy (8bit):	5.647106626359981
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFS+GwSeKaTLnhORVFAFjVFAF0xwSeKaTLnc:UB4v4SfwzXLnhOB4v4SwzXLn
MD5:	73E4FAACE7166B0584E30F15798A858F
SHA1:	71124980D570B653826412E5B5FCEBCDFD544B04
SHA-256:	61E2927F0F71EA353DE8EF5425A70302E549D968030F6F88BF02862505412EBC
SHA-512:	69868E9160C8A9C8900A891BDDF97607EAACE104AE9154801D67A5F3D7FB27EAC30801DDEB854D5B441402DCFB188B63A15B3421AB17CF24FAD28B422A815C0
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 ...*..#/....."#.D.....4.A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....Y;.....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 .}.X..#/....."#.D....4.A.....H...{...2../.k`..r4.C. .A..Eo.....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):	5.46060506024362
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuKTWGqQCyFY11TK6tf:BsR2EseGtQnGF
MD5:	39DF203AA8966E4DD4ED69DB0A53A7D3
SHA1:	59D26C0A6E185B4CE16575C38EA915D29012F30F
SHA-256:	3C418EE0885FE9E80C35299F7D2FC40B7B514CD3F2A18A684F445639BE84F8CD
SHA-512:	2E7FAE698364F974BE6AA5581D44B84A4680FAB5364A70E1ADDEE98E36DA61953027554431C1A6C10DD1F4BE66B165DBCDCFEFD512AAF43657D890C4A619F26
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...X..#/....."#.D.....4.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo...../.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.635533380100546
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQHyl/lL4B7OhKlvA1TK6tR:RbR16K2/lL4BJkb
MD5:	7995BBA1CD3050CAEA634F8D2819FD08
SHA1:	22789307A71C51B4A2359D81DF214EA6CB2214CA
SHA-256:	8B81E1C67EB9F6238C228C38F3BC839984C1CA63ECF17F95CB9F349A179DC62A
SHA-512:	168C0226F07BB8B8B8F9FD6E7FCB06DD89C78CD3C984A7421D419F1D84D3599E53E79780DB232981E956C560B87F50C759CB1DA67548C377F272806EE239E1C
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...S..#/....."#.D..}..4.A..4T].....Tw.....(..b...EO....9.A..Eo.....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):	5.565707635380663
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuhGXZt1SQdFt1TK6t:B2geRHRQkGXNS0
MD5:	069E764E21D8A3C08BA921228270AD6D
SHA1:	50BA5990584DE441462DB18FFF76D8F08FD6E744
SHA-256:	6F9EFD61B4E21BDDA6F6A51E01352D762E414BDB65F15BC8C59DB5CB666F1592
SHA-512:	EDCAF72D1094881ACD6DDF5B59A5A8F4D16BA35C1B7EA91E3EA17097ABE2109503243D6A238CE0D503044549FF843E6610D853480D1AF1BDDFA4DF67DB6227 3
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...W..#/....."#.DR....4.A@..{o]...9o|..qY....T....{..u.b..A..Eo..... .....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):	412
Entropy (8bit):	5.614018114509351
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQLM8t1S/1TK6tl+tMzyEYOFLvEWdrIOQC/lZZt1S/1TK6tw:WyeRlqHt1wC+yeRlj/dt1w
MD5:	A3D489E7F671F109ECE19AFC41DE381B
SHA1:	1F4075EE25D9565CCC26598277217A67A070865A
SHA-256:	52A0E3C5723D3818ACD982770DD2223B616FC628E42480591E6946BBDE572FAD
SHA-512:	F52900E35BC98C7A9E8E5505DB02AB9966CDD52539E27E4029E2F91677F4A87F45FA5BE9B9BA703F4B05BC3C59CD4E5ADCDB718AC625E2630DEAD3D9A2C3F 58
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...&..#/....."#.DN....4.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ...qv.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...Q..#/....."#.D+2t..4.A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....r.....

