ID: 458993
Sample Name: CUNA-uncashed check.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 01:20:55
Date: 04/08/2021
Version: 33.0.0 White Diamond

Table of Contents

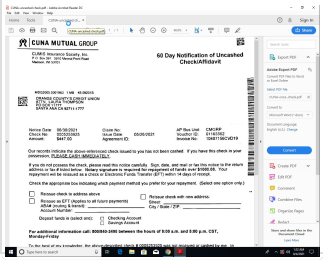
Windows Analysis Report CUNA-uncashed check.pdf

Overview

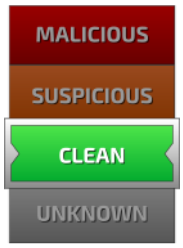
General Information

Sample Name:	CUNA-uncashed check.pdf
Analysis ID:	458993
MD5:	8bc64f6d8200077.
SHA1:	6d2cbe3e6fc6193..
SHA256:	ff391ed81da3dbf…
Infos:	

Most interesting Screenshot:



Detection

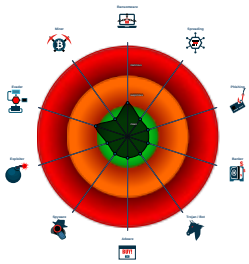


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 6992 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\CUNA-uncashed check.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 7112 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\CUNA-uncashed check.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 1372 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6540 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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16643864859160111475 --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=16643864859160111475 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6336 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1720,6803796534539775004,11392875392024183128,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8013375785811497341 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 3436 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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7474857484354196562 --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=7474857484354196562 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6532 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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14789584177783671881 --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=14789584177783671881 --renderer-client-id=5 --mojo-platform-channel-handle=1980 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

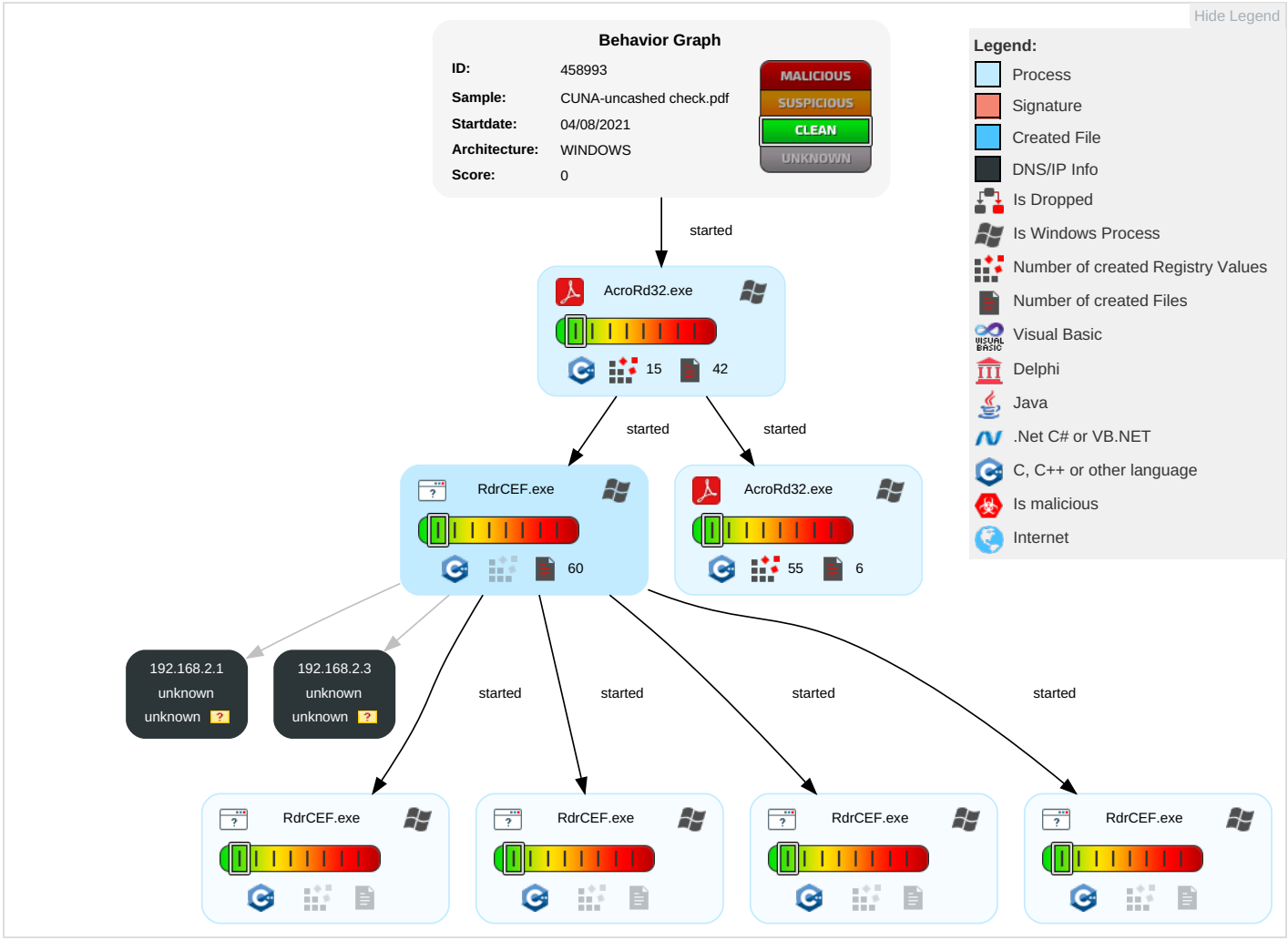
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

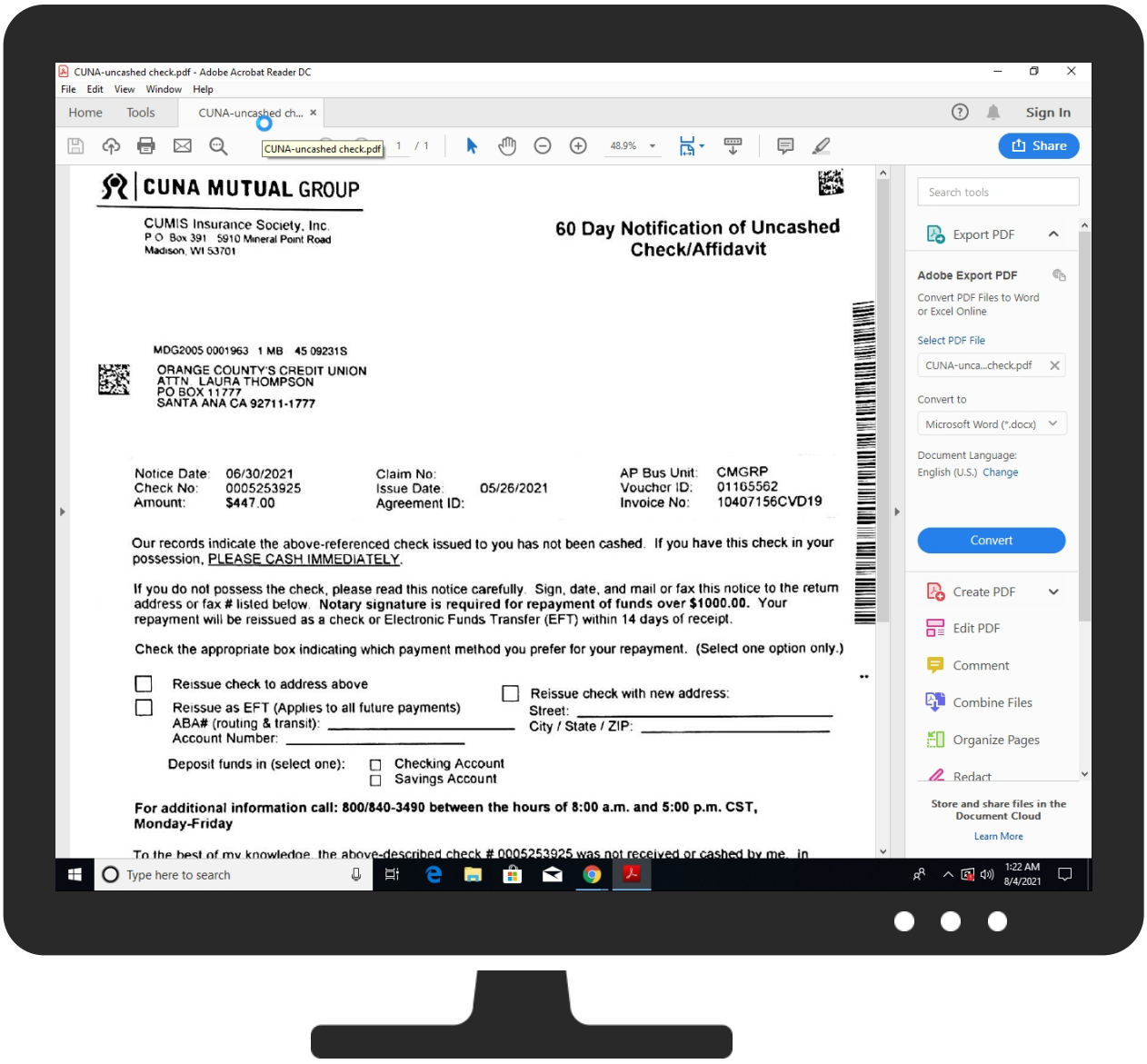
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
192.168.2.3

