ID: 483802
Sample Name:
8795156_490162680Email_Correspondence.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 14:03:45
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 8795156_490162680Email_Correspondence.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
Jbx 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
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 24
General 24
File Icon 24
Static PDF Info 25
General 25
Keywords Statistics 25
Network Behavior 25
Network Port Distribution 25
UDP Packets 25
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: AcroRd32.exe PID: 6380 Parent PID: 4896 25
General 25
File Activities 26
File Created 26
File Moved 26
Registry Activities 26
Key Created 26
Key Value Created 26
Analysis Process: AcroRd32.exe PID: 6472 Parent PID: 6380 26
General 26
File Activities 26
Registry Activities 26
Analysis Process: RdrCEF.exe PID: 6520 Parent PID: 6380 26
General 26
File Activities 26
File Read 26
Analysis Process: RdrCEF.exe PID: 5344 Parent PID: 6520 27
General 27
File Activities 27
Analysis Process: RdrCEF.exe PID: 5132 Parent PID: 6520 27
General 27
File Activities 27
Analysis Process: RdrCEF.exe PID: 6772 Parent PID: 6520 27
General 27
File Activities 28

Analysis Process: RdrCEF.exe PID: 1972 Parent PID: 6520 28
General 28
File Activities 28
Disassembly 28
Code Analysis 28

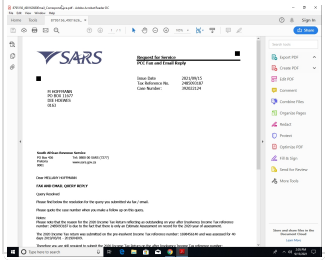
Windows Analysis Report 8795156_490162680Email_Co…

Overview

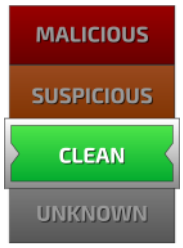
General Information

Sample Name:	8795156_490162680Email_Correspondence.pdf
Analysis ID:	483802
MD5:	20da3e9fb6519f8..
SHA1:	1d064b479bb9c3..
SHA256:	65492564da5ba6..
Infos:	

Most interesting Screenshot:



Detection

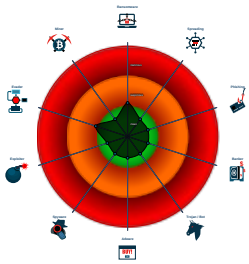


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 6380 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\8795156_490162680Email_Correspondence.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6472 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\8795156_490162680Email_Correspondence.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6520 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5344 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,49734726695296726,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12528180285023581782 --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=12528180285023581782 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5132 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1692,49734726695296726,14708380478045234943,131072 --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=13295799918542925837 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6772 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,49734726695296726,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14045389042154872069 --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=14045389042154872069 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 1972 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,49734726695296726,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8578766355593294049 --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=8578766355593294049 --renderer-client-id=5 --mojo-platform-channel-handle=2112 --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

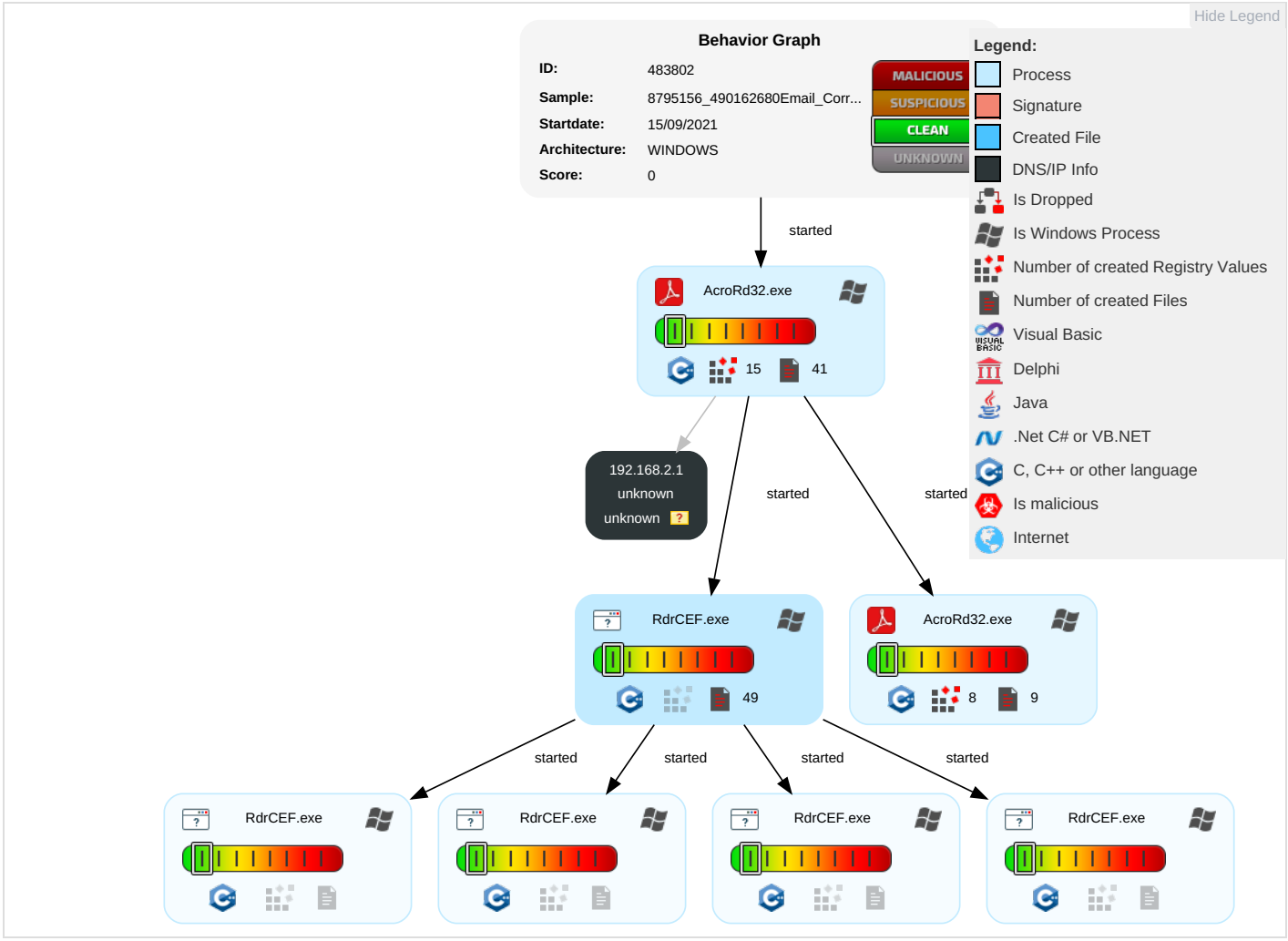
Click to jump to signature section

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 2	Masquerading 1	OS Credential Dumping	Process Discovery 2	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 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

