ID: 534007
Sample Name:
akos_bardoczi_cv_eng.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 23:52:12
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report akos_bardoczi_cv_eng.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Sigma Overview 5
Jbx Signature Overview 5
System Summary: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
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 24
General 24
Keywords Statistics 24
Image Streams 24
Network Behavior 25
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: AcroRd32.exe PID: 7116 Parent PID: 5480 25
General 25
File Activities 26
File Created 26
Registry Activities 26
Key Created 26
Key Value Created 26
Analysis Process: AcroRd32.exe PID: 5496 Parent PID: 7116 26
General 26
File Activities 26
Registry Activities 26
Analysis Process: RdrCEF.exe PID: 7004 Parent PID: 7116 26
General 26
File Activities 26
File Read 26
Analysis Process: RdrCEF.exe PID: 7140 Parent PID: 7004 27
General 27
File Activities 27
Analysis Process: RdrCEF.exe PID: 6268 Parent PID: 7004 27
General 27
File Activities 27
Analysis Process: RdrCEF.exe PID: 2408 Parent PID: 7004 27
General 27
File Activities 28
Analysis Process: RdrCEF.exe PID: 6912 Parent PID: 7004 28

General 28
File Activities 28
Analysis Process: RdrCEF.exe PID: 6300 Parent PID: 7004 28
General 28
File Activities 29
Disassembly 29
Code Analysis 29

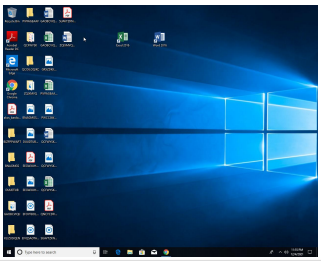
Windows Analysis Report akos_bardoczi_cv_eng.pdf

Overview

General Information

Sample Name:	akos_bardoczi_cv_eng.pdf
Analysis ID:	534007
MD5:	61155ce562820a..
SHA1:	c2267b76c0c9e9…
SHA256:	7cf78d07e0a83b8.
Infos:	

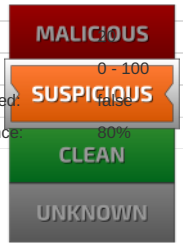
Most interesting Screenshot:



Errors

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

Detection

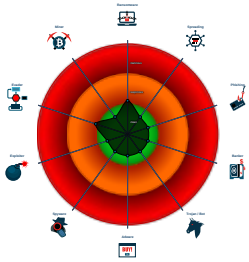


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Potential malicious clickable URLs f…

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 7116 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\akos_bardoczi_cv_eng.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5496 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\akos_bardoczi_cv_eng.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 7004 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 7140 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=1568,12052173175988817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6127630510957074088 --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=6127630510957074088 --renderer-client-id=2 --mojo-platform-channel-handle=1696 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6268 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1568,12052173175988817585,11176571729766905782,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=585970285045658890 --mojo-platform-channel-handle=1708 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 2408 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=1568,12052173175988817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6328359103851257533 --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=6328359103851257533 --renderer-client-id=4 --mojo-platform-channel-handle=1940 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6912 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=1568,12052173175988817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17081285814894932504 --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=17081285814894932504 --renderer-client-id=5 --mojo-platform-channel-handle=2008 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6300 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=1568,12052173175988817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3781967090892827746 --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=3781967090892827746 --renderer-client-id=6 --mojo-platform-channel-handle=1932 --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

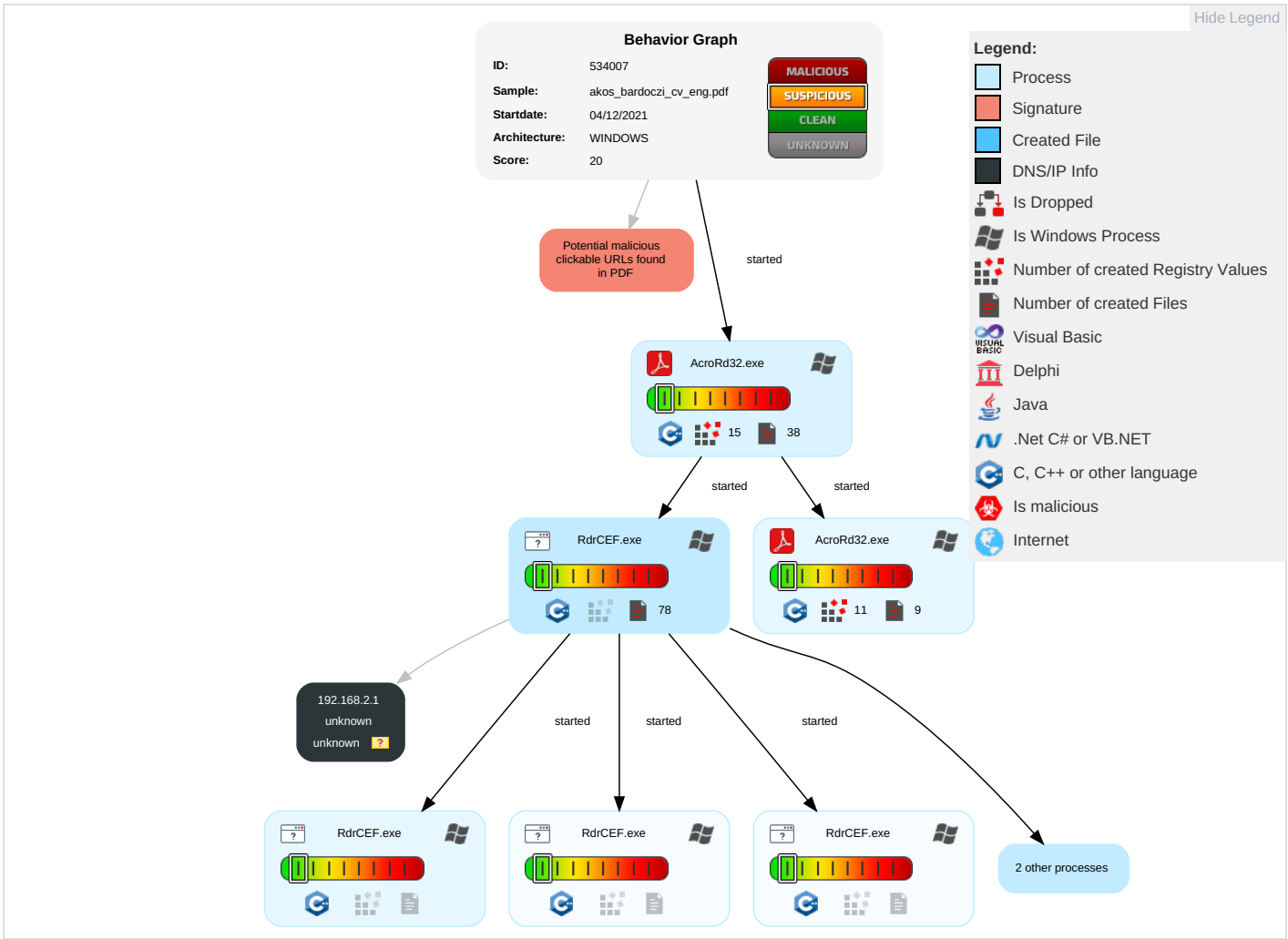
System Summary:

