ID: 882708
Sample Name: Electronic Invoice Print.pdf
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 17:17:59
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

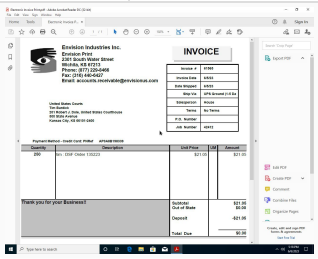
Windows Analysis Report

Electronic Invoice Print.pdf

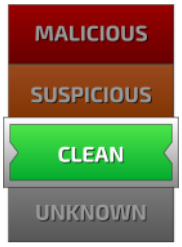
Overview

General Information

Sample Name:	Electronic Invoice Print.pdf
Analysis ID:	882708
MD5:	63dcc6758edd…
SHA1:	9a52ed2a5c8e…
SHA256:	8f30bb76174ce..



Detection

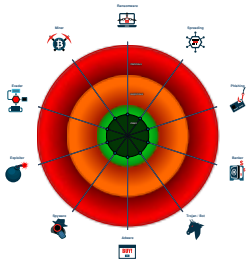


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64_ra**
- AcroRd32.exe (PID: 1484 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Electronic Invoice Print.pdf MD5: 0EAC436587F5A1BEF8AEB2E2381D2405)
  - RdrCEF.exe (PID: 3688 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 4AC861CBCAFA331A72C04BF35AE792E3)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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