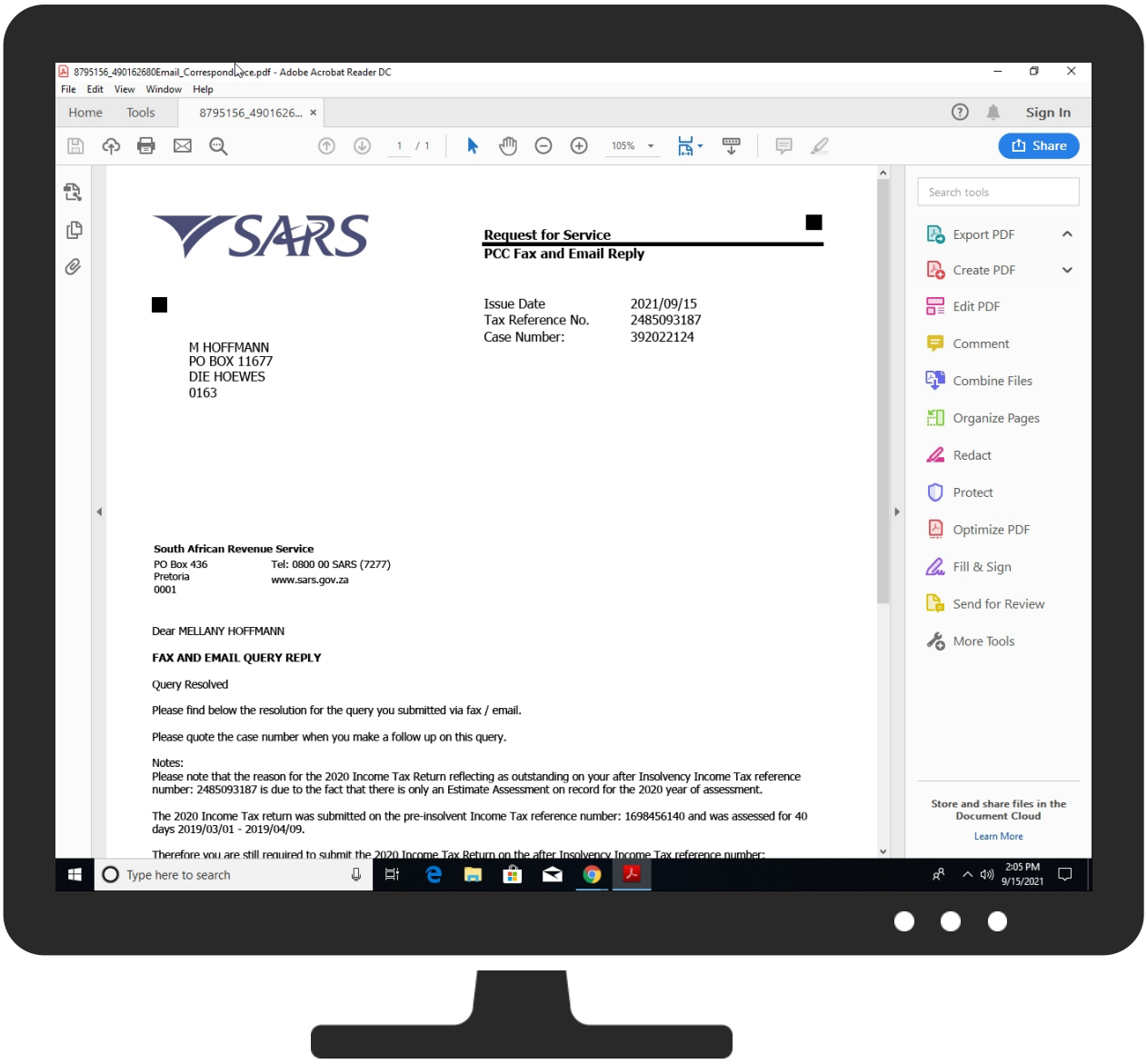
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/&	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/F	0%	Avira URL Cloud	safe	
http://www.sars.gov.za/forms/_	0%	Avira URL Cloud	safe	
http://www.xfa.org/schema/xfa-template/2.6/	0%	Virustotal		Browse
http://www.xfa.org/schema/xfa-template/2.6/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://ns.ado	0%	Avira URL Cloud	safe	
http://www.sars.gov.za/forms/	0%	Avira URL Cloud	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/8	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/X	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.xfa.org/schema/xfa-form/2.6/	0%	Avira URL Cloud	safe	
http://.....Acrobat	0%	Avira URL Cloud	safe	
http://www.xfa.org/schema/xfa-form/2.8/	0%	Avira URL Cloud	safe	
http://www.xfa.org/schema/xci/2.6/	0%	Avira URL Cloud	safe	
http://www.xfa.org/schema/xfa-data/1.0/ns#/	0%	Avira URL Cloud	safe	
http://www.xfa.org/schema/xfa-data/1.0/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483802
Start date:	15.09.2021
Start time:	14:03:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8795156_490162680Email_Correspondence.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winPDF@13/54@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

Simulations

Behavior and APIs

Time	Type	Description
14:05:44	API Interceptor	13x 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):	5.632200167803923
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QYqKdqi7Z+P41TK6tv8en9YOFLvEWdM9QAlri7Z+P41TK6t2:vDRM9GeZiEJxDRM9nQZiE
MD5:	6E1D86002F7A733FB4D6984504B43AC0

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
SHA1:	CD0EE4273D47FB6CEB2C3CDE909A3E1D1834E02E
SHA-256:	9D67B5AA9008C6B6D93B506CA84B964C05F8A18F0A7B029CE16035A785CB7CB0
SHA-512:	1DDD41FA2764CC3CC4D5520337A73F8E20F3113C3D1A2F44CB629C727E71D61DAFFE0F2F615A3E554F404C828EB5A197B5595CDE8922E7E356A29CBEA851E3 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .-.!Y.*/....."#.Dx...P.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... o.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..jKY.*/....."#.D.bo..P.A....d.{v.^.G...d.W.:...P..k%..A..Eo..... A..Eo.....f.....

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):	5.614451603773727
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkX1V8Be7Ywcr1TK6tfFl2i9NqEYOFLvEkP8Be7Ywcr1TK6tn8i9Q:V9zFV9PQpFll9zv9PQx9zVVz9PQZ
MD5:	67F5164EDA2E7820698C0EE48D596F45
SHA1:	E467E150854945CB32B07236AE22B07ABC476CA5
SHA-256:	E88D04237C6C715E0062B5879E3A8016C17EB42596C0E2589F2C1BFFA9A58DBB
SHA-512:	F4A288F86E7D2EF4EB69C72DD45DFC8F2E7C5143F6C7496679D83F78F67005E1872EDC6C594C4FD4EEF8B6F1F56FEBBBB8BD1BA9E55CD822949D72B9B0CC6 81
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....X.*/....."#.DP6...P.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....I.cT.....0\r..m.....,....._keyh ttps://rna-resource.acrobat.com/init.js ....X.*/....."#.DKv...P.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....0\r..m.....,....._keyhttps://rna-resource.acrobat.c om/init.js ..4Y.*/....."#.D.....P.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....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):	492
Entropy (8bit):	5.571813094426878
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFGflUo6jnyeRVFAFjVFAFxWWjYlUo6j:tB4v4GfSBJB4v4xDYSB
MD5:	D6C92009DA5F383ACEB0AAE97DC7A4F7
SHA1:	63E68E8DE11C7C19455B4CA75775CE967FB128B9
SHA-256:	66E9BBDF25456624AAFFB80780D9027E5924601C0F16630DA3F1573A76746041
SHA-512:	7BF58C6315D930EA0913F1FDD74B2544421198814D9ADD30EC2C89CE2EDFA5BD689C99CE2DE2425E1E65CBC2806E20428DE5AB80CBFC900B45BF313EE39E1 E7
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...!Y.*/....."#.D*....P.A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....&L.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-vie w/selector.js ...JY.*/....."#.D.cd..P.A..hvDO.N.t@.....n.*..... ....A..Eo.....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):	5.623627279463471
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rs+/9no2iWulHyA1TK6tYH:IbRkiDX/5oLWusse
MD5:	5E3C164E2E400B01F1D37275BCB9BF18
SHA1:	C427F23422BBA6FE8B9C59CA2840F7177870CF8B
SHA-256:	4D519EF67CC87433ADBE1B0EDF8DF644344536A24C205F37907F3A19133B7169
SHA-512:	19740527DD39EE07522C2D8D944C88767FC38C396B451E3E9656E34AB48CAE20AAE832C7632280083BF090793D1D9081EDCAF0E18DA1B3ED8C47A0581F1122A
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...(Y.*/....."#.D.<...P.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....tT.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5158169861620525
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu3WIPVyh9PT41TK6t:pyixRuVrPV41TE
MD5:	5A4359C1E52704D12A4B8125D6B6366D
SHA1:	5DBF2888606F35470AA4DD28BAD65076597F7B57
SHA-256:	FA5B64A037AAA21E462613580D46E7D06D27FECFA0D9C239968FDD1289450D3E
SHA-512:	81DA5236E3B5E962F0EB3E8FD614E0D8CD75C8E520B29CBD281019ACF57EF72BF854540BA84DEF754DBA348CBFA95868F816DE1E9C09A3990711789DAB2DAF AB
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .u.JY.*/....."#.D.e..P.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.634864353628472
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVKylbXyhco2sZI8xeGvP5m1TK5k4:mvYOFLvEWdhwjQmXyhLZII6P41TK6tC
MD5:	37607E180F394DABD026491367B706C3
SHA1:	9F1D75C376E4488A4F4EF3F4411A1912CA34F709
SHA-256:	D124C3E3481FD4DA51FBEE027ACEA27A1041C6887D5E792A6F8AFB73B2E3CF7B
SHA-512:	5D0CD06AB44AB77B0D427DB4A92EBA95F1E4190B284FA4C00BA033B2C503030E3CD40052101D9B9F5A3421BCC501D1233340DEC08FFFD52101EB9F898E33F7 7
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...FY.*/....."#.D}@L..P.A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....u.....