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):	5.543749265788109
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyull/oeTrqwK+41TK6tZ9l:wRhEl/7GwK+E3
MD5:	FFA527C58808733DCCC5325E68FE839C
SHA1:	654DFBE989848BDDEA7CD932715DF4D2F4B9A337
SHA-256:	1732734AEDA7F9DCD339E721A89D1BE2CF3B7E42394E72014113DD1ECC5843FE
SHA-512:	525266C30A661F98AF628F911A26B94FB895AE427D7454A1ACC8BBB430A5CBDB57CC7A9593D969CF9EE94B53FA4D2A0161E3005C3A0654CC9412641721B21C4
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..pS..#/....."#.D.}}..4.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...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):	460
Entropy (8bit):	5.611423047928218
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuPmKhcIfO441TK6tR+YXYOFLvEWdrROk/RJbuU0x8//Wd:/RrROk/NKfLED3RrROk/p0xc/WpfLE
MD5:	9077EA56BFF507671E013020EAC54243
SHA1:	DE005FEB8590B478BE92ED5D949A35A99D1D643F
SHA-256:	A6AEA1FA64F477CA600B39B9A5B3449B5B1437EA4B7BD55A11AA184A4D659CE9
SHA-512:	C7763E559B2116D42A7785E5E906B2F78B358426BFC50C913F94CF67174067DE6BB4F4D226F3E57F374B3FA0D88CD47105D88E086C0B202F35A4E3FA1616A071
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..&..#/....."#.D.{...4.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....O.=.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .X.Q..#/....."#.DX.t..4.A..~. .rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....P..P.....

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):	372
Entropy (8bit):	5.606214784428297
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXILQtsePS1QPLr1TK6tS8mDEYOFLvEWXIc/DgS1QPLr1TK6t/:xqTFtsxCPLnkTqTZDbCPLn5
MD5:	734E94143FFBE0C90E8D22BD2748AA19
SHA1:	BD29D21CBCC4D660241C10B049C0830474FB3291
SHA-256:	6B57F374C4F638F83678948EA61E64CD37705B080685FF1F0ED6B13FB8E4F6B0
SHA-512:	3A50B97A660CA9F9C0FC816908735B0E793E7155BE142F75D94D645DECE82FD383B4B7AABAFE080313261448FD89FEA66976FB17C09F4E791179F4D200C8A770
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .pz$..#/....."#.D....4.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....0\r..m.....:. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...P..#/....."#.D[.n..4.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....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):	414
Entropy (8bit):	5.615322966725482
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuF88/sEJ41TK6t252YOFLvEWdMAuKatRTZsEJ41TK6ta:zRMo8/sDVRMBRtsDE
MD5:	A58CDFC149EFF0E3F8451EEABCF304C1
SHA1:	6653F9200687BDCF6A1CC4773699C6ED1093FB43
SHA-256:	AB67B7C194D460F0EB18C02390DBB0F51A2CA8745ABBF4CB12E17DB14D6D370B
SHA-512:	B7F3E1B9309509E2CEA5CBA675F49A57596E85B85A6ABD21EFBED1044A727A5D364962F65E5ADE8F68934E4A7E890AF131E9869C5A135B6394E26D55050D6CF
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..#*..#/....."#.D.U...4.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ..../.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..LX..#/....."#.D+...4.A..z._a...'.v.....4p3..1.']...A..Eo.....A..E o.....3.....

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):	420
Entropy (8bit):	5.5866936729564705
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAul8fFong1TK6t0YilPYOFLvEWd8CAdAuxPoUK32Fong1TT:6lJR08fFoM6lJRyoU9FoMJ
MD5:	DA76BD3A328C507434E542D7C6D0CDD9
SHA1:	FA09D39637F32A3C412B69F2D408AE363C5642F9
SHA-256:	950AE3651E47C238D8E1BA153CA287D62DF577AB0F18355286906368827B007D
SHA-512:	0E102091C9BA704040A1F1574506F9C46312C3F12443DB08086E62344AFB3FCD64DCFCE37B577F3BCE5D7297E450E430FDBA10350255E42525ABA3796D125339
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..%*..#/....."#.D"....4.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....w.....0\r..m.....R....\|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .>OX..#/....."#.D....4.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo.....G.....

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):	446
Entropy (8bit):	5.5627807381616154
Encrypted:	false
SSDEEP:	12:F8hRrROk/gtYd2e2/8hRrROk/Yl/5g2e2r:UPJ/g6n2qPJ/Y82
MD5:	BF9341321E4B365575936D038C4F203D
SHA1:	83B309FFC820FF61CAEBF24512B36AAC24619596
SHA-256:	177DAF0E0B14D13A106DE0F91D088DBD99C61940389081195A6E229C11521B03
SHA-512:	8AD91CD6D2E6758C311D159BCFF532062CA5C277F362CF9AF4C714DA39DDEF113D3A41AB62962C3F631BB6BA062A57DD5FFEC4D9382B43AC7C1EC1B4EB7C EB
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .b.&..#/....."#.D.j...4.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....3a.5.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .raQ..#/....."#.DE.t..4.A..%.k.SZ ..~W.....:)'B..ad.....A..Eo.....A..Eo.....H.....