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458993
Start date:	04.08.2021
Start time:	01:20:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CUNA-uncashed check.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:	21
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@13/55@0/2
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
01:21:49	API Interceptor	10x 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):	615
Entropy (8bit):	5.639121270329041
Encrypted:	false
SSDEEP:	12:vDRM9smZiEpDRM9V1aZiEtDRM9JzfZiE:7tEteE52YE
MD5:	C902FC0AD9F4BD0B57B0D35FF8FD01BE
SHA1:	4B9758D3014386A9108CA956FC9460C2FDD1E50F
SHA-256:	038A2E03DCB691A9FC51841AEA9BD84D623C9CFEC2E99D2E55284CC5EFA9E25D
SHA-512:	721462A01E8F6D255566C3A5782C35DBEE5B64EA1B74AA55E69163C47445AFF5C67A3EB0CC383A8549CA7778EB9F3B98E1F368A0BFF72CB9DD19202FC1CD2CB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..|.<F'/....."#.DB...sB.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... /..$.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....<F'/....."#.D6.v.sB.A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .A..Eo.....9.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...<F'/....."#.D..B.sB.A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....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):	522
Entropy (8bit):	5.588792797062588
Encrypted:	false
SSDEEP:	12:V9zH47W9PQ5/P9zZ1xU9PQxn9zPxi9PQ:XzHL9PQhFzZvU9PQLzJi9PQ
MD5:	C91CA85B49D248FF9BEA00A1FA51299C
SHA1:	DFBD50642CE4C8FF4001943DAE302EBCE1A1A3D4
SHA-256:	84FBCFF90D657F35F57B3598C1AB81752DCD452393EEC275ED393E20585AB2CA
SHA-512:	E8E1A26DCC852BA103168E29CC7040E8AE67DB31226B8D64A114515852F4ECFFB46EAB0AC553254F4BD687FF6A9C485426AA59EA7559C1FC09748408B35BDF9F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .h7.<F'/....."#.D.fz.sB.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....f0.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..On<F'/....."#.Dvn..sB.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....N0.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ....<F'/....."#.D.:..sB.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....C.+Y.....

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):	738
Entropy (8bit):	5.590323436483168
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFICefYlUo6jXLsyeRVFAFjVFAFQkdJ/tTLqYlUo6jB7yeRVFAFjf:tB4v4ICAYSB0B4v4xvp2YSBBFB4v4jB2
MD5:	A48E698C3FF9DA47EB75F8503A0844B5
SHA1:	A841D68870D328EF549E4E32FE495120E003054B
SHA-256:	7E2A9A5CD1B5F6190B307B8639B5C82EB62BCE103BEA6E659879CF310E70E9FE
SHA-512:	D242404C8083AD5DD87CFC3D14D0582FFD297E9B62BCEDEB08075730CF9AE324C89CFC48E91D1F784B1821C742C36BA0A2C75DF2A2E7AF8051E8CCD8FE9B40F
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 ..y.<F'/....."#.D)...sB.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....W.W.....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.<F'/....."#.D.?u.sB.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...<F'/....."#.D4.@.sB.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....j.n.....

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):	464
Entropy (8bit):	5.6880734940577025
Encrypted:	false
SSDEEP:	12:IbRkiDOjbIZLWussCQbRkiDU0kjLWuss:OpDOjmNbpDJkjN
MD5:	71BA03EBC73862E6409560AAE64F5084
SHA1:	F789ED29F605E8CFA96A5062E6F4E355A917E819
SHA-256:	915A0F27D986958DF26CADF9446F9500304CF45D8620B185B30E6DCA7E05E610
SHA-512:	68B3340B019578524949696C379A99C103EFA0634EE9DB8900327CD87339C24E7CC0741A5EA44A6D9B87E25A4AFC8F5D8A9A6E1C7146D624CD7E5E5683D06CC
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 .].&<F'/....."#.D....sB.A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....I^.....0\r..m.....h....'...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .JB.<F'/....."#.D....sB.A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....O.6.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.573490671546765
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVue/ou1Vyh9PT41TK6tvO:pyixRuYx1V41TE1O
MD5:	1E252954D8D7BBD096CB0D4503FB4223
SHA1:	1461E24582A1F1015EDD5FD5270920D8E3BC412C
SHA-256:	B654AC6C0E1FAB5FBB61CC446C5C3B6716DA234DAFD266D4B4F30F76D0ECD7DE
SHA-512:	540D9D7DBDE74349BB3D715F17B0D5D2BD726BEE15A183EE49BBED2C9271FD3C29699AB063A0F78609AAB12E94D948CA8029388C05EB719184127B35C9B7281
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....<F'/....."#.D.dA.sB.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo.....fV.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Size (bytes):	216
Entropy (8bit):	5.630538741006959
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQ1kK/l/0aKGLZIl6P41TK6ti:0RhkqJjpLZCY
MD5:	CC6BE06BB35A7F0B2702BA157334A2A3
SHA1:	98980D0FA82831DECCEA39C604E5D7BA282CA349
SHA-256:	C45A2FCB62798326C3533B0AA81CFEF9B86712BBB211475377E2FBEC83EB1613
SHA-512:	B85F91735FD0F62D5F7432FC09004C722E846EA4D01C01E6422304FEC8D393D1B993E9572C7A1B3ABD1899404F0E50B948E1C88B0C990824F26F99E8B4B91668
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .^..<F'/....."#.D..).sB.A.].>....uUf..N...k.....c..l.A..Eo.....A ..Eo.....3.....

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):	5.522102780025063
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVdH/SwpEwcyxMtv9EWm1TK5kt:mJYOFLvEWdGQRQOdQSH/Sa96g1TK6t
MD5:	5E04FB87131A82350CE827E995917637
SHA1:	DCF98C0CEF9AB8A65D96A10B31408D041F3839C7
SHA-256:	74899002F23C16632AD33C1BEB31BCE2C9779AE8D9185FC90606E77CE0C5A244
SHA-512:	2CA466C89D98FCE18CF0782F7364991AA1570B572F05E6B18DE3B6D3551328340128107F1DDD220C5DE6418BB75565B34959B68CEE146C6F7EA6AF0D2D298833
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .)..<F'/....."#.D.A.sB.A..c..y/L....|y.n..C/l.....X7-ne.A..Eo.....A..Eo. .....1v.....