Potential malicious clickable URLs found in PDF

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	Imp
Spearphishing Link 1	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	Mo Sys Par
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	Dev Loc

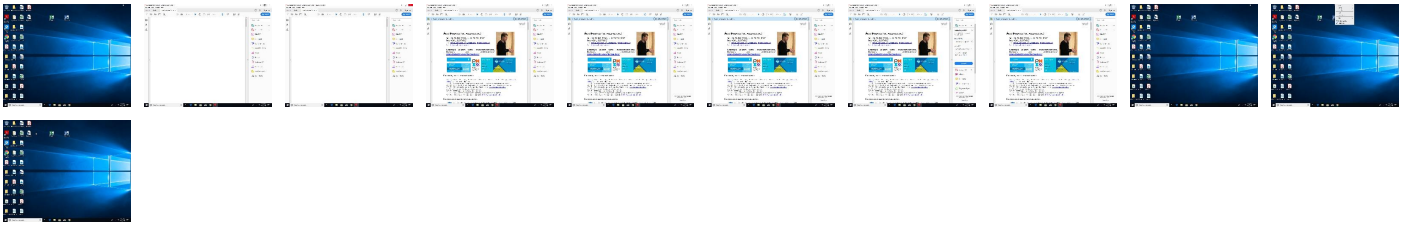
Behavior Graph



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
akos_bardoczi_cv_eng.pdf	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bardoczi.net/	0%	Virustotal		Browse
http://https://bardoczi.net/	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/DATw	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/~AJw	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://.....Acrobat	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://https://bardoczi.net/)	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/C	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/m#	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:	34.0.0 Boulder Opal
Analysis ID:	534007
Start date:	04.12.2021
Start time:	23:52:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	akos_bardoczi_cv_eng.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus20.winPDF@15/53@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 • Adobe Acrobat Reader window no longer existing • Close Viewer
Warnings:	Show All
Errors:	• Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database • Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service • Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP • Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog • Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell SAM Copy • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Simulations

Behavior and APIs

Time	Type	Description
23:53:42	API Interceptor	3x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.571924451896122
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVx4K/y3qWktDiTFJrqzOJkvP5m1:men9YOFLvEWdM9QVKaajtDi7Z+P41

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
MD5:	A2165423D0E2E80B9C020C15DDFE041E
SHA1:	49E924E18BEC80C165FE308432064C3412BE55B0
SHA-256:	48AAF663888B6947C6B1771BEEE7A3DE47A1EE79FF71E504269E06E442B2976A
SHA-512:	D67DCA4F099EFFCFD3B53469C77614C9FCE7E9844C16F3F03917EC633E60418B4A37B7570004B26B143B01A65C4C94F50E4619B84793CCC76EB45D6673C4E1D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..j0..0/....."#.D..!..k.A.A..Eo.....v.....d.{v.^.G...d.W.:...P..k%..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.534692695322481
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVFVud9FSkUkty1e98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkhkFNtyo8Be7Ywcr1
MD5:	2426E7C96C153258FBF0FCCCE6969748
SHA1:	077718CD1815B13D3A67704F71751F9687BD6B86
SHA-256:	5CD6A51924D472AC0EAE6E26C379C716B65D48DB352D0B6BB4F4CA837D0792D2
SHA-512:	C1EB74E4A5C9B835A4FCF6E237C16791660C36B175D8206B9C6FAFDD6B18D6653E916B399EC82CB89FC419666BEE919AA150EF422AB83CE11E5BFC629AA4D9 42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....0/....."#.D....k.A.A..Eo.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.522037648069265
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuajt5t/RlUoSjGY1:DyeRVFAFjVFAFWrtZlUo6
MD5:	17DF325D5FFA0024CAE75EFBFD3C5F44
SHA1:	39218074674BCC23F0380C053D95B09A21439A65
SHA-256:	E066BB8512495C3BC63D577D9BBD887C2E903BA7B746D6B8D48EF4EC4D4FCE88
SHA-512:	77A04E5DFCA989EEB0CB3E48C25378376A37C3C622E3182F06D34CD658FDAB6A2C2D3887E1A60133499011C7B04D56717593DA93C7E2D81F9B7DAA10974CFE 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .....0/....."#.D..9..k.A.A..Eo.....cl .,.....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.605955445540584
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsJSV9wNatrTuiWulHyA1:IbRkiDim9wNa9TjWus
MD5:	844BDC8B9CDDA878A78092C57C6C42BF
SHA1:	617674AA1CDE6F183E0F6FFEFE2160D0E2B6A23D
SHA-256:	777C65B4521C7E2DB81AF6128BFDA0E95438AA0335C68F70A97B87F242960F95
SHA-512:	747206638F8347E112DD6E52254B106E400C7B45B7259565A78E3370BF5DF8A0299EC0A48A68A3231FF5AE0E12037E1A25DD192D3FF41183294C244175AD6E39
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 ..-...0/....."#.D.....k.A.A..Eo.....a.....8 P..a...R..Y ....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