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):	5.530205619802781
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVCC2z4cyxMtv9EWm1TK5ktkH:mJYOFLvEWdGQRQOdQG2zM6g1TK6tk
MD5:	7A95B3CBB009454AFFC2A751E22D4E54
SHA1:	E143FB13908EA187D917BBA43974747399FB5CA7
SHA-256:	33B8BB7F295542F1B8D941F2D4403FA0A97734B08596901B482B2CCF86ACD815
SHA-512:	A61D100B319799B0960EF36122EF8E0BA6AE6DEB9F6ADD9183BCE4461A52148CF8724945B5D93A3CA225332B7CE3FD1C516F22D269A2F791D78BE10EC1CC3F 9
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..bKY.*/....."#.D.e..P.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo. .....dx.....

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):	5.599087539910196
Encrypted:	false
SSDEEP:	12:Z5MuADUMuR/Ey775M+MuR/EpJ5MyC6MuR/Ey:ZSuADNuR/E8SPuR/EHSy6uR/Ey
MD5:	8FFA789F75ED8C74986153B0394AB622
SHA1:	E4EAA0ED62DA0D1A1E513D8D7CE4EAF34A7F23F6
SHA-256:	F94AB27CE92A2684BB1979C91FFE8E06AFEA8150822D6ACB1363B9E7EF2ED392
SHA-512:	96BE36427BAB5CD3359EC22A79907F2648566B3B14A9D24ABE8B37C11D1D95CA536D964BD367F7AD0BBC46706832FD396013B3EB2B470388C4BCE34DBC7A8A 9
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .3..X.*/....."#.D....P.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....S.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....X.*/....."#.D|....P.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....I.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...4Y.*/....."#.D.r...P.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....yg.....

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):	5.519195876402145
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtumu+lzrXYby0zBUKSAA1TK6tR:pRhJoben
MD5:	E58BC2CA037A6BDF12E3697BF1902E1B
SHA1:	34825F81A34D5A6F3C8BA9C89B34256A9DB2BCB7
SHA-256:	BE15B2B1EFD243686823992D88703DFDA4562B197D9D1F56661D813E347C85C6
SHA-512:	FBAE772ECB30E8F52908279B40E7734F18B40D33BA638B27F5C1F4C572FB77A2C66A29717F364C3B22AE5D2BB17809BE9CAF8739981776D81C0B95BF3798CB7
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .1.KY.*/....."#.D} f..P.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....s4.....

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):	5.580555528684587
Encrypted:	false
SSDEEP:	12:KkXxKMSCvhAtUlHkXxKMSCv+ytUl3kXxKMSCvvEiytUlo:KkXxiCZAWHkXxiCmyW3kXxiCRyW
MD5:	41E87449E0D814FBA5BD09642729D0CE
SHA1:	C407BDA504AB5CD9B28A2526BBD08BC588A5820B
SHA-256:	32B1A9CD05B55477CF73683A77C67F3FF2F15B31E71A215D825BB1E80D911893
SHA-512:	915AAA857F87E385C6D5F1B33F0F9F710C6B3EC7012CADE94D7E0D2716D7E5AAAB3956AEAF5489F9DA592AC887E6CC23E091DA8D6406A9B3151A1339A4FB7BE9
Malicious:	false
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js .v..X.*/....."#.D*....P.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 .~..X.*/....."#.D.....P.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Y+.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...4Y.*/....."#.D.....P.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....F.".....

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):	5.56166743695437
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLw28qK/c8yM+VY1TK6tSkl9YOFLvEWsfOLKyM+VY1TK6t:5h6OLwZZ+k/h6OLHk
MD5:	3D214CF215142A2AB014B491EF3D274F
SHA1:	73AB67B6D425FCF787C448E0C722500F4BE7D632
SHA-256:	C9648AACF0FB5F23D5790007F9C9DBBA49873B527EB6B9D283CC03C72F0BBE6D
SHA-512:	EB01C4DEE9874A1600A3ACEEBBC7042B4695482D3948215D7E5C1D35BE58F7C4954C3CAC53693D82F91A180C2E114039630D620F950B0E0768DE711CEFBD834
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....Y.*/....."#.D.....P.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....z_.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...CY.*/....."#.D..;..P.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....R$.R.....

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):	5.626763687376397
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFA5XwSeKaTLnVRVFAFjVFAFUEP+wSeKaTLnf:UB4v4ApwzXLnVB4v4UE2wzXLn
MD5:	AE881DF5539568B9A52A86C8D5A734BD
SHA1:	8EED724FBABBE02E1410329265D581DF1B1CD9A4

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
SHA-256:	D59B37467ABF2B4D0CF95E60AA269EEC579EA8C22A470FE87C668FF5CA6F7B52
SHA-512:	C0BEA2102F004A5F24F12521203BA47FF34BD12AFF54F02006D139DD27809CD490586797DB847BA9320F6E48C54A5ABA4F865E4C2D094D62892485393DA82551
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 ..."Y.*/....."#.D....P.A.....H...{...2.. /.k`..r4.C. .A..Eo.....A..Eo.....l.....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 ..JY.*/....."#.Ds0m..P.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):	5.490460967401582
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXu8vEO11TK6tq:BsR2EselvEk
MD5:	1CBFA3309B58659BB286D9354068F787
SHA1:	67084A261C45B30D82F9F40A540588C062C11B54
SHA-256:	102DF91169678CDF770BF13617C61F5D4801959E7610017EE9E1B121E7EFBA03
SHA-512:	70E06294029B9D7E101FB62DDA440FDF388F244CE1356CE379533EA6A97009D1842F2F695C988B3938EA61AA2F1654248A66983342FBB53E0DA617715E21B42A
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..(JY.*/....."#.Dg.e..P.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo .....*.4h.....