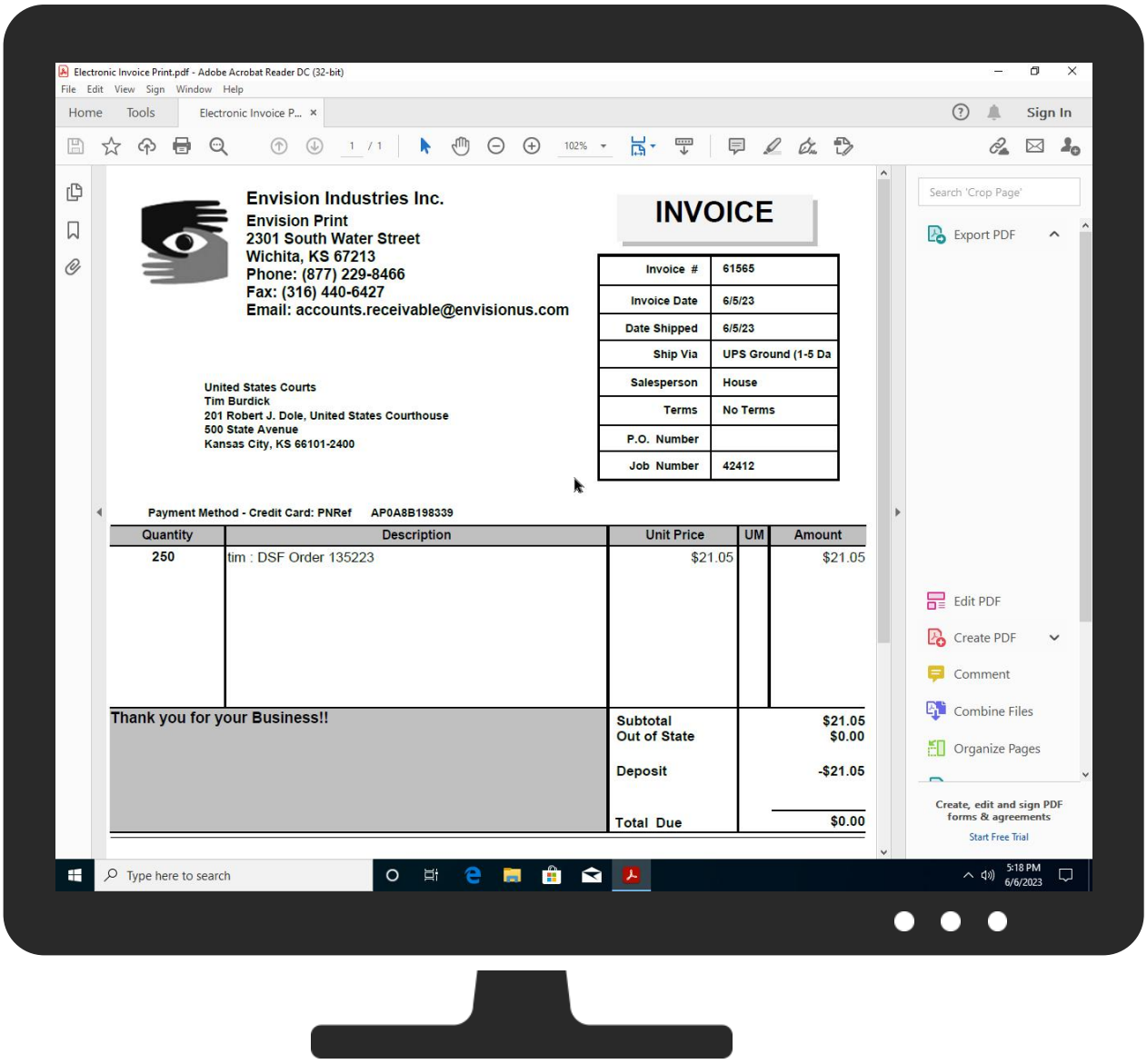
Mitre Att&ck Matrix

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	1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Information Discovery	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	1 Process Injection	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

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

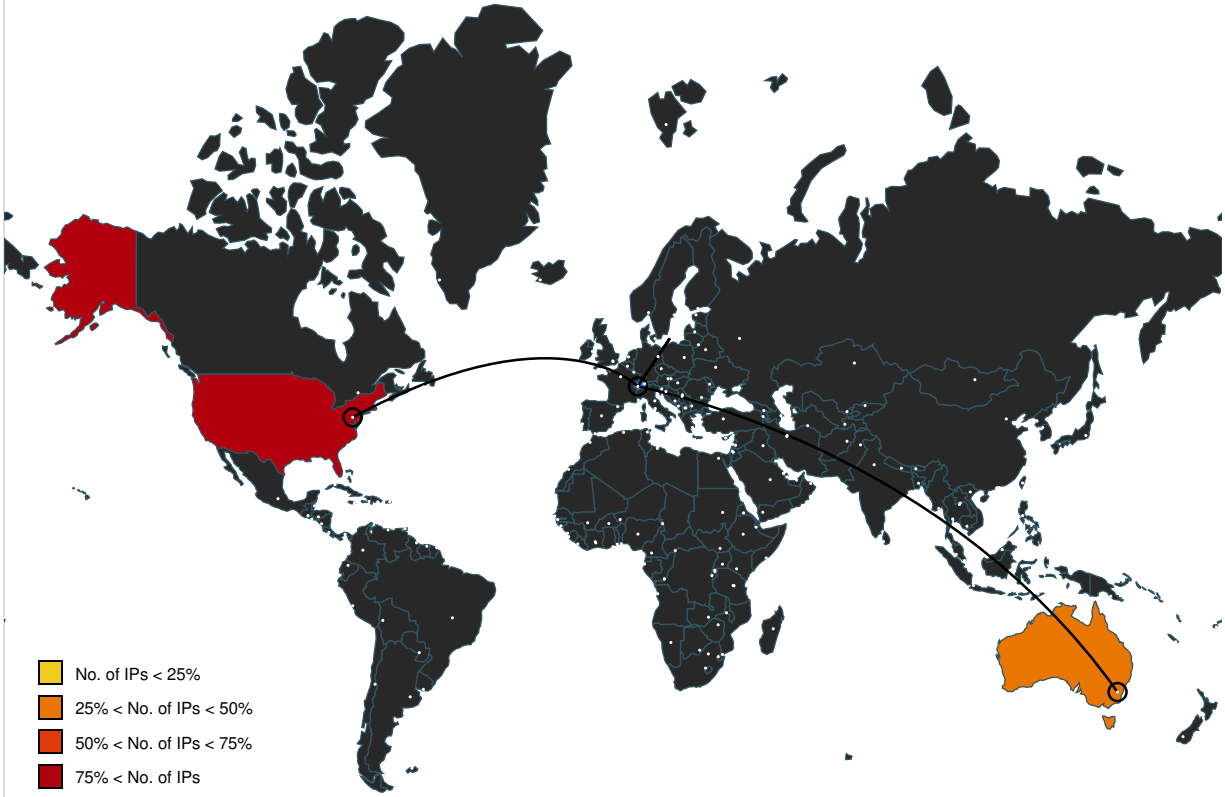
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
9.9.9.9	unknown	United States		19281	QUAD9-AS-1US	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
23.32.184.135	unknown	United States		16625	AKAMAI-ASUS	false
107.22.247.231	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882708
Start date and time:	2023-06-06 17:17:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	Electronic Invoice Print.pdf
Detection:	CLEAN
Classification:	clean0.winPDF@11/65@0/49
Cookbook Comments:	• Found application associated with file extension: .pdf

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.32.184.135, 95.101.148.135, 2.19.126.92, 2.19.126.76, 23.32.212.131, 107.22.247.231, 54.144.73.197, 34.193.227.236, 18.207.85.246, 2.21.22.155, 2.21.22.179
- Excluded domains from analysis (whitelisted): e4578.dscg.akamaiedge.net, ssl.adobe.com.edgekey.net, armmf.adobe.com, login.live.com, ssl-delivery.adobe.com.edgekey.net, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.net, a122.dscd.akamai.net, p13n.adobe.io, geo2.adobe.com, acroipm2.adobe.com
- Report size getting too big, too many NtSetInformationFile calls found.