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):	5.534630524294804
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVupPaNt0/2Vyh9PT41:pyixRuEi2V41T
MD5:	37DC8C49A96B876C874442CA5C9305FC
SHA1:	B62727E209668B534A919C70D5D1B619FC90B18B
SHA-256:	55DF15EC2F0ED04861C334EB3C3B9D9C7839C1F9B38D306DE51F6021C970DDAF
SHA-512:	836A44CFBC074BAC0E72529B92D012629F0AC1D8875591D5C7E8AEF76817460D61973719F1B1C3A8E9167043951E09B2B99919546CDD8B38707D43ABBE535017
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .R}/..0/....."#.D.....k.A.A..Eo.....Xh.....k.Q.....-_..y.....O...>..1....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.584610867645724
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVNfS69k9WktxWHlYo2sZI8xeGvPo:mvYOFLvEWdhwjQ8fgtxWF3ZII6P41
MD5:	FD80450B9B719B42A7B9B6380B75B01E
SHA1:	8A46A559C82B55F577214C0D12D0A3D463E4AD07
SHA-256:	130CAB04E00E7BFF1130D9B4C0E2E5898A74D4E03CCA577291CEF91A3C09BC56
SHA-512:	330EAD011DC1FADBF2B3BB3B5D4742D9A52D0AD6CD7B4148E0ED8E1DD26DBEBED3C4D9E6F60B0452D2FDD0604CDB49D56408CF170FF0B189E346C50B7AB9 FB66
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...#..0/....."#.D.....k.A.A..Eo.....y.....].>....uUf..N...k.....c..l.A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.51420094053031
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVim+lmBkt89tlrcyxMtv9EWm1:mJYOFLvEWdGQRQOdQI0tklrD6g1
MD5:	F9D52370B983757D4D9537BD189E953D
SHA1:	4FC5D9438472D9708A32CEF890FDC2AA101F7D92
SHA-256:	F6D0E3E39A196A344B8866E13FE9E4AA6B236096DADA0CF117022F1320D852CD
SHA-512:	40C8248AF6350F24DA646CB36A107A8D587492058FFF149CF52535D6C37CDB19483A4075DA8762C39F91AA896DA723C83D3FB4ED9CB1D679F5E6A95934B0B0C
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .2.0..0/....."#.D'i...k.A.A..Eo.....<.K.....c..y/L....|y.n..C/I.....X7-ne.A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.527193597198409
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVJcSgUBktDl/NQMWqg4nRb7om5m1:mOYOFLvECMLyMStDl/2uR/41
MD5:	464144CA77CBF78ABED62E179213C54F
SHA1:	3ED5458987B0E7BAFCC7F7E3A7DD34DC8A425650
SHA-256:	417F72173C76A04E4D25F6CDE9B76C9BB41474AC916AA0509F9B4220815DA311
SHA-512:	F2CD1C4F1A2ED4FF7E87E0A08FF00B7CC1E6DA2E01CBD8222CE8F678DF24ACFBB5241E2D02248313705573E3FC16291399012CE9EEE2C2D466E045237F4D6F 5
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 ..N..0/....."#.D..M..k.A.A..Eo.....6e.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.58688935346858
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAubtWG9tEvCGm0bbsIDMGH41:XfRMDP9CvCVKsIZ
MD5:	698074A2479AC70310A104EDAA79A1D2
SHA1:	03233C8F5B4211B4F4C95416FA7F8ABA022217A3
SHA-256:	D084F4D780499570FC69E453C9CEFC52E01A4608EA3907AE681F638496E266A2
SHA-512:	57A903294E84E0910661FD09EF31B52655900ACED3C14C60B7DDAAADB353698C72B218C6F6731266D2A2C75F973C1E06FBCEAFC17898A1B74623DBF5E2FDFF 0
Malicious:	false
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .....0/....."#.D..X..k.A.A..Eo...../.....`.....^....L>..Xa./.....C.y.A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.47246690443953
Encrypted:	false
SSDEEP:	3:m+lS8FlC8RzYOCGLvHkWBGKuKjXKSO7p/KPWFvoVcQBktTfzYuuUy0tlBUKSx/yA:m4fPYOFLvEWdtugetTJby0zBUKSAA1
MD5:	116D6A8A593C301C967E66AB689EB445
SHA1:	884B939CCFEF1630C9C1D5B8C9C83E0C7EAF6D44
SHA-256:	FC184DA180D3214106F5BBECDDD2745A08D3056C1A2AE9C3D2460A1E5441303B
SHA-512:	86778F80031ED30D5AA321A2D2542FA8E3AEDD2261C816F747C2DE1661914C418C57D328CFCF2911576E95A1AD1B5FCED97F7BBE024E5DCCB2E305ED0A2527 2
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...3..0/....."#.Ds....k.A.A..Eo.....~~.....Q..E.=....=h`t..t..3%A .F$..w..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.469453568966127
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvD3joLktfR+d1dn76KohyP5m1:md4HXXYOFLvEjMSWFvftfIjUdyP41
MD5:	8E0C938422F38D4069C35E207065CB01
SHA1:	B1D0218F3D08E9650B620298B23BA9E101F4A120
SHA-256:	17093AB87F5D498F0355FC4537D7340E6A2E630CF7F5FF9FE4D85EFA94A287CF
SHA-512:	AEDF81CEF66DDB479ADA5B0BF95E8863FF78ACBBD6393FCC376000BBE1BCFE059BCDBCB99E79B38D6775C482D9F83ED97D305FC429FBF75921D5CD5310F7 02E
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .^M..0/....."#.DF.B..k.A.A..Eo.....nN.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.54791009196045
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLmnvFOqWktCNjUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLkzteoPqVyM+VY1
MD5:	B446AA4600192D0D371B0691968A39DC
SHA1:	EF9C864C07331F70D7098F2E7810148E93A6F883
SHA-256:	B88905352EA797BE084728BA7AC3AD1B539458043BD79FE37C85C01AF2A3DE38

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
SHA-512:	639298A9E7465055DF9C24131479469749420908CFE773027E8B4ABF4475E66EDC8B9E851A63BACADC64EE30E9EDD7B5DC008C1950269B301B63929CFB75D3C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .V....0/....."#.DR&...k.A.A..Eo.....1.....q.O...j...._y..L^z...?..@N..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.570691183764618
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyfLdat9ltwSeKaT9pr1:URVFAFjVFAFOaktwSeKaTL
MD5:	AD6EED966A66DF24DC44AFDE08232757
SHA1:	1F35F8A0DC0AF65882EF4A521F1290AFC69C7244
SHA-256:	173D97DAD0187E2890FDCC1B21F8505C7DEC387935B555D00681F09B764D11BE
SHA-512:	7D8E4FFE7761CBD05FD87FCBE61957B8DA3E3B91D55917D8D9D1C88C900DEB41F75753E966FD2E6E3158C644AE48255DB887BF0037FFAEDC3941E2216FE001D
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 .../..0/....."#.D.....k.A.A..Eo.....~.!5 .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.568017853699673
Encrypted:	false
SSDEEP:	3:m+llys8RzYOCGLvHkWBGKuKjXKmbKPHJXKLuVVur0pQ9LktNE6kV5t0FCV66zu1a:mq9YOFLvEWdzAHdQOv3tKt5GFCaa+41
MD5:	1E6339237180508BCA3B2AC02170257D
SHA1:	C1C47FF2FA7FEFDA4CBC711111C9C357CD36A799
SHA-256:	61FB8719A29CB0AFA8C17A0EEA3C69E3433B940AFD0E04AC8418E351378834DA
SHA-512:	F2CB67C3C1E07E5B3BC8F042294FC820EC03AC0BD8C20D317ED2BB1BEDEA92AC0AE02E919988E3E26947647EF9707300F5BE045E4B1B1E54CB6D2EFB81A1411
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ....0/....."#.D..Z..k.A.A..Eo.....3){.....G.3D.....Q.g0...._.Q.....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.503044010207523
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvn9/WaSLkt0/llhyrpYFm1:ms2VYOFLvEWdvBIEGdeXuNZNt0/l211
MD5:	C6FFFB7C21437C8255A65627BA3D52AB
SHA1:	3FB05AD247C60FD1426052B60A93BCE2320BDB6F
SHA-256:	17ADF8026EB3E67988DCF4C7168F2846F90E631C8650EA830987C6281AC2C518
SHA-512:	F95AF41E020C182F220FAD5BC2395FF705672CD194B581376CF82788853BA98A86F32EFDC763FBBBC474ED2F0F8D86EEA272968847B00D8A6D6090612208C2BE
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .....0/....."#.D..[..k.A.A..Eo.....7.[.....A.o]@r..Q.....<w.....].n\....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.631796313258154
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ6O5tN/xm7OhKlvA1:RbR16a53xmJ
MD5:	C3E236C83FF5A0868E262095C4EE8BC0