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):	5.63796023651477
Encrypted:	false
SSDEEP:	3:m+lOy08RzYOCGLvHkWBGKuKjXKrAUWCKLuV1l6GXa+Z/7Ov9PPKMkvg4m1TK5ktn:maVYOFLvEWdwAPCQyzB7OhKlvA1TK6t
MD5:	DB35346E7D6E1F3E721520C7167F1CEC
SHA1:	F233BCA9057F2DCC2E7AA718E9AAD4B778E16028
SHA-256:	E45EC189CFA983A9D239ADBC90BD425D2FEFE3C6BB3122B0D0B6C3CF91AD1E93
SHA-512:	9E04A4F974873D517CCCB9C76AF1C6C9A7C9708CD50E813DCEADC560D17443957D95A7BB37B3D581721EF3A34BCA8E67FA3B80D78882BFF684753CA087D2AD A7
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...FY.*/....."#.D..K..P.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo..... .7.....

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):	5.5787639742534765
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu48/MA0QdFt1TK6tt:B2geRHRQz8/MN0v
MD5:	95979210AA22C64AF53EF0B09EBD487E
SHA1:	ACD7857448302AFD87F44BA3D2073A7A14EDAEEF
SHA-256:	96D396F1FAE3A4B2DB39438557E5DB280DC2D3EB2EBF2552CCEBF92A8E10A170
SHA-512:	92B8BCB7A0F249FF5B43953F5D4896EF515D772630054D6CF3AB4219E80BC26E3E60093813081944B84C17E8F2612D0EF0E52213776FDD01092E56C5D176709E
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...JY.*/....."#.D..d..P.A@..{o]...9o|..qY....T....{..u.b..A..Eo..... .....A..Eo.....h.....

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):	5.630575162617822
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
SSDEEP:	6:mzyEYOFLvEWdrIOQ5kTt1S/1TK6t7j2zyEYOFLvEWdrIOQWLaRt1S/1TK6t:WyeRl8kTt1wtmyeRluRt1w
MD5:	4C835D7ED76067066595C31A62B0E0DE
SHA1:	DBFC2BAB6F94F91CAF8F825886B40C4F7984174E
SHA-256:	9D2DEC5D2D9D138B02D2AAA2BE0F98B66EAF244671CC2355FF820E34A3DDEEBB
SHA-512:	3D197A84C0EB259AC57358EBA839735D9D23258B07D22AE1D89CC5E9E75C0BA87E3BE9A13D0C0B26AC52D898304F034C7DCDCA102E52ADA5AC26AA12808F8C8
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..r.Y.*/....."#.D.....P.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..gDY.*/....."#.D.VB..P.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....?u.....

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):	5.569023463055665
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyubCVK5QfqwK+41TK6tVD:wRhsKSwK+Eb
MD5:	6DA6436B18F2628F0B69966BD2C683BF
SHA1:	5C88EC8E608C493A1762EC0A2FB97546E798B900
SHA-256:	BC5E8B9AF31EA2CF88261FDAF8879FD799510B9726BA647859BDEBE0B3730CEF
SHA-512:	9634B84680B9968FC2084FD4C5CA8AD913C474B4CBF8A6F5B8D58019C8A136230EAF7AC87571A2209F007FE5DAD95D4E8D00A793620566296278CC6ECA25042
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...FY.*/....."#.D..K..P.A.....7...o..a=.98I.....(3.$G.A..Eo.....A..Eo.....W.....

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):	5.590176085661555
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbu359/ZAfO441TK6tp0MYXYOFLvEWdrROk/RJbutkqkbo6:/RrROk/45zAfLEX0VRrROk/RoYfLE
MD5:	4974BF472388DF190C35C6D1DD4371C9
SHA1:	D1437F8A105073FEB7FEC72D4343B4F5A1DF8573
SHA-256:	3658876DDCA5A192047800C5E1C18A7E21DE0514C460381D9AB6F9A1DB027B0B
SHA-512:	8ADC9FA4412FAB11EBD404A11A075E9FD88B1078CFD14BCC47390E6339400B4917652F6B1CED9A6D7F94E5DC26F402E035E1D22FBACE5F86A3F2D895AD8F06D
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .8o.Y.*/....."#.D....P.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....k.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..,DY.*/....."#.D_BB..P.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....QHN.....

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):	5.582481124688214
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIVeW2K1QPLr1TK6t2mDEYOFLvEWXIg1QPLr1TK6tR:xqTAhCPLnnqT7CPLn
MD5:	5E8EEF61EBFEECD21607802CBAF93D5D
SHA1:	A487E20CA55055D7CA7677D153000FB1FE57C2BE
SHA-256:	81F4B00A93245E7ADAB673CE71D300C2DFBAAD1AFB4C597546A5B2FF72145698
SHA-512:	B1487BE3266C146628616E181FE6E49D7CAF84E962688EA3E103CDEB72C704B38A2044AA49C5ECD247F6A9BCF964655D7EFA439D2C8993B628F9D59156655FA
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..p.Y.*/....."#.DB#...P.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo....._H:.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...CY.*/....."#.D..;..P.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....LY.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.607109789200285
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuGFo1OLsEJ41TK6tmM52YOFLvEWdMAuG/uy+wOLsEJ41TK6tj9:zRMsLsDIRM8/d+wOLsD
MD5:	08F88D5C3B37319BC23791824BFF2C4D
SHA1:	15BAA791960CBDD6DB3648AB1F543E8A43BCCA74
SHA-256:	6FB9114B36F0AFDF9658B779198503DB27C4280A5C67EDFE59377BFA189A9EAC
SHA-512:	23863A94DEFA7E77CA64415D4CEA3BDB4AECE9579BB76179C137B27A252ED63CFAB2444D80D85D3891877F6328D3E4E6309C6ECA8154822FCDE3D69C7B3059D
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .m@ Y.*/....."#.D/...P.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....[.d.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .._JY.*/....."#.D.Fe..P.A..z._a...'.v.....4p3..1.']...A..Eo.....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):	420
Entropy (8bit):	5.567381537981501
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuYs+Fong1TK6tueYilPYOFLvEWd8CAdAufPpaHFong1TK+:6lJRrFoMAClJRcPEHFoM
MD5:	08BCAF73D8AA8CDE8D079C60773B92D3
SHA1:	10B9A1FD679549D594B449700493C25FC4D009ED
SHA-256:	D524D68ADCED3AD2093E7C5474D085537354C7ACADAC6754671C492D9ACF31CD
SHA-512:	F3652ADCC177C790ABFA8FDD3C7C793E8D8CEFF2460CBE0AE0EB8D8FA66CBBC570E7D452F5CEBE7ED09BEB6207AF908A7E63AA1260D35AF7E5EABA8218D6C559
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .[F Y.*/....."#.D.s...P.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo....._m.....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..bJY.*/....."#.D.ae..P.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....,O.....

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):	5.622711762458552
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuAEKBZce16wG1TK6tVG9XMY8nYOFLvEWdrROk/Iu6uUceS:F8hRrROk/iZce2XG9X/8hRrROk/pe2
MD5:	14BBB5B5F9E24FD455940F340C56C707
SHA1:	8364053D636C2A2DD6AE2230D6D1DC33DF3B6B93
SHA-256:	03C68052ED79C15B2DDA99A9F4A16FF66440DDF5FCEA600EF026E16AFE79B9C4
SHA-512:	C8F8CEEB2B058DA93839A9887B2EDF6155AAB1EDA868881E2428FA5CC66A67976FB049F4D4BEC5E779B38ACAE620BB20AB2B097A54DC388EC79FE4F1C4A71E27
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...Y.*/....."#.D.....P.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...CY.*/....."#.Df3B..P.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....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):	426
Entropy (8bit):	5.689061162859286
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQgXrNJIi1TK6ttLrnYOFLvEWdrIoJUQY3yRrNJIi1TK6t:ehRcLXrNJICfhRcB3YrNJIC
MD5:	4497C83A014AC57DD6FBFF43ECA23D24
SHA1:	968B8B380C0CDC255841D5926EDBDFDFE0B7245A
SHA-256:	C6C6FBAACE16EA60B4604A10DD707EDB1D7C1B803774479B170BF82369317874
SHA-512:	B9F62D3F3DB3305864E97A026A60A6026F88F3DEFDD0A22A915997CED18D3E52A0DD0DD6E706501727E4CDCC95A2902F036A8CB70E6410D1C70FC602F7D1A68
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 ..x.Y.*/....."#.D....P.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 . .DY.*/....."#.D.~B..P.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....a.....