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):	5.603142076678274
Encrypted:	false
SSDEEP:	12:Z5MyX4IMuR/EQh5MMbvLMuR/E1Nr5Mg7bLMuR/E:ZSWCuR/EeSMsuR/EnrSSMuR/E
MD5:	54D7B47FF3A3DC313FB4DD78BD9322F6
SHA1:	BE49C8988DD55CB9F2FA0D3CF351DA38EFA80B6F
SHA-256:	7F61FB24DDA21E509B0069CBFB328D1A485AC8761AAEC359CF218ABA859399AC
SHA-512:	6EFD131F982438F6F91AC1F59CE920CB07BA57DFC95BD1D2A66CF3FFD067976D8F15D6F77B8B79BFFADA3D003E5AC540511428BCA9849D99C3224D6BF9E9F8 5
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ....<F'/....."#.D.z.sB.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....6.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..gn<F'/....."#.D-. .sB.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....)y.....0\r..m.....3....<lb... ._keyhttps://rna-resource.acrobat.com/base_uris.js ..<F'/....."#.D.Y..sB.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....n=.....

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):	5.522723388094498
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuol/4Yby0zBUKSAA1TK6tIH:pRht4YbeW
MD5:	CE7CD70B8717B826F37AA850B22962CA
SHA1:	F91D6B304D477D2F6BCDD63F1DFC2E5B9D99D89A
SHA-256:	22AC4FB657348AC1FDDA70C36E134505D4AAAC8957D79EDC5D0CC24B5AB9D31D
SHA-512:	85CF3519BC18A8C2FFC6C459530EB91CF54FA0C0C3D0528D4A040456BB293FC1CC7A2B9FA697D58AE00F49555C59969B740E2D573E9D6593A900A1F7A4D83B7
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..>.<F'/....."#.D..@.sB.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....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):	531
Entropy (8bit):	5.568035854717068
Encrypted:	false
SSDEEP:	12:KkXxKMSCvx/tUlH4kXxKMSCvG8tUlvkXxKMSCvPktUl:KkXxiCRWYkXxiCRWvkXxiCkW
MD5:	88A28501A0ADEC78830858E86B856523
SHA1:	24D524340CCB536C258EF754A2A70A8487FD6DF6
SHA-256:	4BC29E0EC8C43E9AEF34D00CA8842D89C104B990611460E3F512CF41EF202E38
SHA-512:	A69C73C85F6D713F006B57B8831FA68DD6C1AFF11830E46F812077901E6D6DD81A1C3C99AD583D6CE70045F931CE677428F19AD4955CA927357EBE62DBAEFC8
Malicious:	false
Preview:	0\r..m.....1.....5..._keyhttps://rna-resource.acrobat.com/plugins.js ....<F'/....."#.D..z.sB.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....rf.....0\r..m.....1.....5... ._keyhttps://rna-resource.acrobat.com/plugins.js ..Qn<F'/....."#.Dd...sB.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....i.dG.....0\r..m.....1.....5..._keyhttps:// rna-resource.acrobat.com/plugins.js .k..<F'/....."#.D.O..sB.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....v.i.....

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):	561
Entropy (8bit):	5.615352347649131
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLPl/1nW8yM+VY1TK6tXakl9YOFLvEWsfOLTeF/DYryM+VY1TK1:5h6OLPtMk91h6OLSNDdkAh6OLiHkkhY
MD5:	104A0E14339D6512E7A9040684F17EBA
SHA1:	E8CEA19DB49D817E1FE16229CFB06278298C815B
SHA-256:	B1ADEAFB87688C58049AA1F750A6E22F32C58AC4F0A3C490AF3B00A2FB8C3EF1
SHA-512:	006A2BB3E410AEAB1D478A490D7773516863D47BB1C73D5F14ED84BB218DA36F89294688A9CED935F19340BCE29A6C693BDEC967153A94E4714A815B2E8574B
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....<F'/....."#.D.B..sB.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ..{<F'/....."#.Da.Y.sB.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....^.{.....0\r..m.....;...I....._keyhtt ps://rna-resource.acrobat.com/static/js/desktop.js ....<F'/....."#.D....sB.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....JF4C.....

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):	732
Entropy (8bit):	5.630201971884375
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFaeYwSeKaTLn7RVFAFjVFAFJaIwSeKaTLnXRVFAFjVFAF1XcYwSeKF:UB4v4AwzXLn7B4v4YIwzXLnXB4v41twf
MD5:	E2D0A9BEAE6FD53CD93C8FC2B333F6EF
SHA1:	848D2DF3E7533F42352BBE454F49DEE1B86DDB13
SHA-256:	3861129FC70DDD4291B8A12B3C79D4AC9903F84EE1A00A49C8ACD56B423140F2
SHA-512:	3226D31AC0E74A196418D00A91315D5A1D45A3488C3F835FB5C620BA138B5359AFF06D2ECF79923B365926478FB7576E83810EBE2EFCC156466EC291553D7E72
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 ....<F'/....."#.D.z..sB.A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....sef.....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 ....<F'/....."#.D..~.sB.A.....H...{...2./.k`..r4.C. .A..Eo.....A..Eo.....8.....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 .4..<F'/....."#.D.:E.sB.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....E..d.....

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):	5.5159150409414375
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuCGJ/l/PvR11TK6t:BsR2EseeJ/tHP
MD5:	66482B47741587722FDB82D5FDCAF954
SHA1:	F8B9B7A415AE232F08EB5836ADAF59DD6C79EB0D
SHA-256:	62008A55654A69E04FD262EED0DCCA59E48E359865102CD87C5624B41B3A6C48
SHA-512:	360C5BC81F9B8D86C7F14BCCFF675DD53D83E200BB068EF00ED92644ABA8A8038A03A7E807201C2971097627EEE86CDBA3A0869DA0D499526A529226B446A74
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .R..<F'/....."#.D..@.sB.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....5.....

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):	5.596952395032958
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQmrll/tGB7OhKlvA1TK6tc:RbR16/cBJka
MD5:	AB36269753A9291776D67A6A8A234681
SHA1:	AF395C1304D9D4EF6F1F4D8068616A83EA98A491
SHA-256:	CB8D04ED232932242F9E59EDAD398283202B29A81DFF5D7DC598D54FBFC5FE48
SHA-512:	9356E7044F113F20AA6BFA5EFD2594FA7B07F4EE3279778E8E331D07DBC210277731511846063D1349B181E1679F6FD70AE447CBCD0895AAB1949DA47980E7CA
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ....<F'/....."#.D)x).sB.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....4/.....

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):	5.58573399788864
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuAgl/TLQdFt1TK6tl:B2geRHRQTgtP0
MD5:	337F4551AD4796024811102F3B02E40B
SHA1:	1762AC6C82189FA8DE19F941FEBF88C728967E2C
SHA-256:	8CD713C5D51C2B8591206E58C005F8EBBA84C3E3FB45B08FC54D4E06C98BD6D3
SHA-512:	DE1F57279B8F18E3B6583A6D9AE1F7DC4407AC40A6531EC8BF75921E30E68ACCECEE656BE30ED6640D0EA4157DCB36E9C713F5F1784A639A3B1E5155F5A47DD6
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ....<F'/....."#.DH.@.sB.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.635771960194467
Encrypted:	false
SSDEEP:	12:WyeRlQBRt1wuMyeRl3S4At1w6yeRl6PIRt1wH:WJeRfwuMJ6Xfw6JigRfw
MD5:	D98D4BD3053286FA6D540EA158F135BF
SHA1:	0750AB12878C313F8998E83B9903151ACEDBE8A2
SHA-256:	F290C485E3C3FA0830F24711A15223EDE68B46CAAC856A2D21332F5CA8EE5C50
SHA-512:	F6E351A5681C8D10B8C4D26837148115C90BE21F63CCC692D7DA955D0C099B0AA25BDA3431423CD815711399E74EA4DE4E53ECDF5050C16CF09589E43B7E217
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .n..<F'/....."#.D....sB.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 .Qa~<F'/....."#.D..b.sB.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....XW.c.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .[..<F'/....."#.D..!.sB.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....D.....