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):	5.5871411127681405
Encrypted:	false
SSDEEP:	
MD5:	4D8A0F8444F18FE993529D1A6366C9F8
SHA1:	04C892B7FEFE65AF31AC7051944E7BEA2F3B867B
SHA-256:	4A566557666D64826C0D6C69879BDC002C07CE074DA24F3F9236124D24C93513
SHA-512:	30B28C103288D4FB08B2042CEC53CA0B46AFEDA12CB28C2A388079483B203EBFC1CF9EDF09734B7EEE6CA21B77D0C195B94CE30E1FAC6B9AF093C0EAC395DC4C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...n..\/.....*..t....A.A..Eo.....d.{v.^.G...d.W.:...P..k%..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.479464876503879
Encrypted:	false
SSDEEP:	
MD5:	1E0AC7F16CFAE7EF8F2DD181649AA080
SHA1:	867088B1B0C82CE18659AADC451D0B2276C4D356
SHA-256:	24C2BD61530898575B776CF61CB591DF7DF55324C62F98109C4A5B86430ABF43
SHA-512:	CF09589F31E3B27664520EC6CB36E7863DD355BCB6F73718C364B380A7F3598F420AA8EBB891D93FCF7C172528C4D3502A1700BEF2996E42AE717D75FF554803
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ..C^..\/.....*.....A.A..Eo...../. .....1.x.'.vl..*|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):	5.56268805457333
Encrypted:	false
SSDEEP:	
MD5:	6C249123E8E37ABDC667186D59E0BB54
SHA1:	0D314B38BC9F4E8D99EC9A313242DFC1427A7FCA
SHA-256:	6FB1C6A5385A80E01C69C8307D44594F406856B2D151C746A2C66B3B10875FBA
SHA-512:	D942CA26850245851A7B40E19CF29FE3E0B9AB317D4A3AD8C6809D8682704E16B04E0D956EEE3DC556B1731FCC7A290FD768B3E0C531DE1D5CB5406BFD5798B8
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 ..1l..\/.....*.o.....A.A..Eo.....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):	5.6655090945490185
Encrypted:	false
SSDEEP:	
MD5:	1CBEAD89F2B9F2A4E54E69FD7927D528
SHA1:	429D48D7D1604E2E52995A91A9F3A48E8A03F1E6
SHA-256:	F4DCC7BD5A0A55BF9AF02AB9E059B31E4B1017824C36F761353D46257B999F31
SHA-512:	26562E3D55C60348D15AAF40ED08A3109770D677B3B40B420903F7DB5322755362FB25B04D18CFE8C15980B2E0E011703C3C3762E952C6AA10FE0B7A787C7CB4
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 ..ZE..\/.....*.p_0....A.A..Eo.....].....8 P..a...R..Y....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.518868409703817
Encrypted:	false
SSDEEP:	
MD5:	3193AF260126354FDE58BD9F3F12194C
SHA1:	EC2B81E4CBF1C83A2036420B3F81CD9199E19DCB
SHA-256:	31464E24012266CABB660CC3E291F51D8978A7348D7233D3E82FCC69A83D35C2
SHA-512:	3D5380C6F277DE82D5850983F255B0EF0E9E2F163B8AA3F9D10E4DF6A20AD62BD2FAD3FF670F8293BC48078D3A5E99C09857D7358CEF62A44B75A861D3EBB631
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ...m..\/.....*.....A.A..Eo.....jU.....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):	5.610119085258349
Encrypted:	false
SSDEEP:	
MD5:	0D4F012C40C91FE10218889D2E14AF0F
SHA1:	6F409D779B50950B7C8B46337E716224EB519952