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):	5.5730104224195
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhu3Ry/E6UWhhLzgm2d/1TK6tGh/EOEYOFLvEWdrIhu2ylir45h4:0RNRhVwReQhSRwwRe
MD5:	20784B0F65C8B20882A5BEB4EF4157BE
SHA1:	97AC55B57356C1BF6B67DFE628F713CD1D8DF224
SHA-256:	54D74515B8C7C0C5645F035094C36D51E87DE2D21ACFD210B26C4CC7125D853F
SHA-512:	AD42B94C81C80834CC313200FB515F73327DD5CE75FE18B505902A5230B31E235F5D4B74D46E9C2772D29EC28FD8B48CED7B8EA9C9EB612E910FE0C9888F847
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....Y.*/....."#.D._...P.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 ...CY.*/....."#.Df.A..P.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....e.....

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):	5.662019108593247
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KpDgUhkx56uvp1TK6theAElVYOFLvEW1Kv65GOkx56uvp1TK6tX:6JJKpDg3yJJKiKMJJKJUY
MD5:	3084EBAC6615F43586D310C9699FBC59
SHA1:	14C7D52CDA7EFFC4E162443982F2794B3A2440DE
SHA-256:	2F331D58D5ED5DCED135FB6FC0CEA4183B521280F909B3DD1DDFB0061A4FD0E0
SHA-512:	175FA5FE4A3B86FDE183D3F19162109A54F4A76A8607D4E5FE553A9A0F376451730BAB6374A717149F41A24CC71AD7A00FE943194B9EC5B7B2416A87B9D6313B
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....X.*/....."#.D.....P.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....".....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....X.*/....."#.D5....P.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..?8Y.*/....."#.D.-...P.Az?...SwC...^..y.....V..7R-O.....A..Eo.....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):	5.6157166555211795
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuNE6gjyhUDLYtmOZn1TK6t1OH:xRBJFLDDcFZLm
MD5:	A8B586FD35465C1EFC5561E14B8912B2
SHA1:	62192B5E50A6499FE2E8D66972AD85FE8FA7525D
SHA-256:	5B6583636357E91F44A0AF758C19900814B35F0BE00E3CA34D7CC938EE8BEFD3
SHA-512:	3EEDE2031C6C7EAF9643FEEB4713417D9BB3E7538F718B69A5C69FE6D7C2664009838A50423ABF3EACE5B5C1A0B9093C16B8C2019988B58660D4436235869B68
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..\JY.*/....."#.D.(e..P.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....L.....

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):	5.647406235864043
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7jZ2j9x7VPu1TK6tnP/EsRPYOFLvEWIa7zp7nkVPu1TK6tSL:BPHzK3cx/TPHxkcyPHxi3cl
MD5:	58919786C14177599661FC853A1C0B8C
SHA1:	9E112C8D2D37BD57321D4C7A2819BEC94A66F09A

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
SHA-256:	F2D9D7FA185BB471B02CC0E93C3D079A3644F051E57C1986287F3F82002129AC
SHA-512:	0827307A4E965F4ADE9F56CB8C6030DFD76D770923B407EE10D5DD35DC3D7ADDB3A2F9444ECB446B21A60307D945E158166269271D825D4C276CCF3E4EBBF41
Malicious:	false
Preview:	0\r..m.....S...{.j...._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....X.*/....."#.Dn....P.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 .1..X.*/....."#.Dx...P.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 ...4Y.*/....."#.D.....P.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):	5.563960851854799
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QuVUXgNiM3Y1TK6tW9:bJRT9qsr0E9
MD5:	6A5AD39C831C62B20DEB2BF5A5700AF1
SHA1:	4365C7D0DE35F662E55373E505D07BCE5072F56C
SHA-256:	A1FFA380C48CF7D0517AADBF0EF6ECB230DB5062F51FF8541424BFA570C82648
SHA-512:	4FB102029A56E060590A4CE33BF819E4C619D294F96DCC08753860C48156ED7F86D3968DEA5A798389D5DA61A189550479ED029EF6F9EF8DEB2A2CAA91D1FC3
Malicious:	false
Preview:	0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...FY.*/....."#.D..O..P.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo....._.Y.....

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:	modified
Size (bytes):	208
Entropy (8bit):	5.556578128040905
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ7flNQjBRCh/41TK6tK:XRc9bDi/E
MD5:	9C78C7DEF755C0BFF6D33A0C45125DEE
SHA1:	F31535749417ED441433E51484F92087E2E68A71
SHA-256:	4BC2DCAEE03E5DD5103AB14E3E28F741771789C0EE4CE245C80D41B4404166DC
SHA-512:	187E5D338102E911A538DF651D4CA61485BC46DED22E1BD5AA6108F0478D4E4B6924F0A3968DBCEC2998B43294F670F38B92E104A91FE11AFE6E2B3C5A79BED
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .P_KY.*/....."#.D.#r..P.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....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):	5.559487569468152
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuvtzULlF4r1TK6t:bs6xRkipaLlF4n
MD5:	CD1B8357F473652A4178283A5A7DDFCF
SHA1:	74487EAE347D230E05CD716712DCF905626590FC
SHA-256:	10CA69663AE712C239970829838E15C72FD505FE6970A8108094507793F3C2BA
SHA-512:	F1F8E5FACE60A86A0358E6D6B190B857653679B6FEEA055194231A17D222304EAFF0AABC1C072E8E2F4A6B234D7EA30164876E0CDFE54BC39FC30F4FACBA7CFA
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .%..Y.*/....."#.D.C...P.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....L.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Entropy (8bit):	5.484446086540566
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvXp8ZMXIrcu1isLK5m1TK5kt+5/:mhYOFLvEWd/aFuj8ZMX/941TK6t
MD5:	B0ADAADBFC713426ABB015F146E43BFC
SHA1:	40EFCA64335561553C6234634C8AF4346E93C18A
SHA-256:	4084D70C2139035390B49B4B283A2B31DBAFD2B64E97ABFA3573AC27306F1D9D
SHA-512:	1404AA375FE9F2FE80EF230CFF494CE6BB855529283D47A6368F4345E83A50CE0A66954E06125B49B4F487F5A88664740FE77D5E9F57545D3F27BE9E10037E33
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .~.LY.*/....."#.D.3f..P.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....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):	5.533384126243726
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQUAP+l5wmBoBMqVd3G4K41TK6t:2DRuRikwpB9Vd2k
MD5:	3D5ECCFA12C785EC6BA8F01E0E82AC88
SHA1:	B4997997273A3989CDA79A50E694ECCD7F429DBD
SHA-256:	B073C64F602B3DD8B40FDA5F0C7B070E03CF864426F3025F259AB5F57EEC0FAE
SHA-512:	14E6877FFFBEE1DE8D129516EC8226B80E2CC948A35FC5A204D2386D3440A6E51DA221ECBBB8EBF0A6BD16986135DCC5A56942A226981D5E1E37BD61410C71A
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ._.KY.*/....."#.D).e..P.A..y.$..$.v5j...T...z.]..._S....A..Eo.....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):	416
Entropy (8bit):	5.585806364028061
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QPAuA424r1TK6tFkqYOFLvEWd8CAd9QmBtuA424r1TK6tL:+RQYLrnbRQRcrn9
MD5:	31A8DC89520045154FB04C9803B9E9E8
SHA1:	BA2E29A6C04FFE9F155DEE5250D25111BCBFB0AF
SHA-256:	3EE8ECEBD1F6051B9BF10F1FC79573B33C5DD49F2B2CD859D71320C63331C51A
SHA-512:	BEF99036CAE135730C01B91A7BD7228E8130706CD6E49763EDED736FACED85AF14F385BD454FF7F439D6845A0C66C047D3DAF96E16F01B8DF6E8706DD363C27
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .K.!Y.*/....."#.D.....P.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 .~.KY.*/....."#.D.#t..P.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....K..5.....