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):	5.586404588278233
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvQSH/EMN9JyNqww6U+5m1TK5ktm31:mnYOFLvEWdhwyuN/BIqwK+41TK6tm3
MD5:	DA656468B51AB2FDE2AA19F66428B652
SHA1:	84E666AB4957F029671E0AE5F6544CFFA52331EF

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
SHA-256:	7DE9372B0125AD030115DD7C886EA06B9E968A9C4A7C1DDBD85A88E735098E86
SHA-512:	02AD108704C02AD6D378B9978B3B198A11B0B51D535DAB26F09F849BE33B039F4AF89BF77A88950D5294F41CCCEDD65A9945D913E6E76B736E5937A563781CF
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .5..<F'/....."#.D.L).sB.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	690
Entropy (8bit):	5.576530453009646
Encrypted:	false
SSDEEP:	12:/RrROk/HjrfLESRrROk/ZZDufLEzRrROk/XTfLEl:/PJ/Dr4SPJ/Zxu4zPJ/j4
MD5:	4461DDDC0E2E460D74A120971C6BF5B0
SHA1:	349FEE48A87F6CA86E052B74CBE6A4EFC9E95E5A
SHA-256:	879F80E29CADAFC74A8F911BB2725C9F8A99F932494457273DE57BF5E249394C
SHA-512:	A9D20EDE1DE60B5351BC3F4317CB53454DD795194D949071EC97AC1D589B4988CD6F37E2738058FED8AEF19AB583B2F09BA3E99FA02064EEE38B6B74D868C8 C
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .^..<F'/....."#.D...sB.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....<~.-.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..'~<F'/....."#.D..b.sB.A..~. .rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....es.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/sele ctor.js ....<F'/....."#.D.t!.sB.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....Jf.....

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):	558
Entropy (8bit):	5.625788624623151
Encrypted:	false
SSDEEP:	12:xqTCtmCPLnsqTh7eL5CPLnVrqTMfQ5CPLn:AGoMnDiMnVuv5Mn
MD5:	6988E4A2906A49AA3303CFBE23FE02C7
SHA1:	433A5DFA36AA384679AD6A9098F425E41986E07A
SHA-256:	7E6C948EE07804D357AED084FB1AAD2462EEA1B717B1BCDDD1415807068DA485
SHA-512:	CA169D7E12BF869B43670BB7F01845EF9A03C49D407A59D66D1EF8C72AAD427F5F98FE40BBEC13ADB8F0B15D508B44EED642AE56EFB547058DF60B6D35557F 6
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....<F'/....."#.D...sB.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....}3.k.....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..~{<F'/....."#.D4.Y.sB.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....{Vz3.....0\r..m.....:....f. ....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....<F'/....."#.D{...sB.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....Z$.....

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):	621
Entropy (8bit):	5.601367285637151
Encrypted:	false
SSDEEP:	12:zRMmkLsDOfjRMWQ9tOLsDxeRMoatvLsD:zzDObezDxefD
MD5:	FE7EE665D0FF5ED1FBC95F5FB8605CE8
SHA1:	4367CCE85588D91A1A5758A0B9641D1A8C03245D
SHA-256:	E6C2B46555F8CF1CD02DB4ABF40A0F6A1EEE54AB6B26A69E576079FC932928EA
SHA-512:	A4067220D0E05062D1E6DACC67BF6494A63D27AD275C1BBBBB4EEC7E488C6F78E17928C8CE3096D70009B6DD05D4DA7A8552252DCAFEECBDAF9D5A66285A5 CCE
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .c..<F'/....."#.D.Q..sB.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo... ....x.%.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..a.<F'/....."#.D..u.sB.A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....rj.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...<F'/....."#.Db-A.sB.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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.619228466218923
Encrypted:	false
SSDEEP:	12:6lJRbNzFoMVlJRhtV+FoMQlJR0tuP2FoM:YVFFoMxH+FoMmPP2FoM
MD5:	CC45D338885CC922CD4DFE9FCBC06934
SHA1:	F2AD2277ACB0006F3EB0F3CB2231433EAC06EA67
SHA-256:	8D3CAC93D22CE01242B0F71BCA34F55EF35FCF04C577FB1FAFAA4F3CDC2EDBB2
SHA-512:	1E9226C5D887DA776C812D16BA554A488EB0F602FE090BA451336617471C7B0DD9B14FE6D7A1E69443180E35386A3994F8F7B7AFD6D808EE5A97F5C5CC8F884
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .;w.<F'/....."#.Dhz..sB.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo..... .....0\r..m.....R....\|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..d.<F'/....."#.D2"u.sB.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo..... .....A..Eo.....b.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ...<F'/....."#.DxBA.sB.Ac}.H7M=M..-.....Ix..R.l.. .}Rl.$q.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.601174550967074
Encrypted:	false
SSDEEP:	12:F8hRrROk/UWe2w8hRrROk/4vXmgqe2qA/8hRrROk/2Rce2:UPJ/y25PJ/MR2qfPJ/cn2
MD5:	53F53E99C43DB1234A696941AA575BAB
SHA1:	E6E1062949F321DAAA5D648A83E383CE15D50BED
SHA-256:	81343054CF3F6050A1B57731CE3A0E0299DC6C445FCEC09EAC654887D6E8025E
SHA-512:	6E4CC41BDCFF17734C6EC22C1B1E5C43B706DA04D4924B9947DEF731B65E3329615440A47FC39FA8638F9D799400662D9633972B951E6BD3189ED961FC8EABE
Malicious:	false
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....<F'/....."#.D...sB.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 ..$~<F'/....."#.D..b.sB.A..%.k.SZ..~W.....:) 'B..ad.....A..Eo.....A..Eo.....HQ~.....0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .&..<F'/....." #.D.f!.sB.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....3.E.....

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):	639
Entropy (8bit):	5.697334298001777
Encrypted:	false
SSDEEP:	12:ehRcIerNJIC4IhRcdXfXrNJICYIlhRcaenYrNJIC:ehmJIC4IhehJICYuh/JIC
MD5:	A26AC369C79C8BDA90DD31A8DEC1A9C6
SHA1:	5F1ED2FC3435931E2A1931E3CCA6C39475D9AC77
SHA-256:	5C921ACAAEA36B73954EF3804D2726FD375D8EF236BA1F4B6D19921AC81B4F46
SHA-512:	23C510CC29D85C2C5E12B8BDE7F74D086714656D2315DF64046DD18A1742983B3AFD495C4CA4F845BC7DFDB34AB9A743A3509515693D1E3FC8AB9AC57C8EC4 8
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....<F'/....."#.D....sB.A.;''./N_.,.:C..2....9L.H...3:...A..Eo.....A. .Eo.....g.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..j~<F'/....."#.D1.c.sB.A.;''./N_.,.:C..2....9L.H...3:...A..Eo .....A..Eo.....vY3g.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....<F'/....."#.D..!.sB.A.;''./N_.,.:C..2 ....9L.H...3:...A..Eo.....A..Eo.....Z2.w.....