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
SHA1:	7CD779B70A99732888860314F0E3180394E6C3DE
SHA-256:	2BB29919DA86543F9B3F87C4E86B637C1AE077027F1A56D6944466DE9C460979
SHA-512:	BDEA50637F02DB26EFFBC926786C01F67F15CBFF9DB1E9ADB8396632F10D76C66272070224DFEB9EF588A5B99C39BD60E729C5B85A78CF8D3FFECA9FDE7B3ADA
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .Q.#..0/....."#.D....k.A.A..Eo.....=.M.....4T].....Tw.....(..b...EO....9.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.553905621183161
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVur+CNijjtdddFt1:B2geRHRQWPNijjn
MD5:	D244E657576860CA9C0035CF562D288C
SHA1:	5824D508DCAE1C14688ADE041F93D492ED56CB0B
SHA-256:	F5346A433CEDABF495FFE4DD1CB6BFFADE2AE3B4C787760300E03C1AF45F3D60
SHA-512:	49CAD8F3B2060E8DE22FCD2D564EDACEE9ADD62A3C44354EECCD0DC6FA5D2428790F7F124529BDCA6B71ED62E87963EA7CA8EB35A361F60D8E64BAB7E089E883
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .....0/....."#.DBBP..k.A.A..Eo.....W.....@..{o]...9o|..qY....T....{..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.596819938885584
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+lAHKLuVguy6GUktA1lGEnNWQ1SUm1:mzyEYOFLvEWdrIOQYy6G9tGGEt1S/1
MD5:	417F57D5BC93330BB7019D81BF8E7358
SHA1:	5FD0FF2E0587FEEC63FA8CE719A456E2702A2630
SHA-256:	C0303C0F431B6FDD81AA317026C54673ABF0468551381648E88A5C35437E742C
SHA-512:	4587A4F6353BD12CC88B51BD1B558B8B79F611C35DA346E58ABC52FF7503F3233CB7C01AF2FE455A4CA3237280987761FEBE6918743F46E605129ABF23998FD5
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..L...0/....."#.D....k.A.A..Eo.....9.....t\a.....x5.'OuE.C..@.....x..A..Eo..... ...

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.5598491511290575
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFv4ISVKlRWktZ/SlwJNqww6U+5m1:mnYOFLvEWdhwyun5tBSlwrqwK+41
MD5:	490E66A0B852783EBE89FBBE9E26FBA2
SHA1:	C47E02127D5299BECE61180908A1CD072262B8D9
SHA-256:	23DB354BC00B50B79269AD06B029D8DA5F93FA378D1914AF2F9E71388E87231A
SHA-512:	C0ED831434DE984DCEBCFCA5C76458CD036D020D4B4D76FADD2AD93406684AF30F5A98E0C74AF8093EEEF7A63986AE514C49CB211310C7C1656572E309B0986
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...''..0/....."#.D....k.A.A..Eo.....{.....7...o..a=.98I.....(3.$G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.568197757006861