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):	5.561286413101437
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAu0lAyC8n1TK6tE//:xhRTqu7QS/
MD5:	D33F818DA456840F5FC00533B3801BCA
SHA1:	40C1569B7271157B7CFB8FC6CD807050257AF7E3
SHA-256:	E8BD5A4FC6D32EDC1A6A0ABF159040EF009B0AB08BE72D33DF4B9D2D18FD03A6
SHA-512:	D3DDF4EED057AA6044ACD1567B16C3C8A31EBC9038F824212C1D7EF944252C860BA35BEFF4367FCD980CF76506E0472FCAD1F44EFDDED40F99BF833E2D79DC8
Malicious:	false
Preview:	0\r..m.....R..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...FY.*/....."#.Db.K..P.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):	5.656796901572202
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQGxDLmB41TK6tm/MQZYOFLvEWdrROk/VQDhLzLmB41TK6t5:nRrROk/Vjx+mY/lRrROk/VALumX
MD5:	2EC300B2AD6692B7823CCC6A4C086305
SHA1:	C9A9AE9FCB5CBDC6CCD1CDE60428DF184C932DFC
SHA-256:	C19B0EA72C580D583A5FB5358AF0DC5FCD542E7D2F82223FA6857FC05A0EEEA0
SHA-512:	E0EBDEE5EE1040828FA7D23B5475EAC1F0022D9128128AC44362DF916F978629A080840D8CD85AAE6BC4095314348E0999F1CB790DAD1313D32BEB2689A7DA7
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..{.Y.*/....."#.D.....P.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo...../.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...DY.*/....."#.D..B..P.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....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/lXYOFLvEWdccAWusvEk3woAdm9741TK6t+l:qxRcCcEAdu7Ekl
MD5:	1CA2A89CC914A749519CDEB13F3E90CF
SHA1:	168D9051EC84C7B02E1CD0815871A337E314FD4B
SHA-256:	EDDAEB2B67C1D638CE9494AC8F643052CCB79A34C57F0187FE02EA944026AD79
SHA-512:	768F97CC798303F7C2FF2BB87D58A4A87833F01EE10A448C020D26EACE937FBC8FAAAA37CCB210C23780CBD9BCDCA07840903371074D3B2542CC41C1C1CDC52
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...JY.*/....."#.DG.d..P.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):	5.541318607795365
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvL5APFOB6shoq+Nem1TK5ktKXF:mMOYOFLvEWdwAPVunAPFrJn1TK6ty
MD5:	5BD3D78E7A02514410CC22933AB599AC
SHA1:	66C46E1BE79126AEF201D010358570830E69A82E
SHA-256:	529FC945FDFE7D304D74D3B898AC8DC36C86207549A49E5F400F0F76AD08E48B
SHA-512:	78DD198AC81F8399E90C65D6C81CFA158968D075FABDAD0139C662ACEF08C725F946B610662A9332819E1AC64F69D760033B5B905A9273E6ECA400711FAEE15
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .G.EY.*/....."#.Dl.K..P.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....h.....

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):	5.664042270149457
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQtLGSzhcsBXIh1TK6tS:mxRBJQ7SDB0M
MD5:	DE872B8495CE2A814F5DFAA8EBCF68CC
SHA1:	B8ED59AA49CEA7B56C0A994E831AA501ED5B3E1E
SHA-256:	0D3E6DD387FF371E49AD89D2AAAAF4C56085F806644CAD53BC81F8369BB79CA4
SHA-512:	6B6C24A8046CA98B7423D4684A2D9320E6EBF292D3DC8313975362C1D985CE3FAB5A13E5A7E0CF3C2DE4A7AC8F1A6806F793B5266B5E0B02B9EB5CBE14FC743
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .'fKY.*/....."#.D.Xf..P.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....>.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.639486773852637
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQN8jmcHc3Me/1TK6tR2sPYOFLvEWdrROk/RJUQe8BwPHG:3RrROk/sA8vcLHRrROk/svowvc9
MD5:	51ADCB44242ED85598E855F74443F67E
SHA1:	310856E04DF917857A47A1EB2794D7E4FF78833B
SHA-256:	E40DECEC0ADAA984022649E1A19C7C58D676A90A809C04D8B68CBF238545711E
SHA-512:	4EC0B3CE60B74A22B7E8EE2B05552CB54D0896CBCAB3E45A6421F950E554614E767708AEF208ACC4DA33F71DEF1A0C0398D388C6B68FF15A894AE1172D24BEFD
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....Y.*/....."#.D`....P.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....^U.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...DY.*/....."#.D..B..P.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....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):	2016
Entropy (8bit):	5.171545917276375
Encrypted:	false
SSDEEP:	24:0I2bYdB8J6MbkeljKqRomcT1p1BQwHMrVwhIDEX0O4Aw6:t2kdhMkCqm81p0wHM4X0Ohp
MD5:	267310602D3E672C77161AE5CE186774
SHA1:	BA078DBA8F2F63C21615A3AA8BF48098B5D4C636
SHA-256:	D8B3A83C1E838D9C6634AD81B428355F1CF8D54B51CF9C5649BFCC0716AE3434
SHA-512:	0C51629CEEF974238537E0C8DF75D095882CA4BA2C395E451D5634C470AF94B9FF14A14C3A180DAA5F23DF78DC513E69FFF0043F9A9B31DF6E3AB16FA1DA40F6
Malicious:	false
Preview:	.....goy retne....'.....'.....;.y~A.@.....*..@.....oB*.....#...(@.....k7A.@.....D.4.@.....[.i..%.@.....<...W..J..... ..,+..._.#@.....J..j...@.....6<|.....A?.2:..@.....+.{..'@.....*)....J:@.....2q....@.....P....V@.....+.U.!..V@.....P[. q@... .....!...0.o@.....u\]..q@.....@.....*....@.....o..k..@.....^.~..z.@.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@.... .....v...q..@.....C..M..@.....a.....~.,.4>.@.....&.S....@.....@..x.@.....=....m..@.....;/...@.....q.@.....MV3..@. .....:..N.A..@.....Z.....(oy retne

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):	2016
Entropy (8bit):	5.171545917276375
Encrypted:	false
SSDEEP:	24:0I2bYdB8J6MbkeljKqRomcT1p1BQwHMrVwhIDEX0O4Aw6:t2kdhMkCqm81p0wHM4X0Ohp
MD5:	267310602D3E672C77161AE5CE186774
SHA1:	BA078DBA8F2F63C21615A3AA8BF48098B5D4C636
SHA-256:	D8B3A83C1E838D9C6634AD81B428355F1CF8D54B51CF9C5649BFCC0716AE3434
SHA-512:	0C51629CEEF974238537E0C8DF75D095882CA4BA2C395E451D5634C470AF94B9FF14A14C3A180DAA5F23DF78DC513E69FFF0043F9A9B31DF6E3AB16FA1DA40F6
Malicious:	false
Preview:	.....goy retne....'.....'.....;.y~A.@.....*..@.....oB*.....#...(@.....k7A.@.....D.4.@.....[.i..%.@.....<...W..J..... ..,+..._.#@.....J..j...@.....6<|.....A?.2:..@.....+.{..'@.....*)....J:@.....2q....@.....P....V@.....+.U.!..V@.....P[. q@... .....!...0.o@.....u\]..q@.....@.....*....@.....o..k..@.....^.~..z.@.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@.... .....v...q..@.....C..M..@.....a.....~.,.4>.@.....&.S....@.....@..x.@.....=....m..@.....;/...@.....q.@.....MV3..@. .....:..N.A..@.....Z.....(oy retne