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):	624
Entropy (8bit):	5.600733058978801
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuot/c0eFhLzgm2d/1TK6tG8OEYOFLvEWdrIhuss/XhhLzgm2dB:0RWk7Re4SRCMX3ReKcRnNGRe
MD5:	7ADD62E888F8DC9FE7CF55037D0DE116
SHA1:	2EB06B3B1EB239FC30A4EA5173CF50C5FA08E11E
SHA-256:	A63A265EEDA8514EBFAFE8E81B20A827FE91553CB7504075C7599E98672D2CEA
SHA-512:	31CBEA3409435ED6155E34BD3AE2B89ABE9704ABE11E433A577937F3F7F2D36365731F079C610080C0514B4EA08D71D11C0C180B1F805346647EF92649BA416C
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..i.<F'/....."#.D....sB.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.. ....D..C.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...}<F'/....."#.D".a.sB.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 ..<F'/....."#.Dp. .sB.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A ..Eo.....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):	564
Entropy (8bit):	5.638414874503237
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KqKt/tLWhkx56uvp1TK6t92AElVYOFLvEW1KS/uIQFf2kx56uvb:6JJKqep3KJJKiuIK9+JJK2lwN
MD5:	2625FD9116D6D711D2C860A9254AA7BF
SHA1:	3CBE9DD3D678274BA9696A74DD83871FE2AD0BB6
SHA-256:	69639404BC95D1E2A53A6F67CCA3CCCC1D6A2989A84609D95E0E375EC471F5C6
SHA-512:	27231F0E2A4FB7CDC2AAD8A4BC3496986E197F20E5B4551B74D6BCE44B48C3D72E8B09EB3B6B3DBDC1EC1F7E99EAC9428E211CEA2E47F82D5CE4811E76135A8
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .we.<F'/....."#.D.N..sB.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....K.....0\r ..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...q<F'/....."#.D.-5.sB.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....0\r..m..... <...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....<F'/....."#.D....sB.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....x.....

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):	5.608087085143884
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvusAal/UlyhUDLYtmOZn1TK6tq:xRBJ3tUeDcFZLY
MD5:	3E403BF3D244CBF7A61972A7628BC4CE
SHA1:	D3C371A7D2C30F60265D6028047711D9264098BD
SHA-256:	F1F6BA6BCE5C47CF5BBBAC660F8B8AE7F32C0963534A0940A75C55100827F256
SHA-512:	481F43D2AC82AFE676D48113173530C38B19C625FB6F93C9B39733FB700DAC92539E7136EA4E3E712AB227163746364464F0FB0FAF095C6614C721AACFAA6993
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...<F'/....."#.D..A.sB.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....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):	633
Entropy (8bit):	5.63363288444617
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7pvF/K9RVPu1TK6tssRPYOFLvEWIa7zp71kKl//MVPu1TK6G:BPH/FK9RcBPH/kK1McAPHbagpEc
MD5:	771EDD31E4F440B11F5B0100A4BF45A2
SHA1:	3563112FBFA728572A8BA387D23EFE4C20710DC8
SHA-256:	2220214C340FCB04CEA4FC9448C6423304A79D8BB4DF156E9BA5979B62DCB3D3
SHA-512:	73778F34FDC03BB50F7C428867ECEE06CD487484678ADF6344EDE72416E848B32A6057D70BF089E3068C15FC64E5AEBE8BA37361BC7456D4E2E70C1B0A3C354
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....<F'/....."#.D..{.sB.A...L...Im.@.....E.nW...IP..A..Eo.....A..E o.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .pin<F'/....."#.D,F!.sB.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 ...<F'/....."#.D....sB.A...L...Im.@.....E.nW. ..IP..A..Eo.....A..Eo.....E.|.....

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):	5.586438294874944
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
SSDEEP:	6:mKPYOFLvEWdENU9Qol/HMiM3Y1TK6tOQ:bJRT93HMr0gQ
MD5:	3B2E124CCCB0D0542B1BB7A492E42D0D
SHA1:	DF1E763BA5547D31EA6C9247EEC2CBFC5702CB8A
SHA-256:	D6D083B688175A559B0C3CD15A869861D46774355F0D0A5B2B29720A8B392E4B
SHA-512:	DEDE130124577B3069298C6832A8322F8F66046ECE667E2CABC7789A13BA4A373E6DB9F0B5B0A61EBA44A1723733BE9F95A058DC038BFBEF1424D64B148EE3D E
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ....<F'/....."#.DM.,.sB.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... ....A..Eo.....*..5.....

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):	5.558767027520876
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ7Zv//LUjBRCh/41TK6tW:XRc9y9XLUDi/Eo
MD5:	EB378D01055529351F61F3B00F11C853
SHA1:	A99444C6B209CD6FF1A395F8731BC9B03C1F2EDC
SHA-256:	2488DF4D63786F6EECA3F86B73BBDB3078D9652723496C712FAEC4CF68B49F0E
SHA-512:	A941F984C1E0BC7EF09FA884F157D3AFA82DBB5FE86CED5E63A9206E241D6A1215F48EE55167416638FE82545642E313F45C9E6186EF724EAD9B60EB3B3806C4
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ....<F'/....."#.D8.J.sB.APJm...0x.x..RD...BB!@5..<..]....A..Eo..... ....A..Eo.....g.....

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):	462
Entropy (8bit):	5.605580839692195
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu2/Rkn10ULlF4r1TK6trf2qs6XYOFLvEWdFCi5mhuGHlo:bs6xRkiMCZLlF4nNs6xRkigULlF4ny
MD5:	513CBDD13A36F37BC54836EE29E3E850
SHA1:	DC8AC0902E9B14055D9B9DC8DF47D2CABE0957B6
SHA-256:	7A497B33487DC5C3B26BB69AF96984C91829711BA991681F1175A4907A8404D2
SHA-512:	A9D251EFE2F50F766768578D8462E40A2CEFD4E3DEF60F75FBE54C3328AF33B52B96BCDCB30AF830D84C59AC83BED961DD6A51D456DC52DE3377B8A6F3DF6 9A
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...<F'/....."#.D0...sB.A.P...#4..l....5...5..).w.. .h. ~..A..Eo.....A..Eo.....W3.Q.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .m.~<F'/....." #.D.9e.sB.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....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):	5.5312597217325195
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvqK/l/dYkCh8rcu1isLK5m1TK5kp:mhYOFLvEWd/aFuQal/a1941TK6tfl
MD5:	2D962F1A48CEDC40667AEE532D69D87F
SHA1:	A3A16F18031A3DF7CB212859319E82318657F340
SHA-256:	0FC523EF7692B63BD49A7D8E4351F010EE3FF1D838F9375823D462F15212CC04
SHA-512:	6DF57C4AB670A4E6B6D0CAAAE66200DAAD5B66F7FDE9BE212E3BCE0CCC22FE58776A39A8A950C4A619739E152350D318B61592674B30BB8E76415C93251A69 8
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .gT.<F'/....."#.D..@.sB.A...a.f.m.i.o.p..3U5.....^...I.A..Eo..... .....A..Eo.....Y.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.5408438328989815
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQzl/SBhBoBMqVd3G4K41TK6tc:2DRuR6tSmB9Vd2kK
MD5:	6828BABCE1D5280B5A20A680326CA7DD
SHA1:	B490143F2428164515AB5B9416B9BD0BE233935E
SHA-256:	2E1C253B6D759809C9A80D04464081FF681D20750630976109116F62FE18F206
SHA-512:	C7470C46F86DD2D3894CF6080BE860085C4B3C0F410C11C070A4E026144DA89D8D773CEC14FD94E2B5F55E20E0C94ADDFCE88661E8241BAA00B4C0027E5F61B
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..(.<F'/....."#.D.l@.sB.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....qZO.....