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):	426
Entropy (8bit):	5.677923308547351
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQ1tOogeXrNJli1TK6twLrnYOFLvEWdrIoJUQsl/HZfrNJIN:ehRc4t7rNJICyhRc9/5frNJICY
MD5:	D224D7B4F36D1F165905B873B95D7A5C
SHA1:	60D8DA2F682065CB2FE885F97384B297779832F4
SHA-256:	29124ED305AA1807C98B1A328D6476F704053475AA5AF234304C06E005BB9D94
SHA-512:	A8CB32242BD5BE658115C75665E00D3101C69E544206BE3DC9A3AA95C48824A5E947E849AB7802934E06F4996887EAE212666DD24165EE0F5481F2A482826058
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...&..#/....."#.D.....4.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....|.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .l.Q..#/....."#.D.ft..4.A.;"./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....@.O.....

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):	416
Entropy (8bit):	5.557609316093466
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhukqUukpZLzgm2d/1TK6t8eOEYOFLvEWdrIhuMl/Re/hZLzgm24:0RFUuk3RedRy/Re//Re
MD5:	A4D73DEAD1EF6CF6BA0FF132DE71ED43
SHA1:	58121E093F6E2C7EFE165C94E23474351F9DC7BB
SHA-256:	7D6F6D0B8C7708456513E495EA842864204587ECF99E990BD1E42762E9B0DEEA
SHA-512:	039C48AAB76EAD66DA5A45A33118D0AEAA24D39670379B603391C6A320321A562906AB996F4AE430F1F38AC8CC0EF7207A7157A5CC7BCD7D83B2435CA2C1094 3
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..n&..#/....."#.D."...4.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo..... [.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .-^Q..#/....."#.Dz.s..4.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A ..Eo.....t.&.....

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):	564
Entropy (8bit):	5.6255356743410045
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SSDEEP:	6:mAElVYOFLvEW1KWvX2n2kx56uvp1TK6tE8AElVYOFLvEW1Kd8/2kx56uvp1TK6t1:6JJKmQSgJJKdIcfKJJKRyXt
MD5:	94842761AC6612AF3B0EA21904CCD903
SHA1:	E71178AD45CC34CE732A251F05BAD133A0F7DEF9
SHA-256:	7D6A628118028452162F00D9B9BA0E7B434C5C1D86B290056947B526DC5FDA8D
SHA-512:	FD2ACB8A277D5B064A095C9233367C280E39051382B4B9C6906B4D19BFB3DC889DBC9405650302F34CBF127706B704840A59A2DE0706910A5085041C437384AB
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..`...#/....."#.D.0?..4.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....h.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .M....#/....."#.Dd...4.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....5".....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...F..#/....."#.D.\R..4.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....U.....

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):	5.6292521552979995
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvulCtae/rhUDLYtmOZn1TK6ty:xRBJftADcFZL
MD5:	4855D0FB8D021C63F85116EC4D22CFD6
SHA1:	FA500407D8E797096A95A571AF66DC31649C9123
SHA-256:	20295A6679547C2FC961A3506DE018244D6D9810104CB413CC285E8CFC40841D
SHA-512:	8E3AC5E83D05AE28B8F4790645DB2762ED79F2513EA958BDC4CB6431C84E8CA3B15A69273C49EC75C8132E5D9C8CD2293A1E630EFEC97CA36578DBCF90B531BF
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .*JX..#/....."#.D.....4.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....m.....

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):	633
Entropy (8bit):	5.653556408651703
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp76t/vEaVPu1TK6t1sRPYOFLvEWIa7zp7iXGObaVPu1TK6tAz:BPHktXEacEPH8XZbacuX7PHqGacV
MD5:	453DA6AF8C92DA821B292578547DAA2B
SHA1:	A1F27C72E7EA67B866DCACDB1145FD4C763F8138
SHA-256:	291B2086ABA5368966083253D8F63F3AD786D6C3EF888ED526540696FBD320E7
SHA-512:	D2329AFDB4A453E916F134F647C5788E6AC8A7461AAD84A5A147A660A5C037388B6CAC11E64BC6E102C1D1FE94CB2ED7F0070C707D3EB21F02F0B64D72B70E9
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ......#/....."#.DOZ...4.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....0.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ......#/....."#.D.+...4.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....|.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...C..#/....."#.D.*:..4.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.565233267751388
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Qx/mTwiM3Y1TK6twAN:bJRT94/mcr0uAN
MD5:	308C2F83E52F7B2E9DE6CD15ADD4FC39
SHA1:	0FA8179D50DE0D4EC8983B11B63238996C4A440F
SHA-256:	208489A622F18628711FB11453F43B3E9EE982DD09F8BA3442FCD4D7E97549C6
SHA-512:	9214259FFD49F888FFDD5D2298686398AAE28A08B160DD46CC2B5426D95B8ADD3365E1CE9F6071BDF4D5A1B6B77F2458F7AF62EAF5DE835DB38BCB1FEB70FE49
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...S..#/....."#.Dj....4.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....`.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