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuQvnt9Qtp2KYfO441:/RrROk/DPYpYfL
MD5:	66CBC4AC5A111BD6808D2D2CF1CBC954
SHA1:	67B6D380F1A9D8A3A7C23B9B076ADD1D13C01801
SHA-256:	7AEE80327E1F0FB3EE2F91A46FC4CB5ED7F53F3292638ADC0CC59B6150A83385
SHA-512:	9C7E166305774F9FBDDDECC01B09E67B2D7BCA943AB19205CE9EF50858834D479905507FA167B7F53E182E4985B54B105413BFB26ED0D0F24E6DA60C14BA930
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .?K...0/....."#.D....k.A.A..Eo.....NX.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.5780582990394
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVE4V+uJOO90WktZzoIN1OFPL4m1:mmDEYOFLvEWXIEYNBQtZzV1QPLr1
MD5:	6F1142CCCB1B5FA16DA4115CA5BECAB1
SHA1:	C5440654B9F40904CBCEE0A2688AF31309EFFCC7
SHA-256:	229F70D7755392EC4168DB63C4BCFC669BA759BBF63EA7DB7AF46F1A4B9067F9
SHA-512:	D402F29262AC55DF6F7F6755B59B44DF58C03D6DFF303BA84A39D5C5BA56D4BE294D11AEDB8C966BB542FD720AD2B9C759C6ACAAC4CA769731BAF140BC3FFCFD
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ......0/....."#.D....k.A.A..Eo.....[4.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.574660922878286
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFve7jvEkt8O9llM8D6EsEJeUm1:m52YOFLvEWdMAuKjvNtVllMEvsEJ41
MD5:	3F735F3065B575E0D45E1CD18BDF3349
SHA1:	E2FA407B543BAB61866802919C9FB7EDEDEAFA5F
SHA-256:	36D86345EF9543B9CAC7917FC5C53E74EB3DFB632FBEAF1269A6A6BE006CDB3D
SHA-512:	4564CADD89E85B4F36E61EB03AE391BE1E02261089A49FC5477AD802E144B539F263B8DE3904E8C1686A83AF0D1964E33A17D9480C14BE39BFBF493BEA362408
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .../..0/....."#.DK.g..k.A.A..Eo.....z._a...'.v.....4p3..1.']...A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5675944695386255
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvQKOnuEktRlIFoDb7T2/Mm1:mYilPYOFLvEWd8CAdAu2fuNtRlyong1
MD5:	4FB28E9174EA42839E2EAA33A752DC80
SHA1:	6DF341F0F1474FE7F70672FD3E121EAB53709338
SHA-256:	7D0A0FC403E93CF8DB1D9ED966648FEB44164233A75996C4B5D4D81B281874C8
SHA-512:	8AD147DEBB913EE7AD814AE644BC7320C85F9BD5E6BDDB67DA84A300031F4B2E4B5166E425ABCAD09F323E28E7D03BF0BAAA50DEA80C225020C2F86719DF7479
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .../..0/....."#.D.~..k.A.A..Eo.....c}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Size (bytes):	223
Entropy (8bit):	5.572820744435803
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/lux+pStVVdN16wG1:F8hRrROk/vXV3
MD5:	677671E364AC6A12431DCA5C43E334A9
SHA1:	99B58B17B4A7D6FF6262C3D0BCF9F7D4D71FAF64
SHA-256:	0ACA0D400742C3B04CA91A7C7DEF039841386BE82A10AD2E26AA1A0058B5A484
SHA-512:	966FD9FF5B46E80AC2DA42CCCD56779F06F56A0F6EA9850F1D583659F88B5946DB59EC4219D82A8E8926BDC6F66CD200CF76CB9236AD4F9FE8DDC7FA01CAD55
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....0/....."#.DC8...k.A.A..Eo.....?..X.....%.k.SZ..~W....:)'B..ad.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.6277708234506765
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVz6gaJ0WktclWPmJelc0Ry:mLrnYOFLvEWdrIoJUQvRQtUWeJli1
MD5:	C8033FA164DD541D23DD633B7208C29E
SHA1:	8805AD6F0102A1D560A847CDC1291742A971321F
SHA-256:	ADC99164EB6E25BE7FF41E8FFBCD57641BE9E728F376BB67873CAFF1DDA32073
SHA-512:	131C285B1CC3FEB5D48B5EBD96BB62EA5E25CD62CA57ECA76C37D2E3B91EDEB48035D7622368D94BBCB37EC9D9039FE5AF689207E93EE944007E3D81B763F44
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..N...0/....."#.D....k.A.A..Eo.....=.....;"./N_.,.:C..2....9L.H...3:...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.559561258157458
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvbs9LktHyl/n6mgmOZLhT7Um1:mOEYOFLvEWdrIhuxcQtHytnzgm2d/1
MD5:	3FA6A97ADC708A76D08D36079FB9EB16
SHA1:	C72FEBBC94E8E3F3C3BFF0710B9B58818FD902D4
SHA-256:	4DFA8C3B0355C052D0918A37B7F5FACFFCF05230DA2B95F3C4516F8E37478E95
SHA-512:	02FB0C49229170AB7BD8B766E668AA2818B0FBB01ED043B603BF51D5E41655EC075F0581062A6952632588B3B7B87B579572026CC979C8E114078477761C7FF9
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....0/....."#.DCr...k.A.A..Eo.....v.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.561159621652287
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cv+SgYpX9WktU1GBiaQ562HvpMm1:mAElVYOFLvEW1KSX9tURx56uvp1
MD5:	B6B297155883C4F690E616EE55BC8D01
SHA1:	15C3B2D24056358E763A4F8C08347FACFCBD669A
SHA-256:	0253E3DC0021183A645A5727321D0EBA2D2740E9F314065341184FD42ECFE281
SHA-512:	1432EF7BB98685277D3078FD096C5CAF41C35D058DF292ABDC3EF084ADD6615089B40E3642D3E215DD267AB2136CAFE969B48F3476B779226C4298CB4F7B11D
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..e...0/....."#.D;.n..k.A.A..Eo.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.597341307525521
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuQR+JtglTUDLYtmOZn1:xRBJlRWqYDcFZ
MD5:	F4858F23F5CFEE617A4DCD2E9B1471F1
SHA1:	3AD269279E701DDEFAB53ACF43CD147A583385C0
SHA-256:	DE1E589824AAF8C293E90839BF662EBE391DF4A8F7D39CCB795486343F00EE75
SHA-512:	19AC912914D4A04079951CE7438BD8260505F9E06BBC2DD75F1DEEE8226133612DD145EEDA9C137A3C9896CA516CBBD4B9A989BB8762ECD8FBAD362BA6F0F4EF
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .../..0/....."#.Di.s..k.A.A..Eo.....].....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.5717984748834235
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvVVKtQs8FSLkta0tPpSKGop:msRPYOFLvEWIa7zp7ALs8FNtaC8VPu1
MD5:	FBF4262633028FC5EFF22650CCBB36E6
SHA1:	7D4F18CD2A034BDFA1E847DD1AEB4DC72517C613
SHA-256:	224460F065B25CD736C102A38D0324BFE469A13B3C3D9AC4ECB0500FEC826A97
SHA-512:	5B7F308AC74074BF6EFE85664C76932C79A323807D2584923402FE4B30073B642A7F950E6537123858F8EA5A36C3DAA4F71D8D6C5D7EBA6942BD6E8683E55EA3
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .jP..0/....."#.D..Y..k.A.A..Eo.....L...Im.@.....E.nW...IP..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.550716200402089
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVafmSzUWktnl/96F4XVAZ+8cV3I:mKPYOFLvEWdENU9Qv/zUjtl0wiM3Y1
MD5:	078B190CECE7ECF64ECFE0FCECDC3E53
SHA1:	53133156F2280C044C41C4663CA11D04B2BAF5BF
SHA-256:	9595E0A397AA7C07038AE535ED1B6163A197FCE47EB37CC0D1E8D32CA1A900E8
SHA-512:	6F9FBB95613312D1D4B500627E702F64D864FDF770D543A57370413D977413DCB5071C8DDF348E13755826622289CF8F62D670DEAA97E651411EC2498128C0B8
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...#..0/....."#.D+P...k.A.A..Eo.....g1.....M....m+lS..e.....<7.U.P8*.0K.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.594559544049992
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQzOfathXwjBRCh/41:XRc9da4Di/
MD5:	E2A943D4D1D0473083A8DCDE1F5A2096
SHA1:	43DD310865ED3F02E5F3281CD383ADB947FF6C4F
SHA-256:	4C78018F56476683386FAF24F000FF9755383664E65E77EB449C301BAB1090BB
SHA-512:	18FED1718AC3696FA89BAD84EC14FDF79BF678F3609B9C92E4B521513C8004742AC8C86F52C9C708A27F7666FA00B828375781034489549FDDE4C60E7C3B58D6
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...0..0/....."#.D.....k.A.A..Eo.....dN.....PJm...0x.x..RD...BB!@5..<..]....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	231
Entropy (8bit):	5.559487569468151
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu5BbdatWvkULlF4r1:bs6xRkirRdaw7LlF4
MD5:	3E3CC7B1E387A94548961F981410CC9A
SHA1:	183BE7329A5232FDD512559ECA625AAA9CC03ADD
SHA-256:	1DD917BF47D6E15338F5DB0F5A7CE1402E6586AA34937030594F18AA939E1B04
SHA-512:	F77846C8ED9E5E3063CA9195FAB9F144BCC56EC171217D2CC80C2BACE5D461670DC20EA6D5FF2E45DAABC8B24809E69558B89480BC4F6D43A6BF78F9125627 9
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .!!...0/....."#.D.....k.A.A..Eo.....J.....P...#4..l....5 ...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.497724007341836
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFv6Es/aOGUktlVPECcu1isLK5m1:mhYOFLvEWd/aFuX9tlVPEN941
MD5:	EDB500CCA519E246EFC9FCEBB67C9702
SHA1:	9729D505A6920C2051C81E80F26BC4E8822654C9
SHA-256:	0D1C0794566B7C75D73DBDB57427A7C7B55BA8F9D570BCB6A561A5FB60CF9559
SHA-512:	85749760ADB28DC95F826F711C375C0F6395664887FFEF9B34F6C88294CB3A69FDA34C5766C52B6371259321D703B19ED4CA1C3FC12F45462B68FE81EC32DAE4
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...3..0/....."#.D.....k.A.A..Eo.....mBK.....a.f.m.i.o.p..3U5.....^...I.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.490131903059353
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQLFrjt5BMqVd3G4K41:2DRuRKFvHB9Vd2
MD5:	E4DCA1D110EAE3B44BCCC4FE39578E5A
SHA1:	CBBB721E621366BEE352E815CD517DAE56B432F5
SHA-256:	4EBDE7DB19CD96B95E91AC0404FE4BAC22CA03BAE887CA89AA0156A779A7BCBF
SHA-512:	715D5160C68CA7C77BD77864D3CD1AF2C6C23E1DD857BEFEB5D7B2E709BE817032E51F4D5F562E017DDEB00161BF7B03E959070259173C0DABE2FF50255B40 E
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...0..0/....."#.D3T-..k.A.A..Eo.....t.*.....y.$..$.v5j...T...z.]..._S....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.545086014937237
Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVP1HlXQZktcW4ThzJuA4bi4B:mkqYOFLvEWd8CAd9Q+CatKuA424r1
MD5:	9116945B893BA68FA6882C94F6F72144
SHA1:	5A8014E5D984E18BD92AE023857154186B55F645
SHA-256:	6D00BC2DD54D5991E6742D4FB894D5FE569B71538E80099291E440045CFA5F88
SHA-512:	7F0890F9ABFBA10F8A26CEDC219F3E60DA1D3AC8E378B50BEA8066BE858F93895564161EDC8772BADBFEEB7B6CD667CDC5F6AF3A439DFB922A5C06F20464D 15
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .=.0..0/....."#.D.-...k.A.A..Eo.....K.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.519596472614944
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvI1dS0WktntTAg2iHio/Mm1:moXXYOFLvEWdENUAuuNtnt8yC8n1
MD5:	77A929DC6DB10C1CF1C53BB6AC805F95
SHA1:	A57B5541C723C34CCAC2FF2543AC9BBF9F56843B
SHA-256:	0868042872496D4EF50023E5EBA90E4DA62B04F5651E452F84BB277CCFFD8678
SHA-512:	BDE8284024CF68AC25AC1672AA8AE599254E52431512F4D718F68C5B89F4E551637461A7A08A2A62FF1FB601BFCFD6E785CB07874F05C68138022DC0ECB69D5
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .-."..0/....."#.D.....k.A.A..Eo.....pL.....8.../...;.\\o....1.....+..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.556855579240912
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVIJ/2kKLuVYmaIjQBktxm/sYWmYk5m1:mQZYOFLvEWdrROk/VQPA3txm/sLmB41
MD5:	212E8D23A127E8BBE67C1ADDE878EB5D
SHA1:	014EBCF89EB956C193F2DB15291A3162075B2039
SHA-256:	9116AC5FF20E36355177CBB2BACC51ECBDF8098A6946D15D03A9EE5FD6706ECF
SHA-512:	5E59AF2A89E7BDB31E73BCBFE2BFE199CBF0224BB86107F52DC7C809C824A5ADBAEE97F8B82EB911AC0473B96D78B30F2DF60AEC1EA95B0C826EE90D03391 107
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .:p...0/....."#.Di....k.A.A..Eo.....9:..... ./.ev.....N~..6.b.....$ .j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.53646875445157
Encrypted:	false
SSDEEP:	3:m+lUV/la8RzYOCGLvHkWBGKuKjXKjcAW6KPWFv+VKG20Wktj1Xrobk9mZa6tokPo:mZ/lXYOFLvEWdccAWuWhjtj5dm9741
MD5:	9A5FB72535F25621D596235C418798E4
SHA1:	CA58EA8EDE18225E34A9799E322B8108B5DF18E6
SHA-256:	35F64434EAF3AD44B401A67ACE3D6C96F5599BBA41B4B05B2D8D50E736FF2D00
SHA-512:	C9536AA9C27D3ABCF5BB477D74E1863C7C7A735AA1B4A629BCCD4838FFD02491A9B6BFC1D9E19B619717252DDDC90D39CE8CD03A174A504C97EBA2FA5762A 87
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .k....0/....."#.D.LE..k.A.A..Eo.....w.....U...I.>P...X...x..0U.~;m.x.k.A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.498267096060822
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvKHfVF9kUkt9Jtl2B6shoq+Nem1:mMOYOFLvEWdwAPVuoqtaB6Jn1
MD5:	94429E0E2744707F4D716742E100C664
SHA1:	021F3B6AD8184EF3C2B8C3700EC9B90826F4F6BA