SHA-256:	E92BE3A3D05AA38AEF9F65D746D1C3B43D63BCD862D17EF979479974D8408D05
SHA-512:	33CD60387CE1248F1FA400F04B7A0A80F424E8A9E785C3D9451FE0AED5A3E6D46A29ADF52FDAA340C8711274107517D62CC985D58F336D6BCA9E106FF6054DE C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .Swj..\/.....*.<.....A.A..Eo.....].>....uUf..N...k.....c..I.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):	5.516068689456449
Encrypted:	false
SSDEEP:	
MD5:	E2480F17D9D6920A52A10A1801E2A5AD
SHA1:	85B40226979AE2042227AAFE33B29B997B21C95D
SHA-256:	DE019E51100AD8C6476969519362F6F56A25ACB9D6C2CE06B712F74DA20573A2
SHA-512:	617494E3E73DDCA04979DB3CFE31AFB95B70BE7BBB8B19E6334E085354767792E1490C2EF87FECC0943A0A2056A74149888015B87B89D6CF38E4D51504D2102E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..m..\/.....*.M.....A.A..Eo.....k..J.....c..y/L....|y.n..C/l.....X7-ne.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.541105468682616
Encrypted:	false
SSDEEP:	
MD5:	7BD633E1176E20D2DBA0483963583151
SHA1:	0C6E672A275509F5A33D9E65CAD3AC9C087254F4
SHA-256:	A67FB26CAB70AFE9A8957C57F0A2847B8C2CE7F05D24850A30A74FC21C8E0004
SHA-512:	0D9F35FAFD11D018B01546E9C75EFA84A4C977F54F1AF901EFCBBE529BCDC3328B4D8BD14809D48AFAF3B3C0D76950B69463C0A4D595B66D85F66ECD1AEF0 B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..F^..\/.....*.....A.A..Eo.....(../.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\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):	5.503351874050875
Encrypted:	false
SSDEEP:	
MD5:	897A306D09302296870F878E8BF52664
SHA1:	8F6715CA3D038BC48BCB9FCF8C35078495BE756F
SHA-256:	A3CFCEE30E35782B45E4FAA2C66D4DFFEE869D3069453F97B5E16735F31E6830
SHA-512:	592F2306804FF49E28AFD7F885F159DFC862378FF5878DAE9A893C7CA32F92E5642CFEA46C817AF841774A526966BBB4F4A9751FFD43513656F80009671F34BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .}E^..\/.....*.....A.A..Eo.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4ca3cb58378aaa3f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.564849936107878
Encrypted:	false
SSDEEP:	
MD5:	453FE7464AA7EBD0C75419E81DD1EBE6
SHA1:	53A168FFA7C79FD4E1BC6F4BBBEC94681B09B27B
SHA-256:	67074A19F08DF1E54C80D284F0DCBCF907DAADAF831C1B0672336BFF4EFD0213
SHA-512:	227BC305C596579F53F4FBC6FC06356895A03637951671068D6750E45A1EE70BB2875CD79FA38B9C164A866E9AB4F52EC5FF63B42D0CAE72298C8E23E5179827
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...9O....._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/plugin.js ..xj..\/.....*.....A.A..Eo.....).....e.....@-H.>a..o..sh.5.A.x..C..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):	5.588069316582519
Encrypted:	false
SSDEEP:	
MD5:	50D8695DBD888E33481F02A659F83D68
SHA1:	0D83E280348D2976C925348C154CDA7C20940C1B
SHA-256:	F727779F53EFA09A98B00D22AC0A692A9569D0F210F9D3A49463ECF12C60ACD3
SHA-512:	24010FABBC8BA9C380AD8C042B8676234E86DE075DAB1C4D38772A5AD19DD887A8B62F70FC89621D51537E8326219679DCD9B8F036E41299FBCC8D81E1CEF6 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...g..\/.....*.>.....A.A..Eo.....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):	5.598430204460034
Encrypted:	false
SSDEEP:	
MD5:	A7EEB868963C909480889E988107C2DC
SHA1:	021A29B7F4D9CABAB3DDA1DC7849B3B0CA45252D
SHA-256:	AEEAAE06B3A0ADB1BAE0655BAD6DBCF048D7010F21F26D7861DDE662DB2B088D
SHA-512:	9F9D8A2B41C5E8DD391939313B9CB07D691AC81D0EA1C03B1FFD8ED89A5C0627664AA7626BD4426B4736DF979AF99C5CBDD03D60DDBD1E0B941CE5E74FBC C71
Malicious:	false
Reputation:	low
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 ..m..\/.....*.....A.A..Eo.....o.#O... .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\64766d63a539c3ca_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.597927446614784
Encrypted:	false
SSDEEP:	
MD5:	B19B1CA6544D1FF7568AAC98E1541BC0