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):	294

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Entropy (8bit):	5.168644746856875
Encrypted:	false
SSDEEP:	6:mpIUJhN9+q2P92nKuAl9OmbnIFUtpyIUpkN2WZmwPyIUpkN9VkwO92nKuAl9Omb5:CIUJ79+v4HAahFUtpyIUpkNJ/PyIUpkW
MD5:	78667E13EC98F2D3F3F385686FFD6A68
SHA1:	5972359AC6596A194E0D5BE1AF638E19EED21983
SHA-256:	FE5E66D93DA4608F0310FAAB5C2B8CE7B9CEB7E6BEF352E7C04DB1BED9B8BBB5
SHA-512:	DB4770E51F7B84965A154AB4F70AE17E11371C9B530365373AA144FE30137D2F6114B4FDBA6ADC0E4DB4CA3F3922D1C7AD2805006776E7383F187BFAD68E7E3A
Malicious:	false
Preview:	2021/09/15-14:05:51.469 150c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/09/15-14:05:51.471 150c Recovering log #3.2021/09/15-14:05:51.471 150c 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):	294
Entropy (8bit):	5.168644746856875
Encrypted:	false
SSDEEP:	6:mpIUJhN9+q2P92nKuAl9OmbnIFUtpyIUpkN2WZmwPyIUpkN9VkwO92nKuAl9Omb5:CIUJ79+v4HAahFUtpyIUpkNJ/PyIUpkW
MD5:	78667E13EC98F2D3F3F385686FFD6A68
SHA1:	5972359AC6596A194E0D5BE1AF638E19EED21983
SHA-256:	FE5E66D93DA4608F0310FAAB5C2B8CE7B9CEB7E6BEF352E7C04DB1BED9B8BBB5
SHA-512:	DB4770E51F7B84965A154AB4F70AE17E11371C9B530365373AA144FE30137D2F6114B4FDBA6ADC0E4DB4CA3F3922D1C7AD2805006776E7383F187BFAD68E7E3A
Malicious:	false
Preview:	2021/09/15-14:05:51.469 150c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/09/15-14:05:51.471 150c Recovering log #3.2021/09/15-14:05:51.471 150c 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):	0.007909552735237937
Encrypted:	false
SSDEEP:	12:I+1rDro+1rDro+1rDrolfrgrocrgAmJocrgAmJocrgAmJ:T13rz13rz13r+fUrjUVJjUVJjUVJ
MD5:	28C3F901AA5AC270CCAB75AA191F3258
SHA1:	5D399FD68F093714478F4E722E6432F2F242EC89
SHA-256:	7C8E9508FC031C0B9B0EF7AA2AC874A1C14DE506A9AA035917F03E6CA1D3480D
SHA-512:	FE180F9F8D19E668F38B787F02BA2E6871EB3B9D90BD1CB9AAC9FFBCECD2EEB1F21EE16C422994B096BE8AEAF8E05CDB4653B9DD023B9DAA8C7C870706E1E925
Malicious:	false
Preview:	VLnk.....?.....+.}.^1..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2109152229462-40327686.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.407828856807533
Encrypted:	false
SSDEEP:	768:5/d8B0zRPeRlnXKAECrxoUZhdVLrZCwarQKsKoFef9Eyiq5hLFGgSOrcrn3H:A
MD5:	5AF1248C364B5E5A7C5CCA2456F525D4
SHA1:	5AB48975345257E4C19354DD8E5CF6983DA8163C
SHA-256:	6F1C5DC0829DFC095039477308B637A595247D05D2AED39B2CB73EB857844F8C
SHA-512:	86F41AB8AC989D96A4EFF96F9782A2523D27CD8E4B4FC2DEA5DE40A3D6C7B8DC5CADCE14BE608AFB84CC22CCD510EA1596294B923606027EB984C45C3B7878F
Malicious:	false
Preview:	BMV.....6...(...k...h.... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.386152000167289
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQD9OhFVCsL49IVXEBodRBkR0aD9OhAVCs749IVXEBodRBkl0aN:iGedRBfnedRBzmiedRBnmjZedRBdmx6s
MD5:	47D0C8FD68FC391882B01FF51DE3D655
SHA1:	09836FA75AAD6CE03EA1A72BAEBCDDF1711E7788
SHA-256:	195B16DEAEE0721CA2EE7DD99727D7B19971C6C1199B7304D44B791EB79D1B4A
SHA-512:	D920FC8857C78742CA04C211E36FBEBE3550E6AC139041FC8A20233A88C112E1E254978CD8C54E89C5B0E847FD9C84FD3598CC31F8689A7481C5C03C4BD9584
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):	3.199091260158504
Encrypted:	false
SSDEEP:	192:GRiedRBwoLGedRB9mpCedRB+mjMfyedRBk:SieXLGeyCekfyeS
MD5:	3155D282C551364330A2E1AF6641472B
SHA1:	21CEFF89835F3129A5F300C960D0737F67DBB9A6
SHA-256:	3FD705C1696B9DA8339DF6BD1E9211684E379E05DEB5704B11B069CB1551F197
SHA-512:	AEF8E45F288C6E65898B33377D971D7D79DCB50BB70276473DA2AC4E72D23240F48E522DE3E22C04C900C28F928F053928B0A7463C7EF76E3285BB6131410E05
Malicious:	false
Preview:	.....B..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6472	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

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

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

SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZTqivLdmtOk32PDrvJILHr+Yyu:J0GpiyVFiBWivLdmgFvS7SK
MD5:	16AD42956974EDDF54B46D46A4842389
SHA1:	14B8B2766B03C75ECC2E7E23486A9C3DE79B70A7
SHA-256:	676E321304B578ACF0B13EC195513DD13082BD5D05DFDD93E472A192B9C0794C
SHA-512:	216FB8EC7B9C054C5DA4C46037D471BDF625E507AF6F86F594626F87486CBE7B7A1279A6F5179EB11BDD04848E7B87A5EADFB264810DA761A934A17C1C0E807
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1vhrw39_3n1fzc_4zs.tmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PDF document, version 1.6
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.066365181476659
Encrypted:	false
SSDEEP:	6:IngVMrexJzJT0y9VEQIFVmb/eu2g/86S1kxROO/HpOvAnMpOvYLCSyAAO:IngVMre9T0HQIDmy9g06JXgKQlX
MD5:	134E3453FE72599B85F7552E884C266E
SHA1:	CBD14D65B0D7A105445135AE406B36BFF6AFB17C
SHA-256:	108D90C9B8A4FDAE00D927D69B84CCA7363C8324979D68E5367529FE01B2850C
SHA-512:	E1DC52E80431DBD59224E8012A623C24CB66D2E4A4DED955A0807C987C79D940FA836DD001DFCB0F14426182421CF96217D3F73E4A0D229FB88D9F8DCC45EF
Malicious:	false
Preview:	%PDF-1.6.%.....1 0 obj.<</Pages 2 0 R/Type/Catalog>>.endobj.2 0 obj.<</Count 0/Kids[]/Type/Pages>>.endobj.3 0 obj.<<>>.endobj.xref..0 4..0000000000 65535 f..0000000016 00000 n..0000000061 00000 n..0000000107 00000 n..trailer..<</Size 4/Root 1 0 R/Info 3 0 R/ID[<BE04D718A12F1E4B89DBFD13F7913388><BE04D718A12F1E4B89DBFD13F7913388>]>>..startxref..127..%%EOF..