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
SHA-256:	B505BF446E814C572BAA0F88569558BC81CE7643CC4A660A818D522CC8B76208
SHA-512:	B07A716675A860AAE1A5F3FE609D22A5DA25E9A4D1E5244C6BB2ED931EBB2C25397F14BC23A189AEBEA6D5BBFB7D8E6E46E6CD5AEA2BA38354C241E11801BA24
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .P."..0/....."#.D.V...k.A.A..Eo.....:h.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.619184840883762
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQZG9t3/ihcsBXIh1:mxRBJQqS8B
MD5:	B0016FEB6767107F5DC83C466F434C76
SHA1:	9A66EA33A3BEA5CA9FE41FA5BE3535A78FA29D07
SHA-256:	ECD25D7746EF2BCD9CFE5DF1452C983802A6074EA0C4AE347F7066AD442097C7
SHA-512:	59A63188D5E49CB46C30722D3A9B435520405D6FDD18873F5740C9A210EA1A028411D8CF1F163B6B13CD93DFE2DFE33D2FB0B974F711ED65012C85D39E780DB
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...0..0/....."#.D.....k.A.A..Eo.....)(.....k..`..N3.... ..d..$[.....{.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.594862836252644
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQd+QCtx9/Bc3Me/1:3RrROk/sDDX9/B
MD5:	2ACFC609C9134FFA7C9E8A517FDD7C63
SHA1:	46FBFFF7BB3C879E4D9D00ABA850EDC979666B83
SHA-256:	A12381412706CD8C5AC3D7EAB0785E5BBEBC83762AAA9B99A2375B59CE6C53A7
SHA-512:	DC394D2D42A81745311F53B9358CDAF3C3CDD80D4CA69E0BE1FE911A9E67534B1BBB4CEE30770092A7513F1161FA646B81D3E08199A5B11245AABF1B8297DDF
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..q...0/....."#.D.....k.A.A..Eo.....G.....9Q].8O.z....=..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/I:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
Malicious:	false
Preview:	....h...oy retne....'.....'.....:.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+...._#.z.B_./.....J..j....z.B_./.....6<|...8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)	
Size (bytes):	984
Entropy (8bit):	5.040251725706932
Encrypted:	false
SSDEEP:	12:MeVl/9l/gLnl/2+/l/KLvyl/CAl/q5tbyl/iil/iHl/OHl/Wyl/jl/lsl/lA2l/l:Mfg1zZFufGMisp6r6C9QPr
MD5:	9B90244F9985CBA4985897217DD7C7AB
SHA1:	9BC5919E96D2A3CE20322AADC162056A6B6FE7EC
SHA-256:	E44D4707C1D938DE3374B96940F3B6AB183AEEDDFC92C1B25617C57337E95941
SHA-512:	15C4CB9E0569A8B9A35F369364B2C4312DF76EF721A8DA8C3CEEB4A289D5DE061D0D14EF2C0D35A1DD3FD12014BA67243DB65124376144BE2D2943FFAB742F6
Malicious:	false
Preview:	....h...oy retne....'.....'.....:.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|...8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,4>..z.B_./.....&.S....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.25065734941202
Encrypted:	false
SSDEEP:	6:m/Ug+oM+q2PWXp+N2nKuAl9OmbnIFUtqUgjZZmwsUgnMVkwOWXp+N2nKuAl9Omb5:R+vaHAahFUtQ/LV5fHAaSJ
MD5:	9C355778D6B4ADCFD50FF4EEB6D0C995
SHA1:	878BD5875C2ABED26A5578998883E52EEB9FCFA1
SHA-256:	18D84391B3B7EF52B1E97C35EB7504A615ED1715BDEDBFF7C4C89A9B99A19DDF
SHA-512:	BF897FF108C3A6AD08B867DE0F2F4E73E4A062B5CA01589EED42C403FA703187FF9E7486176AB116BAC41EEE9C6D68F2375EF4A8286565A775F4FE3ABC600C88
Malicious:	false
Preview:	2021/12/04-23:53:46.722 181c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/12/04-23:53:46.723 181c Recovering log #3.2021/12/04-23:53:46.724 181c Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.25065734941202
Encrypted:	false
SSDEEP:	6:m/Ug+oM+q2PWXp+N2nKuAl9OmbnIFUtqUgjZZmwsUgnMVkwOWXp+N2nKuAl9Omb5:R+vaHAahFUtQ/LV5fHAaSJ
MD5:	9C355778D6B4ADCFD50FF4EEB6D0C995
SHA1:	878BD5875C2ABED26A5578998883E52EEB9FCFA1
SHA-256:	18D84391B3B7EF52B1E97C35EB7504A615ED1715BDEDBFF7C4C89A9B99A19DDF
SHA-512:	BF897FF108C3A6AD08B867DE0F2F4E73E4A062B5CA01589EED42C403FA703187FF9E7486176AB116BAC41EEE9C6D68F2375EF4A8286565A775F4FE3ABC600C88
Malicious:	false
Preview:	2021/12/04-23:53:46.722 181c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/12/04-23:53:46.723 181c Recovering log #3.2021/12/04-23:53:46.724 181c Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.010978819626460943
Encrypted:	false
SSDEEP:	3:ImtVdXb+j4x9pPlXlpyPll//zVrzlltD0lGQZ7XEZhGIelHdP4/X:liVtg4x9pdM//hFwl570ZhdelG/
MD5:	E36F8F81D3C03F6AAF7D768706B7673F
SHA1:	EECE93F9E417717892E50F6A159516DD76C255B0
SHA-256:	C6E687FF9677244574F37AD2877726DF64E5BAADDA2ABE8C4759BDE8344E44F2
SHA-512:	0582ADCFA1A09095D4482C9A61475C8B77FF444BF2655DE4F6583BBB2699A054BBB2292DE2741FEEB27AFE0835B0B48F476418EE1A666DE20CA146D1EB4390A4
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-211205085642Z-17947763.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 117 x -152 x 32
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	2.6618016375015423
Encrypted:	false
SSDEEP:	192:olAeIukWQCMxNPYeXTp72PU8TsssFrL1KDOb4UgHdT0OZ/8SPdYkBMtpOwe3cG7o:BVgQCMx6gTc41KD64LNRhH79wN4KVz3B
MD5:	A67E28F325EFBAC368961FC9A1A82AF2
SHA1:	0753A491E0EA35FE63EA3DD4303BDBB0B36DE674
SHA-256:	C3299341FA90A6C3FF8E39022CE8444965D902B028DA490D6816FC4AEC8A71AA
SHA-512:	64CC93B5AD654DFCDCA1F95D5472388E394EBC60DCFD236DF7E657E32D8AA7B36C731593D5D2BF36341F6153BA04743BAE93CEA67CA853EE9A872930F1278C A6
Malicious:	false
Preview:	BM.....6...(...u...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.5643617314174345
Encrypted:	false
SSDEEP:	384:3eI9dThZtELJ8fwRRwZsLRGlKhsvXh+vSc:RkYZsLQhUSc
MD5:	545E53EAF76A94722714C8C5FCEDBF8D
SHA1:	AC1FD4F6A73846C0BF53E4598BB1B06367FF0484
SHA-256:	336DFC7AD191AB048BF5586F63945AC387DCF1E40FD00EDB4F2A65328EE36686
SHA-512:	6A73115CCFCA4AC95A537EEA748185CF98BBC962CB03AACC44716FECEA8FD6BACB5C57C81E1BB5B6A728DC2DF06AC050375F50FAB028FFE901911288EDFF5 71A
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.284797622136099
Encrypted:	false
SSDEEP:	48:7Muom1CgiomUiom2om1Nom1Aiom1RROiom1oom1pom1IZiomVsiomgtqQlmFTIFR:7ugPOhsCstN49IVXEBodRBkO
MD5:	D36B9B2C3F43AA1BF3CCE25F88CC99D9
SHA1:	2B1B72E450D792DB88543FE72101D4A6DC3EBCFD
SHA-256:	AD9BD07AE9819562364DB5725D059178556C9A309F375F0705483B10794575ED
SHA-512:	B0192AF36B678A74648003D9BBC7EE52AA11A5CE3060F9DA6EBE9B066A25ACAB2D9E59608945D19FCB6D083B6433F7DC4203DE747407BE0A67B788991202574
Malicious:	false
Preview:	.... .c..... .....s..... .L.s.y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents	
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):	12288