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):	5.596436272538276
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ0ntIPQjBRCh/41TK6t5:XRc93NDi/E
MD5:	971C764234452D9267D9FFA59D1C7869
SHA1:	0A06FB878585188AFA6A49B08FA7ACACA4AE0518
SHA-256:	B73F51C8E37994197AB708C7030152DF8968B01EB2EC200DE8CF16ECBD947FD5
SHA-512:	EBC23D524BDC8472FD91CB9E3AA630F26540E54EC3A94BC3BFF7682B0D67DBA79D550097CA5F3EA1F094095D872C9B6F705CE3BAFD519472A09553D3C329D0 0
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..>Y..#/....."#.Df....4.APJm...0x.x..RD...BB!@5..<..]....A..Eo..... ....A..Eo.....n.....

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):	5.550216099987301
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhunEwVULlF4r1TK6tR:bs6xRki9Ew2LlF4n
MD5:	1449763468F2E223AE41CE1C2590BB0D
SHA1:	768016DE27175804DE4EDD7F1D6665123CBF07BF
SHA-256:	01A00181DE328148D9EF5255B4A542AF871F7509854061A29F12A228F6286417
SHA-512:	D815BF9A48E9BBCF0144A8198D86FA5B27F8B94A32255025923E621BD587BDFBDC85B4B5BEA0F7848A1EC4E60730A02D6669E53F860A3B917F48C26A32A85A6
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .}e'..#/....."#.D.:...4.A.P...#4.l....5...5..).w.. .h.~..A..Eo. .....A..Eo.....M9.....

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):	5.5251664935273705
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvqAKKX7VVCcu1isLK5m1TK5kt0FX:mhYOFLvEWd/aFu/X7DN941TK6tg/l
MD5:	EAE761436320CC180EB3E56A6867A3E7
SHA1:	403201E304A3F3B06027EF06504D843E6E4B4D01
SHA-256:	E18EC08FA7A8528D495AE967BF36ECF3025815B24F51F9F1748D60FB210D3642
SHA-512:	52E435E825ADF7BF68F5B8D0A770941B5AB15C169B4011B2D2A553A04A7C1F535D58207E3FE07859B29AC5D2079EB55B9905FEA654D79747DD6AFAD597034DC
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...Y..#/....."#.DM....4.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....W.....

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):	5.555764039859369
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQLtA0y9ZoBMqVd3G4K41TK6tNl:2DRuRoA03B9Vd2k
MD5:	2F585974C84E27D691ED9584FE912F6E
SHA1:	98C23EE634D00002AA1F7BC1993625F770023365
SHA-256:	0AD81AC9B6A8811DC5FBB30A7838E7B8940BB68781C221009A94CDA1950C2BD5
SHA-512:	9FF13D8CB4FAC1D45631AFA0B57CC10E587C2E92C1D2BB049C916F738A32C7FC6AA57A7A6C52B8D7F7ABD65ED2C45C56EC04413063D7782C3116159EC495C C1
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .M.Y..#/....."#.D.Q...4.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....Z.....

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):	416
Entropy (8bit):	5.60180146696472
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q2QtaSOuA424r1TK6tFEkqYOFLvEWd8CAd9QthVPOuA424re:+RQ7QtaSBrnoRQehVPBrn
MD5:	DB551B06BDAF78EFF75383E783BD8533
SHA1:	BA974BA3DA10DA1109E126ED168E1F82DC34C181
SHA-256:	C99D0EDB95742BFB2C444569AFDA0E78273B93FEA58DA7262320BC4F33B41B83
SHA-512:	761371D4C1FF5B2364F9F8AEB6015CFB62ADDE5A58F70D5122D560F44C2CDDEC3AA2FD5E3DA925D7DA833842EE2D8475C44D251AFC6A561990DECA1F40CBD 69
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...*..#/....."#.D.....4.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .-.Y..#/....."#.D}Y...4.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....p@.....