C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rgq07pf_3n1fzb_4zs.tmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PDF document, version 1.6
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.070865308982934
Encrypted:	false
SSDEEP:	6:IngVMrexJzJT0y9VEQIFVmb/eu2g/86S1kxROOavA2V/vA2VzCSyAAO:IngVMre9T0HQIDmy9g06JXKZ/ZzlX
MD5:	B01477BD1F7F217A620BA15AEB121365
SHA1:	6A1A8F97C88739155879B82BF215DA2BA2FE05FE
SHA-256:	1C484250E029237C7DE297E2350EA9994114FE19DE89A3CF780ED0AD9877FA97
SHA-512:	1012E785C090B9380F9B508E0ABE8D7C0566C5365B72357007353D5BCAADF84AA41FBC12ECBC462A5781604EC78A9084DFDB2974B3629D23898676090C1D2BF
Malicious:	false
Preview:	%PDF-1.6.%.....1 0 obj.<</Pages 2 0 R/Type/Catalog>>.endobj.2 0 obj.<</Count 0/Kids[]/Type/Pages>>.endobj.3 0 obj.<<>>.endobj.xref..0 4..0000000000 65535 f..0000000016 00000 n..0000000061 00000 n..0000000107 00000 n..trailer..<</Size 4/Root 1 0 R/Info 3 0 R/ID[<BBF5DE1D9D961E45A3B28CDD4D7B7104><BBF5DE1D9D961E45A3B28CDD4D7B7104>]>>..startxref..127..%%EOF..

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):	40
Entropy (8bit):	5.053055907333276
Encrypted:	false
SSDEEP:	3:Nl834Ustk6al8H:Mjs3al8H
MD5:	6F38F14E77DF75FA9F80D6992EBA2696
SHA1:	2BA35DD62CFED5B2296FABFA2217CB8DD48EA077
SHA-256:	32C72D5DA9604B3FF32313FD668569C8C0E3A322455250F2CC42902311D22CA7
SHA-512:	5E9A547F10E3D6B556AB7DD3D1293BDEC6C65BB7DFBCE0C5395160CF763FFB134040684F2274FD543355682E08E23AA7147B6AF8D1AEA89C819D28B255FCF971
Malicious:	false
Preview:	.../B..c....9.(h ..-b.;-Xik.}...mS.....

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):	664
Entropy (8bit):	7.6258222001196865
Encrypted:	false
SSDEEP:	12:2JQkEmqC+vdlxWiPp/8G44Fg8FN9ZkGaPK8oxrjWr4V/QdoiPPegNr81OvA8Qyq:BkP6lx3RU38FhxvWrgQdogPegNo4vAnl
MD5:	B599DD635EAE66871D72628C338FFD2E
SHA1:	1BE4576BC60D3B71D13D168D5114F055B857AD96
SHA-256:	EF6D091DD5EA8E09D10D5D03586E4CC14E4A1714C2EBA04C5D32720BB7BA2B69
SHA-512:	76F03F5AB089DFF92DA0008208D401203D46B2FBE6D680BB3424D5BD8B2B79057058C89AF83F30D0DE4FB9143BEEBD2703EF93128B0A27C57BC14EB05F7236EC
Malicious:	false
Preview:	.....l.jy.v...@K....)G..;S.G\....j.@.,B.L2._..\8A...L.Zx$C.^.........-<..g.N.e.y.....O{.V.]\|B..T3Fr.8...YT......Z#..i...e...9.=..."Cf.pq....z....jl.2...Hu".3Ki.`4..e.....k..r.....5_....*.2F.......0Vt.. ...t7_...a`M..".. i.../.$..pn...W"..G...].H.N?z........../...o....Y...g.;...t.w. ...\..z.;R.[.&l*.b.3.)#F`.!FJ<...".{....uT..wo....t.f.y.,.G...#..&.NSWN0.o..(...H..+...7r.q.-.U..H@.....{K.~.....W. B...,E%...Fu.B..](\.y..J8t<=.].]......X....q/.l..,..k.....Q.....1..y....r.5.j.N.nZ...'|JG.S.bH.(.N...L5.iA.rJ$.]....".A.%.;u..u.#.....V....D'..w..#..D.....Bw...o1..$.,n...9$..$r.9.Y.....@Y.+..**l.|.. #nv....P..T.sP...Ka..j0,..L

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.8043094152554815
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	8795156_490162680Email_Correspondence.pdf
File size:	97361
MD5:	20da3e9fb6519f8ec141e8aa156c0aaf
SHA1:	1d064b479bb9c3561cc80e64fee9c37a43460bf1
SHA256:	65492564da5ba6456e2e2a7f6b91946945833ac33d8334193993b751fd8b5e6a
SHA512:	7fa04f85df3b5731ae290d66e56708872a0fb6e74955cb95d705d480bfbd4e0b062d7962d4a9039828e9bffb0c785c122653c0336f85575069871e428644e1ee
SSDEEP:	1536:+Aw5u1yqsFILzfHgFj2GGVQRiVNGeRgfbDyAgivxWSV/ofzkpXezFDo:+NXqsFOfRGOQaNXR+bGRivxJofY8zS
File Content Preview:	%PDF-1.7.%.....23 0 obj.<</Linearized 1/L 84178/O 28/E 3197/N 1/T 83928/H [440 154]>>.endobj. ..31 0 obj.<</Length 57/Root 24 0 R/ID[<428A600F4E39704C99CC6694B9F44B5D><FD83494961FE9149B503A10F0205E8AF>]/Info 22 0 R/Filter/FlateDecode/W

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.804309
Total Bytes:	97361
Stream Entropy:	7.939620
Stream Bytes:	83979
Entropy outside Streams:	0.000000
Bytes outside Streams:	13382
Number of EOF found:	3
Bytes after EOF:	

Keywords Statistics

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 6380 Parent PID: 4896

General

Start time:	14:04:41
Start date:	15/09/2021
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\8795156_490162680Email_Correspondence.pdf'
Imagebase:	0x10000
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: 6472 Parent PID: 6380

General

Start time:	14:04:42
Start date:	15/09/2021
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\8795156_490162680Email_Correspondence.pdf'
Imagebase:	0x10000
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: 6520 Parent PID: 6380

General

Start time:	14:05:43
Start date:	15/09/2021
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:	0x1180000
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: 5344 Parent PID: 6520

General

Start time:	14:05:46
Start date:	15/09/2021
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=1692,4973472669529672 6,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12528180285023581782 --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=12528180285023581782 --renderer-client-id=2 --mojo-platform-channel-handle=1724 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1180000
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: 5132 Parent PID: 6520

General

Start time:	14:05:48
Start date:	15/09/2021
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=1692,4973472669529672 6,14708380478045234943,131072 --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 =KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAA EAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAA AAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAA AAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=13295799185429258 37 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x1180000
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: 6772 Parent PID: 6520

General

Start time:	14:05:51
Start date:	15/09/2021

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=1692,4973472669529672,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14045389042154872069 --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=14045389042154872069 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1180000
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: 1972 Parent PID: 6520

General

Start time:	14:05:53
Start date:	15/09/2021
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=1692,4973472669529672,14708380478045234943,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=8578766355593294049 --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=8578766355593294049 --renderer-client-id=5 --mojo-platform-channel-handle=2112 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1180000
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