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents	
Entropy (8bit):	0.9016741092246371
Encrypted:	false
SSDEEP:	24:TL5wx/XYKQvGJF7urslmicNSiITFMliDPjNvij7CmiL:TVwl2GL7msXcNzITFMoDPjsf8L
MD5:	5FE8B10220B985A5698625230F331BD3
SHA1:	CA4E39643EB3976636D972681BD893A3DF3458FE
SHA-256:	C04FED1D5865AD94AE903B18BA5F1C265D336B254225E8DCDC4215D4F6965965
SHA-512:	A04BB62CBC4EEB74B717A3DAA4EA0DE2F11729F8090B27C9A780354BD04CC4C9DEBEBE8DF6BA743548A77E9E2DBB9B81C0261CFAED8A70EE61442976A1034AC9
Malicious:	false
Preview:	SQLite format 3.....@ .....$..... ....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	1.2316739716082021
Encrypted:	false
SSDEEP:	24:7+t/mi8SiITFM9qbvij7CmiRqL+jx/XYKQvGJF7ursd:7MV8zITFM9tf8Rq+l2GL7msd
MD5:	8305431455F73B902BCCFA2DE54F283B
SHA1:	30295DC621D5E75824DC67447FA0B572F1CB3844
SHA-256:	45D7DE4B396DEF15A09E80CA2D3A81067403706FF02F799FE8C757ABBDD24F7D
SHA-512:	12F1945E594400749363457D4E36FC30CAC4AAA6F811F7F943BC6B3F60839727C3ACC866E88B2E94503F876D8FE3B934E04C4639EA8C240311B5F1E1B66F98E8
Malicious:	false
Preview:	.... .c.....7..... ....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	0.6750050738677021
Encrypted:	false
SSDEEP:	12:BZ2vX7vz+YXnTIHLjJ9wkI4c6/oCyitQBOIP0xg5/fLM:BZeXTz++IvJ9wkI4c6QbiuBOI2gxLM
MD5:	C38DB0F968872CB3B1FBF6AE9A0EF9DC
SHA1:	F33A6E1368267704758D324C3170FFEC35A64886
SHA-256:	6B804B2E7E3F3F270A809298758697B12697A26846FF9D20E0FBFDC9F64EED8A
SHA-512:	55BC7AE2ABAF607B7B4F6804390ED8FC796EDC0D778728DDF84E62B97BE74C1BD9547CA1EEAF3646BADD30C8AB1A7E20D534249DD976E07BA83B718DF6A39AD8
Malicious:	false
Preview:	...Q.....{W.C..$;..U....b.T}..k..... .....g$#..q.....i>....[]l..... .....M^.....A.....W >.D...{.... .d...h.g.U7.Z..!.....j.&...Q,9.....M4..mN.1...CB&....$.....,1!.f_?.1..&.....a....t. ...]U.hQ.?.*#1....r|..0c...=.....]..J.....LfhI.<.....].5...P.5.9..{`b.GB.....$.....r.&"8..2..x5.n.j.{.S}..l..[..4..K._.*....Q..A..L..YY..vg..M...x..d|0...k..I..~...-Cih.KW...,_".i._.!..X.r..... .&.Q`....90....L... .bz.s-Z.}..;v..>...%.|.^.....}.qm..:....Pf....`.&.L.....ny.....)I.M..Q..xZ...$.I..... ....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	24152
Entropy (8bit):	0.7519410049126055
Encrypted:	false
SSDEEP:	24:DM9iGGEWwXc9BeayznQAY3vFVV5jDBJej5JVzesSSUeolpgdXcdSqx2DX95:oVXG9BCWZ857zctlawz
MD5:	48B99ACAEC7BCFBDB7F0B4B96B2453B1
SHA1:	BE8AF0C8AF83D943747928B45EBBF44ACDCB374F
SHA-256:	D92FEC879C4EAF4D3B887C7FDD0FC602F9C97C0BBA66024E4F280C27DDDFD0A9
SHA-512:	429D4DB90913FA07F2402BBF3802A4DF6DFCB1E367E4B41D8629B85F463FAAF38F5A6EC51D0551C4CA845FDE856C2203875DB5F87DBA6388B0A4A648363DF32E
Malicious:	false