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):	5.523666724863864
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuzFnl/KxnuyC8n1TK6t:xhRTxBl/b7Q
MD5:	4C40D6CE950C0A9574C40B38B95DCB0F
SHA1:	5AE4AD581310FC1340FD140076F1C9679FF6791F
SHA-256:	48BC903968C01909F19768F2DBBE7329E93DEDAC0660C14745E8316F60070712
SHA-512:	C604E07EA6F6D37CFD58CC4BB81CE987635C5BE55056EB3EDD79C3AADAEFD6906F4A2BEDA24D1B21F558E379E721C4BC01B1CAA45A21564C80574EE405F40 430
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..nS..#/....."#.D.a}..4.A8.../...;.\\o....1.....+..A..Eo.....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):	442
Entropy (8bit):	5.587093042252644
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQTWtQsLmB41TK6tiQZYOFLvEWdrROk/VQ4//V3sLmB41TK+:nRrROk/VHtQNmpRrROk/Vx/1Nm
MD5:	64001A2BBBDC223EDCA604B3716F2681
SHA1:	18D299423FD72F543CECA4DAEEB8699967B7FBC7
SHA-256:	4EB67F205C977A79DACDBCDEDFEF0C4FFEC15C0A6AFD84993AE641F1484F8B47
SHA-512:	1358E19F94B21852C493B89A14BDC36C59D6B6CFB0FD1B80BD7FFEC5BE39FEDD54B7454278D19C076AA2DDD52B74DBD0C03EC4E2E8ADF7E3EEAA940F6156 391
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...&..#/....."#.Du ...4.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....r.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .i.Q..#/....."#.DOxt..4.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....q.....

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):	5.574563992546808
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWurERtu9woAdm9741TK6t:qxRcpE7u93Adu7E

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
MD5:	7AB9CD2ACF3F474804F22E3B3DDECA60
SHA1:	F114B897F048C0618C2E92168DDE10D12B2218B3
SHA-256:	4E576D5579EC2CE185414930C744AACE1BBE113A67E6E18011A2A32453CA7BC5
SHA-512:	85C3F797B4513787DB7B25486A7A082B2C5D63C0FD454506D3A3F31294711F2AB5AD2175E9D68DD64C8DE4A7FA43684540D4E593087AD8EA6E6DDDEBAFD8C0C
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...W..#/....."#.Dy....4.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.562223816160515
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuqga/gZKarJn1TK6tXl:2R1Ga/gZKaNL
MD5:	E46AE57E4D3B0A56FA9F623F0797D549
SHA1:	48D8F726E298F6D9E16D9F24F94F923E29C5F8A8
SHA-256:	2DE41DC603C735E36687F1E365832D6B68CACA6E6A3F2319136CCDD849F29A67
SHA-512:	28DC70B794AB6D3C1F07EE55CFC3B56161FF4896E2C4F21D6A8E96A4DE99DFDB718D2BE254316743CFBE21584DCCE8829EA6C2EA1CB823949554B215B272FBF
Malicious:	false
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..gS..#/....."#.DT;}..4.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....51.....

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):	5.626306421092851
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQKrzhcsBXIh1TK6tB:mxRBJQTrDB03
MD5:	DDBF01627375871B051A7DFFE9A23FEA
SHA1:	6795761A11D1D366E8830C1AFC6701E1FC41E47F
SHA-256:	7F3F29C11F1F79A0780796D89B17C9E16A573042B7CE2C8E1502F3A895D8CE3F
SHA-512:	47EF7CDCF87F82F9962EFDC1488260A2748BB750F18E974F3D5AE7A5500AA5F66C3DD483D6CD93925D4A5D4C6C9EBF18536286AE0EE5264C00A4FAC1E43339F
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..CY..#/....."#.DP....4.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....z.....

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):	456
Entropy (8bit):	5.617068312171662
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQDYeKMc3Me/1TK6tn62sPYOFLvEWdrROk/RJUQt0Ta/m0:3RrROk/sC/cNCRrROk/sCSa/mc
MD5:	FDF2164FA980FD3FB07FCBD2C91A7A60
SHA1:	860B95D26A03856DADA958D0374BC7BC0FD272A4
SHA-256:	1D131F9719069A70643B8E4121861B3A699BEB576BAB1EE9F6CE48F21D262AF5
SHA-512:	423AD00A359B400AC20A3A787BCB3AFDB1231890DA93A5C0EDE7F82FADB61353AA001604C6578CA5F634B5DAA31068046E3E364D6352F92E2F8916AC62477F4
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...&..#/....."#.D4d...4.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....W.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...Q..#/....."#.D..v..4.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....T.....