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):	624
Entropy (8bit):	5.6140269328726955
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QmF/dVuA424r1TK6tYl2kqYOFLvEWd8CAd9QgF//sktuA42B:+RQDNmrn+lORQ9NirnY2RQ9tcGGhrnS
MD5:	52D14A7C9AFDD89BCBFDEC308061CD81
SHA1:	24D0AD5DAA7DAD3EAA31B6DD20CE5C5B34690C31
SHA-256:	BDBBDF29FF649A4C79B9E6455DF813EF8352F41A69422DE8885AC8E37814DDCF
SHA-512:	C751CD08827D515F22D51F4B8EDB78F193DF32B68B16ABA1F88F9350B92DD2BE49D039DC41FDDB8A5FB8F9179C9F7310A2B8E8DC9D3E7D876B73EF29280AF11
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..}.<F'/....."#.D.D..sB.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....y.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....<F'/....."#.DM.y.sB.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 .$..<F'/....."#.D|.C.sB.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....w.ey.....

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):	5.527441119512295
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuM/fCgYAyC8n1TK6t+/l:xhRTOqC7Qol
MD5:	164186C50A46BA9050FBE394A7988D3E
SHA1:	B88577BC1630C27618C73FCD5AD6BA33032DFDA2
SHA-256:	83D6B4A95F25E0BABAEECE57E1BD2BA11B7EA4982D6D08B296D84F6C9F5F5BD5
SHA-512:	379D747F989E640267F3495DE03890FD8D3A7E6139AC204E95BECCD88EA9285928E1D42CC20EEDD5B168D8F6991F7C5BE470C4EF8D0CFE84FB87A9E1BC78CA4
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .D..<F'/....."#.D.7).sB.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....c.....

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):	663
Entropy (8bit):	5.652937091839928
Encrypted:	false
SSDEEP:	12:nRrROk/VtaMmtRrROk/VxXgm2RrROk/VIk+mUl:nPJ/otPJ/d2PJ/3
MD5:	B36B994F5EB92B636CB7D909D3A96792
SHA1:	37D7ADCC8B722BBAB562B7E31DCB0B319906A422
SHA-256:	B020B2538FFABB3577A4BF0BC6A82AC6F07535C0335DA32BFF7F180A3DFA2F4F
SHA-512:	668A336165B16DC361A00814613B16EC798FD626AB030A02E93F4BDA8C01E3832E13183969F9AC9274E678066CB8F29093CB6FC35A4A7775ADF9E22C667110BF
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ....<F'/....."#.D.)..sB.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....Kd.F.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..l~<F'/....."#.DT.c.sB.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....9.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .H..<F'/....."#.DW?".sB.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....n.....

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):	5.5515427218033
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuWl/0+Adm9741TK6tF:qxRcwthAdu7E
MD5:	B01DAAF3D8CE54FEE6E547097663EF1F
SHA1:	808425B260D2F6193DC776829223F8D14DBEE538
SHA-256:	9D3F6E931E0A7C714F14957233329E62977300257B4D74A40E89BEC1C4B66FBC
SHA-512:	00ECD4597E3539DDEE6AE157A8D58A9396E87848A8F450A01C27A704345FC0248CEAE9D8A64B4BD2A24D36783ED98CDD5F1FA1504A8B2682934F03C7093D212
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .~^.<F'/....."#.D..@.sB.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....R.....

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):	5.549825164136099
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvNfvt/vB6shoq+Nem1TK5ktu1:mMOYOFLvEWdwAPVunfvt/sJn1TK6tu
MD5:	7B799798C5263412650BAB85A3DF1CDD
SHA1:	132D7433218A6C92DD6AC29FD5BD14DE835C07D1
SHA-256:	6A11C3556D5B48E8CB879EB0EEE92F6D84FCFE6E7CF723D84478D8AB1184AB39
SHA-512:	A14CAF5163771ECD83391CA3079C21C6BFC1B4D8066719DF2D8B735FE81BB845E9B09FA0DF3951922950F8C8989F3E4CE91DC45DE4EE6903E7E00D6F2C23DA4
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ....<F'/....."#.DL.).sB.A.....k....F..D..O.n;[.1m.....=..A..Eo.....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):	5.652964366632491
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQTt/4QaRzhcsBXIh1TK6t:mxRBJQ21YRDB0
MD5:	1273821F51EBA7D5A4167ABD5177705B
SHA1:	AD0A5F7064C25A4791EA5EF7112B59B9D4245C4F
SHA-256:	7FFD4A3B8941F289AA31EB7418D67595FA9F9D726A8CD6BD0875671ADF8E0F2A
SHA-512:	8E7337AAEEBEB719F3C3484754EF38FE632C2877366D30AB7F3B77ADD6BB19E94973F0934849D9E4D69897CB9D45A461A9BDF52A91721E4BD8D0E68FBF55D796
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .F..<F'/....."#.D..?.sB.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....R%.....

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):	684
Entropy (8bit):	5.603610008346174
Encrypted:	false
SSDEEP:	12:3RrROk/sevcCRrROk/s37cwfRrROk/swBcr:3PJ/gCPJ/H4PJ/w
MD5:	04DB62823789FA4AC82827AF28179725

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
SHA1:	BB9E613CF75ADE02382EA2E03B0ECF83B423AB03
SHA-256:	1C0BF53CF36353F86C230B149A5EDEE2944FF6A8B31567126D73960E67F10249
SHA-512:	0CAF3C83571AFBDE6610026F81EBCDC68EF0BB7595661B8C956A15FECC4DB129555256CDCBFE4EC8227F45AD16C502A0453FC29096B8FB7A41BFEEF3DFA49727
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....<F'/....."#.DN+..sB.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo...../.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..~<F'/....."#.D.ic.sB.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....k,3.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .x'.<F'/....."#.D.".sB.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:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.101304580999396
Encrypted:	false
SSDEEP:	24:gSPM9uBPMzI3nhFOq0fDwtEzc6cfGmPHyPHbkDyxejN0R:mMPJRF6fDIEzc6cfGmPHyPbkDyxex+
MD5:	B7C4D40EE6649D26A3CBAD3901A3E6EE
SHA1:	214A702BA6DC3F4AC76C646B3E5BBF874EDBDC5A
SHA-256:	6D76CC721E45C4F48793DEDF003ADB60C847396FC05CF9C67616406A48CD8137
SHA-512:	935034AA9B9A7D09435CC52130F61ABD142AE18C4CD035222122D9036D3FCBC93A926C860CD15DAEEEED6F11F8D20A7B99EE0EEBD65CB467BA150CD609A45F2
Malicious:	false
Preview:	......z.oy retne....).....T.....3...._.<F'/.....v...q..._.<F'/.....C..M.....k.....#...(...k.....]...I.@.v<F'/.....<F'/.....6<|.....<F'/.....<...W..J...<F'/.....oB*...<F'/.....a.....<F'/.....;.y~A.._.<F'/.....P....V._.<F'/.....F..=z;.._.<F'/.....o.._.<F'/.....*..._.<F'/.....2q....._.<F'/.....Gy.'.h._.<F'/.....k7A._.<F'/.....:..N.A.._.<F'/.....;/...._.<F'/.....P[. q._.<F'/.....,+..._.#._.<F'/.....J..j...._.<F'/.....MV3..@..<F'/.....@..x.@..<F'/.....*)....J:@..<F'/.....A?.2:..@..<F'/.....&.S....@..<F'/.....q.@..<F'/.....u\]..q@..<F'/.....!...0.o@..<F'/.....*....@..<F'/.....o..k..@..<F'/.....^.~..z.@..<F'/.....[.i..%.@..<F'/.....+.{..'@..<F'/.....D.4.@..<F'/.....=....m..@..<F'/.....+.U.!..V@..<F'/.....