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Preview:	...s..K.....j+...%...X...Ba.....zzd~.....#B..0_...\..=.u.!!..+@.f...Y.)mg..;...Ab.....a3..k.....MU.Jq.$*.jnG..*.WY..W.~...:.D.M....n.L.....d.."b..]n.....bj....p...d..cN.s..+P8.{z:x.P$:..n.L.X.....co[v"Y....^...59.32.tn/Ce0.*\..i.N.N.}A\.e.U..7$zf_x..j*.buOq.N...P=0'.....e..#.....I..;Aq...|.el.78..g.#.....k...#2>.....G....% ..K..=W.!..@..[..7_>PI..(.$..%..`'.kglw.....UC.4.....^.M...!....4y..O..~.|...vpY.8\H..z..Kb..j.....7G]D.9$.7.rRu..,t!^..0.e...|.X.]..k.KVnb.B;.n..P.....q....P....:mg.jH..R..3m..x.$...zR.b$..QR.M...`.....U{....(.a..Z..EZ.6+.BM.Fq....Wgn...=..k|.. ..>....q...T?6zSB.....1..6.....s...l^k.Lt..f..c`..V.qz@.+..e$.....

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.9043678793345045
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	akos_bardoczi_cv_eng.pdf
File size:	646865
MD5:	61155ce562820a5628a0b321129dd2ba
SHA1:	c2267b76c0c9e97c71756d4357468832d1585afe
SHA256:	7cf78d07e0a83b84446d3f26bce805d67af02da54672b5b9f1220218a0e063fb
SHA512:	efc61db12bf70f3510054cdd1cd641a017bba0447cedfeefc14fc1cddde90a3c56f97d2736e5ab63edb5f30ba318515e33f7a97513f8a4bf7c6cb2f02f008b01
SSDEEP:	12288:j4uRJCnz19Jth76fIAXKEZ+yaDGb/m2tKOHHwS+x3s5:j4uAJrfgDHaDg/6iH1+x3s5
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 110 0 R/MarkInfo<</Marked true>>/Metadata 484 0 R/ViewerPreferences 485 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 7/Kids[3 0 R 53 0 R 68 0 R 80 0 R 91 0 R 98 0 R 104 0 R]

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.904368
Total Bytes:	646865
Stream Entropy:	7.979753
Stream Bytes:	590057
Entropy outside Streams:	0.000000
Bytes outside Streams:	56808
Number of EOF found:	3
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
13	9043631319314b48	039cd2a13e86b032a36ba67677ae3119	
14	3430b4c485868a4a	0c872fd990afafca1cc9254f5a095ea4	

ID	DHASH	MD5	Preview
48	c3c33c8c8ceea68e	d70fea879fe14914eb2e97365cbcc85a	
49	4464252462626364	1e7d30c034cff34f570d5a9254babdd6	
50	18bca463d0c8c864	f8464ddfb13b1e2ebf07882f3204bd69	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 7116 Parent PID: 5480

General

Start time:	23:53:02
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\akos_bardoczi_cv_eng.pdf
Imagebase:	0xbf0000
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: 5496 Parent PID: 7116

General

Start time:	23:53:02
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\akos_bardoczi_cv_eng.pdf
Imagebase:	0xbf0000
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: 7004 Parent PID: 7116

General

Start time:	23:53:41
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0x870000
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: 7140 Parent PID: 7004

General

Start time:	23:53:42
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1568,120521731759888 17585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6127630510957074088 --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=6127630510957074088 --renderer-client-id=2 --mojo-platform-channel-handle=1696 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
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: 6268 Parent PID: 7004

General

Start time:	23:53:43
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1568,12052173175988817585,1117657172976690578 2,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAA AAAAAAACgAAAAEAAAAIAAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAA AQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAAQAAAA UAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=585970285045658890 --mojo-platform-channel-handle=1708 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2
Imagebase:	0x870000
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: 2408 Parent PID: 7004

General

Start time:	23:53:44
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1568,120521731759888817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6328359103851257533 --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=6328359103851257533 --renderer-client-id=4 --mojo-platform-channel-handle=1940 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
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: 6912 Parent PID: 7004

General

Start time:	23:53:45
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1568,120521731759888817585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17081285814894932504 --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=17081285814894932504 --renderer-client-id=5 --mojo-platform-channel-handle=2008 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
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: 6300 Parent PID: 7004

General

Start time:	23:53:53
Start date:	04/12/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1568,120521731759888 17585,11176571729766905782,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=3781967090892827746 --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=3781967090892827746 --renderer-client-id=6 --mojo-platform-channel-handle=1932 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x870000
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