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:	Maple help database
Category:	modified

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Size (bytes):	1032
Entropy (8bit):	5.126604872787435
Encrypted:	false
SSDEEP:	24:rH3AoMzx2awN9MkPFYM1tGnKihRS0htw9Ec+7QAnn0q8AYY+JOcAjeBJ:rQoMN2aS9MkNYWmKihRS0htw9Ec+79nw
MD5:	6EC91480F21B2460E5AD64FF56B07982
SHA1:	86E456A0A64D4E3521A99A0FCF900C84E2E38C99
SHA-256:	90DB5283CDAF68E28FC191E6612E34FD854A3E236AB5864E45D3DD86B2D22045
SHA-512:	F1E0C3094273D67B52852F177CF765FEF3C2CCF922738834FA899ADD799930AC0EBCBEDEC8BC2CCC2007B1627D95D995EB4993DDDDF9C886B04CFF1DAC485 04
Malicious:	false
Preview:	.....oy retne....).....T.....3.....T..#/.....v...q..@^E..#/.....C..M.....k.....#...(...k.....]...I...&..#/.....&..#/.....6<|.....6..#/.....<...W..J..6..#/..... ..oB*..6..#/.....a.....6..#/.....;.y~A.@^E..#/.....P....V@^E..#/.....F..=z;.@^E..#/.....o.@^E..#/.....*..@^E..#/.....2q....@^E..#/.....Gy.'.h.@^E..#/.... .....k7A.@^E..#/.....:.N.A..@^E..#/.....;/...T..#/.....T..#/.....P[. q..T..#/.....,+..._.#..T..#/.....J..j.....T..#/.....A?.2:....T..#/.....q...T..#/.....u\].. q..T..#/.....!...0.o..T..#/.....*.....T..#/.....o..k....T..#/.....^.~..z...T..#/.....[.i..%...T..#/.....+.{..'..T..#/.....@..x..T..#/.....*)....J:..T..#/.....&.S.....T..#/..... .....MV3....T..#/.....D.4...T..#/.....+.U.!..V..T..#/.....~.,.4>..T..#/.....

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):	289
Entropy (8bit):	5.248700541397674
Encrypted:	false
SSDEEP:	6:mv29q2Pwkn2nKuAl9OmbnIFUtpC6ZZmwPC0oPkwOwkn2nKuAl9OmbjLJ:N9vYfHAahFUtpTZ/PwP5JfHAaSJ
MD5:	9E16D1AF1872DBC949A774F7BB843D7F
SHA1:	8BF67B99D000498F538A2F1F0439D1E3F96E5366
SHA-256:	E31F913138991B469E0A65BF2D31DE2A217539BD6366B09C3331E2D7424AF7C4
SHA-512:	27BCD3A1F306D2B537CEDCB415920028E364B292767B7DF0B6065ADC745FF6328E00E2267894807A3860C086167B0BBCEBC728367813DFC0F5B10B0481905FC1
Malicious:	false
Preview:	2021/06/22-18:29:28.941 564 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/06/22-18:29:28.942 564 Recovering log #3.2021/06/22-18:29:28.943 564 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):	917504
Entropy (8bit):	0.007871448983364983
Encrypted:	false
SSDEEP:	12:I+mmTsx+mmTsx+mmTsxlNTpyxHHyTpyxHHyTpyxHHyTpy:TmbsmbsmbPXytHwytHwytHwy
MD5:	434100DF64C916FE8366CC40E90C7EFD
SHA1:	FAC703A9255FD29AC8E8606BE59241C1F07C9A50
SHA-256:	13731A1522DB031B5B50069DDDCAE2A03BACB6B75DFF565CFB25C980126A8DE9
SHA-512:	E750280DC5E98194B163E42D54F049F5D538C09E28F8136D2F56D7A94C7DCA4A3F8BE46BABD18E9E68DFF243C774EB988360A74FB9A04843493831CD4A2FB20
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2106221818092-260.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	3.1254041493636144
Encrypted:	false
SSDEEP:	384:QmK6+Uz4Y93dwLWQcHHMPtAq0KMtO2DCHxuJFpDxy:H4K3fcGq0wup1y
MD5:	289D67A01333FD6F020051216FFDDDD5
SHA1:	404F8A18B941AB0C4DF2E076B236795AE5ACE1FF
SHA-256:	9FD24C51B45B3EB64CCD3D88834E88F52DEC6CBF0EE0D0144680D780A7C5A084
SHA-512:	BF59D003900885C40DFA807B2873D6D3A93D672901807D09FE26B57B9BA0BBD77124DE371F833CA48A0AF67C9E4DDEE8EC3A66E6EBF3E182B10C2C6FEEE9D9 5F
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2106221181809Z-260.bmp	
Preview:	BMV.....6...(...k...h..... .....OOO..... .....___.....OOO... ....___.....ooo.....