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:	Maple help database
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.101304580999396
Encrypted:	false
SSDEEP:	24:gSPM9uBPMzI3nhFOq0fDwtEzc6cfGmPHyPHbkDyxejN0R:mMPJRF6fDIEzc6cfGmPHyPbkDyxex+
MD5:	B7C4D40EE6649D26A3CBAD3901A3E6EE
SHA1:	214A702BA6DC3F4AC76C646B3E5BBF874EDBDC5A
SHA-256:	6D76CC721E45C4F48793DEDF003ADB60C847396FC05CF9C67616406A48CD8137
SHA-512:	935034AA9B9A7D09435CC52130F61ABD142AE18C4CD035222122D9036D3FCBC93A926C860CD15DAEEEED6F11F8D20A7B99EE0EEBD65CB467BA150CD609A45F2
Malicious:	false
Preview:	......z.oy retne....).....T.....3...._.<F'/.....v...q..._.<F'/.....C..M.....k.....#...(...k.....]...I.@.v<F'/.....<F'/.....6<|.....<F'/.....<...W..J...<F'/.....oB*...<F'/.....a.....<F'/.....;.y~A.._.<F'/.....P....V._.<F'/.....F..=z;.._.<F'/.....o.._.<F'/.....*..._.<F'/.....2q....._.<F'/.....Gy.'.h._.<F'/.....k7A._.<F'/.....:..N.A.._.<F'/.....;/...._.<F'/.....P[. q._.<F'/.....,+..._.#._.<F'/.....J..j...._.<F'/.....MV3..@..<F'/.....@..x.@..<F'/.....*)....J:@..<F'/.....A?.2:..@..<F'/.....&.S....@..<F'/.....q.@..<F'/.....u\]..q@..<F'/.....!...0.o@..<F'/.....*....@..<F'/.....o..k..@..<F'/.....^.~..z.@..<F'/.....[.i..%.@..<F'/.....+.{..'@..<F'/.....D.4.@..<F'/.....=....m..@..<F'/.....+.U.!..V@..<F'/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.1622460750735275
Encrypted:	false
SSDEEP:	6:mgJpVq2Pwkn2nKuAl9OmbnIFUtp1Jh+gZmwP1JXIkwOwkn2nKuAl9OmbjLJ:FJzvYfHAahFUtp1Jhz/P1J45JfHAaSJ
MD5:	7A5819DB72CD769F686CD6049D08AFC4
SHA1:	D0357C40731543D8863426F387A7030B5447F6F4
SHA-256:	DF4E7F6E5E272BCF833CF76D4E504E262819F71FB10C86A9C88896396BC2EEED
SHA-512:	4F0BE11292AD085F83129FE3DF7A40B2456CCE2DAC9178BBE9125B66E6DDC8F891A7DF701E20B6A964FFBBDDBD8FAB7321A06D49B50D96257A3F89B7EBA61033
Malicious:	false
Preview:	2021/08/04-01:21:55.005 680 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/08/04-01:21:55.006 680 Recovering log #3.2021/08/04-01:21:55.007 680 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):	289
Entropy (8bit):	5.1622460750735275
Encrypted:	false
SSDEEP:	6:mgJpVq2Pwkn2nKuAl9OmbnIFUtp1Jh+gZmwP1JXIkwOwkn2nKuAl9OmbjLJ:FJzvYfHAahFUtp1Jhz/P1J45JfHAaSJ
MD5:	7A5819DB72CD769F686CD6049D08AFC4
SHA1:	D0357C40731543D8863426F387A7030B5447F6F4
SHA-256:	DF4E7F6E5E272BCF833CF76D4E504E262819F71FB10C86A9C88896396BC2EEED
SHA-512:	4F0BE11292AD085F83129FE3DF7A40B2456CCE2DAC9178BBE9125B66E6DDC8F891A7DF701E20B6A964FFBBDDBD8FAB7321A06D49B50D96257A3F89B7EBA61C33
Malicious:	false
Preview:	2021/08/04-01:21:55.005 680 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/08/04-01:21:55.006 680 Recovering log #3.2021/08/04-01:21:55.007 680 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):	1310720
Entropy (8bit):	0.008399703044392193
Encrypted:	false
SSDEEP:	24:TmbsmbPXytHwytHwytHwytHwytHwytHwy:TmwmEHRHRHRHRHRHRH
MD5:	05C31564F5D129E37A363E150A042D4D
SHA1:	FA62CA0C75E503D2C5E83FE48A9846CD48FFF480
SHA-256:	64044EF0EAA6C2CCA1F6D5E32B8C1AD305D642A8AF7F91C89CACC2BF8642C5D1
SHA-512:	895CB367D69A3A2D619868DBDA6DA0EB5FFDC20D6B9B2740E7CAE3F9ED91F29BFB9DBA5FA68E72998E92AE68B66BAB551A53B48575B3CD1C27ABE3C923E1FDAA
Malicious:	false
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2108040051582-195.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):	2.7945748953082794
Encrypted:	false
SSDEEP:	768:LPjE4wBV/8VacMOMt6RXly2e6bMjzB0+ReFh:HoYYROMgBsD6oHK+8Fh
MD5:	64FC6EA23EF5DC55CF652DB164628A31
SHA1:	42884BA4B430DC42306191761005661BF1AD3DC6
SHA-256:	979B46F8CBB54FEBA8491196EB01DC73B6A2A023834973B08D701B6F8F40F9D3
SHA-512:	246C5B575DAB75A5D3C616951A2569D07750C77BEF5B393E34751A9FD1103738E54173DA9BCA49EDB610B4381C15DF88D8D4820A6D7EB0A24D1740F2D6DFDFB
Malicious:	false
Preview:	BM.....6...(...u...h..... ....zzz.....zzz.....

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):	3.446988739967349
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CKV49IVXEBodRBkWCg2Oh1CKF49IVXEBodRBkWCg2Oh+:HedRBoedRBAedRBgedRB+
MD5:	8343AA2836ECB833F904C1428E6CE514
SHA1:	E31592D62B7B2FAF0DEC3962D186F7E2F5E8FA3C
SHA-256:	A3C5A02B43C86C5C78CF72C5F5A3881FCC5E1EB0D11A7405B34AFDCAED95A523

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
SHA-512:	A3F49EC7058D7B13AA75F52BFC2466F4A149282D51F0E3C4BB31519B0F915BEE16C9F43AFD5A189454286DB25CB1333F5B0BEBC99B3D3D3FCD11D1EE9A78D4F
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):	3.3147821451298762
Encrypted:	false
SSDEEP:	96:KCgOOhZCPF949IVXEBodRBkhCgOOh1CKVt49IVXEBodRBk2Cg2Oh1CKrd49IVXE+:PiedRB2SedRBJCedRB1yedRBL
MD5:	2207AB020B42D385C3C55D021249162A
SHA1:	52412E3E2120B083DC8A606651EF99B3CAD976B4
SHA-256:	B90BB1F5DDF8B54BBE3CE9491788171289806499 0ECB4A65B2A0C2304DACC8EB
SHA-512:	E497FB985B3A89CEF4BA27AB92693D97EC85A226A174C16F089DA573370C809D9EEF73D07EC6DFEBB24F97000ED7B2CC7BE6880C935CC87A0A84DE4D2538669
Malicious:	false
Preview:	.....W....X.W. L...y.....~.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt19.lst (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6EB8
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\AdobeFnt16.lst.7112	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6EB8
Malicious:	false

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7112	
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):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6EB8
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\Cache\AcroFnt19.lst (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMIzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7112	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMIzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC
Malicious:	false

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7112	
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZHbm3h/6f2WZxAjJxZYEAoUHLQQYyu:J0GpiyVFihHbm3R6f2zYEA/rBK
MD5:	0DFFDDEFF6FC78D54CF34F941951611E
SHA1:	95EFE700D08A72FF68EE4316573309A11CB46C35
SHA-256:	6C8190897870867E5A2FA262652F70592A8EC20EFB728606E941334913A144E8
SHA-512:	2D29E7DB2CD500CF29985BD8E7287155BA42A5D8053AA8DE3B01C5FB2C74B983C61A465D91D34EE3DD8FE19F9C67D535911C1BB00E9B6A4E60A50252CFB339B
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\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):	200
Entropy (8bit):	6.934613832614919
Encrypted:	false
SSDEEP:	3:Nlm3TnZ1PWNmIkP/wkIQOpVou3ms8xKGL8sP8PJJYwfZEmaNAkIiidQPeuWr2DW:wdKinJ+VFWVxvRPAYwfZEmapQHu7W
MD5:	5899D998731A4A9337869D49C04FD8DB
SHA1:	15859C86F73A4F8DFEF2C64F4A9833F02242D893
SHA-256:	A0127D63E20482835F839E787AC3B684BD65EF1FDD1D381810240E3F94876AB6
SHA-512:	2C4010EF24D15FEF70055980FCC4927CF629ADB9A5820D3A0670FF4542F6A39633D3198F2684A2B0A8F319BB315F80E062307419662723D020FD2F6D49BE89F1
Malicious:	false
Preview:	...S.v...:@..hC-.H.QE..|....l.s......0...!.k..'T.U.......epaCp\fw.f+.......U.h3..s..+1.M`-..`.....Y.d.{....C.....I*.....lM..=B.]QV..F...)'....^.2........_CR...Y.....m.C..|......q.?.u.{....X.J..J

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	MS Windows COFF PA-RISC object file
Category:	modified
Size (bytes):	1328
Entropy (8bit):	7.8586600085802205
Encrypted:	false
SSDEEP:	24:FDVDuHh0UDvNs90LbglAUnYn/fVtBUG6/HOKZP2ZWedbpUQK:FDVQh0IseHGRc/TBW/uKUEY2t
MD5:	F4DA58794E43BC05D7FBFB49300A3D25
SHA1:	A089EB6F634C19B95A804EBBDDB8854316DD87AF
SHA-256:	B81A2359D689BF6611E529F93A285E3E1827D07E8953DFA92CDE0F85646136C0
SHA-512:	8374395D425C550F42DDE0FB614B0918BD61FA763B2A94A32FCB8EA913CDC97A8FD6202FE6D5EA01A4204DE5213A1140C91D9639585408C198AF9D8591198C6
Malicious:	false
Preview:	.....J0....^RS.BXQ$i.....e._.=#T.e.Z.<.t"5.y..X..X...Wa.....2...0em-...N.&wK.....L.^.X...s.k.fP...W..<yM..S.....<].tT....v..3h...g...:[W...Z-:.q..D.:e..z..>.8w..z..?....F{.n.. ....rP....T8.f..1..v..v..:O(.....$....J.E.7.!..I...>..,...3.D...{....k%..g.....ye.....5..NY2.5.4...b.....~.VEjx..U.....S....6q.:.RDVJ..0.:LDq..c...}^.....-.U..$-....E.....M.....).i$...'=F_....T^..&.V.U.MX.;.....R..h..o.....6.R...SX.....ER.Q1....<^s.zf.eb...M;..1.....TX.....j.Y.{u.....i..4z\[.q.....#.ZZs.uT..(.h9...r....}.....=.RA....ZF.rc....u..t...0).`n.t).W.C...[$.},aC.6....i...?w&rB{..NH9...5..D.'.....'..!.pB.pw..Ks.O.B.....v..>.....%..G."4)....v0..O....,(~..Ti.B;.e.....4...A;...rB..O.....2..]...W.S..Bu.....b.}...9...].dVER.o....:..j.&..:&.)..."<....8....:...$.6yI....4:W.`.....Vlc....|.c;...:..xR+K.d....4:~..*MVs.%.rO...b.....J..F....H.Rk.o.0..Pi.....<_..C.....*kB".y.L..o....J....^.....H.7..4n..Z..&...o.....pV....r..f.}....

Static File Info

General

File type:	PDF document, version 1.3
Entropy (8bit):	7.86570748230752
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	CUNA-uncashed check.pdf
File size:	253039
MD5:	8bc64f6d8200077dd1b20dcb60e6b07a
SHA1:	6d2cbe3e6fc619376d906f6d4b95eb71b80e0c19
SHA256:	ff391ed81da3dbf1b72b40e0939193af6e9d6a67f1445dd3f3d45f0d2279d89e
SHA512:	6b68c487fba84592c055aff148a8704ac4844bea7b7b43b80a7f8e204ecc92e344de17e133433a484f3532c46b8ea098b53595f8c7f14a2abdc2d520a4da2698
SSDEEP:	6144:ChODCAnBT2t8bciQTbHjUClTEQDpNCvYiafDgI:9DCAB2t3iArZTvIvhI
File Content Preview:	%PDF-1.3.%.....3 0 obj.<< /Filter /FlateDecode /Length 55 >>.stream.x.+T.T(T..H-JN-()M.Q(.....).....k.....y.T.endstream.endobj.1 0 obj.<< /Type /Page /Parent 2 0 R /Resources 4 0 R /Contents 3 0 R /MediaBox [0 0 1332 1722].>>.endobj.4

File Icon

Icon Hash:	74ecccdcd4ccccf0

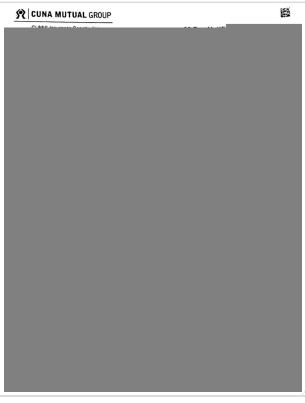
Static PDF Info

General

Header:	%PDF-1.3
Total Entropy:	7.865707
Total Bytes:	253039
Stream Entropy:	7.864289
Stream Bytes:	251745
Entropy outside Streams:	0.000000
Bytes outside Streams:	1294
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Image Streams

ID	DHASH	MD5	Preview
5	737278337f4f39bb	67a41f86893701e25a798ba2366f34d7	

Network Behavior

Network Port Distribution

Network Port Distribution

UDP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 4, 2021 01:22:01.610728979 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: AcroRd32.exe PID: 6992 Parent PID: 5820

General

Start time:	01:21:41
Start date:	04/08/2021
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\CUNA-uncashed check.pdf'
Imagebase:	0x10a0000
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: 7112 Parent PID: 6992

General

Start time:	01:21:42
Start date:	04/08/2021
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\CUNA-uncashed check.pdf'
Imagebase:	0x10a0000
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: 1372 Parent PID: 6992

General

Start time:	01:21:48
Start date:	04/08/2021
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:	0x1150000
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: 6540 Parent PID: 1372

General

Start time:	01:21:51
Start date:	04/08/2021
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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=16643864859160111475 --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=16643864859160111475 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1150000
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: 6336 Parent PID: 1372

General

Start time:	01:21:53
Start date:	04/08/2021
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=1720,6803796534539775004,11392875392024183128,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=8013375785811497341 --mojo-platform-channel-handle=1744 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x1150000
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: 3436 Parent PID: 1372

General

Start time:	01:21:56
Start date:	04/08/2021
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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7474857484354196562 --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=7474857484354196562 --renderer-client-id=4 --mojo-platform-channel-handle=1840 --allow-no-sandbox-job /prefetch:1

Imagebase:	0x1150000
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: 6532 Parent PID: 1372

General

Start time:	01:22:00
Start date:	04/08/2021
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=1720,6803796534539775004,11392875392024183128,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14789584177783671881 --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=14789584177783671881 --renderer-client-id=5 --mojo-platform-channel-handle=1980 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x1150000
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