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):	32768
Entropy (8bit):	3.447738910484315
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CK749IVXEBodRBkWCgsOh1CKr49IVXEBodRBkWCgsOh+:HedRB2edRBUedRBSedRBy
MD5:	60900469F77AA626E6C2AB452A1ABFBF
SHA1:	5D4BBEEAC17B927A153BF87AA4E05792D08CF21B
SHA-256:	F64FBBB0AF766FDFFDF88CFEFAAE394582884985D42D58D7EF4D115FF4B30573
SHA-512:	9AE029721D119E6014A007D60F0CE6F1ED47D74D524E161C796C951E53A090F27FD84F35CE40CB5387F8B3C83FC839C50E1568007E296A10105A6D6238829355
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.3164702667879715
Encrypted:	false
SSDEEP:	96:SCgOOhZCPi949IVXEBodRBkKCgOOh1CKWt49IVXEBodRBkICgsOh1CKUd49IVXEJ:EiedRBESedRBaCedRBeyedRBR
MD5:	5609BC3F0D91B9B62DDBEF0F42C1A951
SHA1:	A3CFFA0EC3E4532664D78488236D7B252DD56756
SHA-256:	C863708F0722CCE066D0233AD75F5C17D35359544E827F9AFD66B3DA3341604C
SHA-512:	C696F75D90175C755A886E93C8832A384C4D60C38782F1812AECCD8787A66980DA86D13D747FC1B26C2ED639843C3C987D6FE2DD389E71C1F2DEC4CACF99E8 4
Malicious:	false
Preview:	.....2..... .....W....X.W .L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZvSUGciYV+aNxytfIwjhoCrMZoTqYyu:J0GpiyVFihaUGciYVPytwwsoTqK
MD5:	57CD7A15901AF46340C5F935D2CE1264
SHA1:	30D8D1CFBADFEFF524D08350BF62AEFC699C9DD8
SHA-256:	9652205F881C14B7B0865AE84847C6A4AA913337E6C80BD1558095FDE698031F
SHA-512:	2214CC4CC7E6B34697EAE30E97A756DE18C2042B13EE1EFCA93B6364467DE1B6AA240843AB1B9B22BC1BC49C86DED4E90D98C6799C15CF7D5EE92EA7E8490 D1
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

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

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store	
Category:	dropped
Size (bytes):	200
Entropy (8bit):	6.934613832614919
Encrypted:	false
SSDEEP:	3:Nlm3TnZ1PWNmIkP/wkIQOpVou3ms8xKGL8sP8PJJYwfZEmaNAkIIidQPeuWr2DW:wdKinJ+VFWVxvRPAYwfZEmapQHu7W
MD5:	5899D998731A4A9337869D49C04FD8DB
SHA1:	15859C86F73A4F8DFEF2C64F4A9833F02242D893
SHA-256:	A0127D63E20482835F839E787AC3B684BD65EF1FDD1D381810240E3F94876AB6
SHA-512:	2C4010EF24D15FEF70055980FCC4927CF629ADB9A5820D3A0670FF4542F6A39633D3198F2684A2B0A8F319BB315F80E062307419662723D020FD2F6D49BE89F1
Malicious:	false
Preview:	...S.v...:@..hC-.H.QE..|....l.s.....0...!.k..'T.U.....epaCp\fw.f+.....U.h3..s..+1.M`-..`.....Y.d.{....C.....I*.....IM..=B.]QV..F...)'....^.2....._CR...Y.....m.C..|.....q.?.u.{....X.J..J

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:	MS Windows COFF PA-RISC object file
Category:	modified
Size (bytes):	1328
Entropy (8bit):	7.8586600085802205
Encrypted:	false
SSDEEP:	24:FDVDuHh0UDvNs90LbglAUnYn/fVtBUG6/HOKZP2ZWedbpUQK:FDVQh0IseHGRc/TBW/uKUEY2t
MD5:	F4DA58794E43BC05D7FBFB49300A3D25
SHA1:	A089EB6F634C19B95A804EBBDDB8854316DD87AF
SHA-256:	B81A2359D689BF6611E529F93A285E3E1827D07E8953DFA92CDE0F85646136C0
SHA-512:	8374395D425C550F42DDE0FB614B0918BD61FA763B2A94A32FCB8EA913CDC97A8FD6202FE6D5EA01A4204DE5213A1140C91D9639585408C198AF9D8591198C6
Malicious:	false
Preview:	.....J0....^RS.BXQ$i.....e._.=#T.e.Z.<.t"5.y..X..X...Wa.....2...0em-...N.&wK.....L.^.X...s.k.fP...W..<yM..S.....<].tT....v..3h...g...:[W...Z-:.q..D.:e..z..>.8w..z..?....F{.n.. ....rP....T8.f ..1..v..v..:O(.....$....J.E.7.!..I...>..,...3.D...{....k%..g.....ye.....5..NY2.5.4...b.....~.VEjx..U.....S....6q.:.RDVJ..0.:LDq..c...]^.....-.U..$-....E.....M.....).i$...'=F_....T^..&.V.U.MX.; .....R..h..o.....6.R...SX.....ER.Q1....<^s.zf.eb...M;..1.....TX.....j.Y.{u.....i..4z\[.q.....#.ZZs.uT..(.h9...r....}.....=.RA....ZF.rc....u..t...0).`n.t).W.C...[$.},aC.6....i...?w&rB{..NH9...5.. D.'.....'..!.pB.pw..Ks.O.B.....v..>.....%..G."4)....v0..O....,(~..Ti.B;.e.....4...A;...rB..O.....2..]...W.S..Bu.....b.}...9...].dVER.o.....:.j.&...:&.)..''<....8....:...$.6yI....4:W.`..... ..VIc....|.c;...:..xR+K.d....4:~..*MVs.%.rO...b.....J..F....H.Rk.o.0..Pi.....<_..C.....*kB".y.L..o....J....^.....H.7..4n..Z..&...o.....pV....r..f.}.....

Static File Info

General

File type:	PDF document, version 1.5
Entropy (8bit):	7.9780418430780315
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	46.896.524.pdf
File size:	225897
MD5:	62b935b490a6b135623d5f50ab63364c
SHA1:	09161204aa313c21fdb597e1d4fe0c8a5e511644
SHA256:	83b25d7d8ab99cedcabc6aecc183b3c949b95c886c9940ab0d2e149edfeb823e
SHA512:	e0d9d77d3a8469dc93fe8157f2456de3a9cb5e472c19ecac7dfad138e975712ffc6e56ab38bea19d010f78eb5eaa0f3f7a3a1d56785555e480da33af31885127
SSDEEP:	6144:IhYqHqiUYVgeH4anU1yQOLFq3p6iCCr5W9m3F:I3LnVbU1hOgZ9CCrsM
File Content Preview:	%PDF-1.5..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(fr-FR) /StructTreeRoot 29 0 R/MarkInfo<</Marked true>>>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</XObject<</Image5 5 0 R/Imag

File Icon

Icon Hash:	74ecccdcd4ccccf0

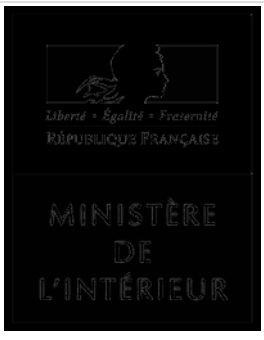
Static PDF Info

General

Header:	%PDF-1.5
Total Entropy:	7.978042
Total Bytes:	225897
Stream Entropy:	7.987463
Stream Bytes:	217198
Entropy outside Streams:	0.000000
Bytes outside Streams:	8699
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
5	8e0b000000000000	07b752382f3f218b367df0893ddb06b3	
6	8200000000000000	2e978f6b1934b8a7eabd5a254294511e	
8	0f274c9a9c6c2b0f	53e6a4527c2896bbb7abc80eb598cb5f	
9	90e8e4d4e8d4f2d4	e78a1f167b42c5f47ed3674a45f754f5	

ID	DHASH	MD5	Preview
11	061315260b0f190a	4b613cc34afe09140936f0848e8a53cc	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 5724 Parent PID: 5972

General

Start time:	18:29:12
Start date:	22/06/2021
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\46.896.524.pdf'
Imagebase:	0xc00000
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 5712 Parent PID: 5724

General

Start time:	18:29:13
Start date:	22/06/2021
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\46.896.524.pdf'
Imagebase:	0xc00000
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: 1836 Parent PID: 5724

General

Start time:	18:29:20
Start date:	22/06/2021
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:	0xfa0000
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: 4180 Parent PID: 1836

General

Start time:	18:29:23
Start date:	22/06/2021

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=1748,247041772033505157,388763858971282016 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=18154713270360583040 --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=18154713270360583040 --renderer-client-id=2 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfa0000
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: 6116 Parent PID: 1836

General

Start time:	18:29:25
Start date:	22/06/2021
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=1748,247041772033505157,388763858971282016 1,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5327604125794324983 --mojo-platform-channel-handle=1696 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xfa0000
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: 4560 Parent PID: 1836

General

Start time:	18:29:30
Start date:	22/06/2021
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=1748,247041772033505157,3887638589712820161,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11484347080584688627 --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=11484347080584688627 --renderer-client-id=4 --mojo-platform-channel-handle=1832 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfa0000
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: 5636 Parent PID: 1836

General

Start time:	18:29:33
Start date:	22/06/2021
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=1748,247041772033505157,3887638589712820161,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9495211575289344956 --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=9495211575289344956 --renderer-client-id=5 --mojo-platform-channel-handle=2140 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xfa0000
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