SHA1:	C82F342D9DF754766F7F2A4B3E7B22A3A32EA13C
SHA-256:	A39E0EFAAF239839B81A4320B4F95A7D4EDF6822CC73EBFE1445077CE6E752C1
SHA-512:	A753B68AF45AA41C5078B47E7494FB7699C9988AAEAD3678202824C99420153E6E9527E2EA06C130A86D300D45B82A47F95B8FEF2911D55F6AF313AF6467FE14
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....."....._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/selector.js ...C..\/.....*.j.(....A.A..Eo.....8U-....a=...`#..VT.k.....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):	5.495888678433462
Encrypted:	false
SSDEEP:	
MD5:	61F637CA4D298E523C9892BC5D023848
SHA1:	2F95FBBA73C5F0607D2DCBA24D0CA997BA56F611
SHA-256:	15C7D928ADE324EEA1F2D933A6EB284C0C8C08673A82C07737B77EE57097E662
SHA-512:	92370EF08AEFC82B51AF0A9AA74AA0B5870B5671DF60F9B70DD86702DB9230E508BE96754AE371A17D5F6214B8587C9A3ED0EC58365D1D1AFDEBB44AC3E2E9 90
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...].....,_keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...m..\/.....*.....A.A..Eo....._.....A.o]@r..Q.....<w.....].n\....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.582291362763104
Encrypted:	false
SSDEEP:	
MD5:	081B34F58D4FAAA9E70DADF7A5094C90
SHA1:	AB4CF77C6BE6CBC9AF2945543597E52133CDB2A7
SHA-256:	9EA82D9EA055BCABFC0802E182B00BB29E5F26038D41369ED7A6DDE737AF2393
SHA-512:	BE8A0612BD3CC8C4B2899CDAFDB6848FA33FAA14FA218D6415AEC6241AE83856D1C582DAF659C87C8F554D34AD2FE15C44ECD97C62D728AC33423DBDF57E 9F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..uj..\/.....*.....A.A..Eo.....m.|y.....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):	5.575186308366446
Encrypted:	false
SSDEEP:	
MD5:	A648FD23E1BA3E4AB92379BC9C3A2130
SHA1:	35263129084F454324CAE7FA9083C162DCA1CB57
SHA-256:	49B23008B5CBB28B3830B5B88FBF7EADA532C2F915F034AE1AF89E33DE85322B
SHA-512:	1D7B91CB74064BB0CDA133E33A95F1BDDFF4C6BAE6C31C4A7E5AF138DB82346518323CD17DCF58FC3558CB459DEBBB601B811EE7C6851EE9639E07CA46FC8 DE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...I..\/.....*.. ....A.A..Eo.....q.61.....@..{o]...9o|..qY....T....{..u.b..A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\72d9f526d2e2e7c8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.578157481721996
Encrypted:	false
SSDEEP:	
MD5:	4B4EC3C9A87A4F5641F990830A2B08ED
SHA1:	DB559F9C15B316F1D36742653DA303267DA9BA79
SHA-256:	E3BA718A329489CF6ED14DA43F499AF85046CDEF70D0F6C215AEB9795777B483
SHA-512:	E4DC5945A86874B8E71692D4CD1D6C6DF3947B9736C1CB0F1F7BC3E044F2310BBA8E21EB13FA278761A5709AFA045382010054A29B1B21E2D4C75974B9D5F85
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.....6....._keyhttps://rna-resource.acrobat.com/static/js/libs/microsoftGraph/microsoft-graph-js-sdk-web.js ...c..\/.....*.U.....A.A..Eo.....Td[<.....-.....5p9o..k#. }..6(..*A...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\78bff3512887b83d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.553265030345373
Encrypted:	false
SSDEEP:	
MD5:	309807505A7E7A398D7E0FC361E0767D
SHA1:	4C192FABDB26C3983DA5021EDBF78CE9EE105139
SHA-256:	F81FAEC5F46F89FE13BC848B427A395071AC130B0724E4625DD9F3093547FBF8
SHA-512:	3100BD55048F8426199D76EE9E47FB35254F0EC1F47D12E1E9538593C5920A35B3CB7831F8A8EE0411E26F494D3E22AD764556B0E2901AFAC73BBF4F358C9DE1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...r.L...._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/selector.js ...j..\/.....*.....A.A..Eo.....U.....&.Y|.. . .&.....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):	5.57245319127076
Encrypted:	false
SSDEEP:	
MD5:	D69FAF22C91EF02AED9F42A3E4577384
SHA1:	35429FD1C8C5497221206591D876379C7EE5A01D
SHA-256:	83AE35C2559F2B54AB0867D156FDCCD13A9BAD850777A262E6E8DCA9DA9B438F
SHA-512:	F10D594750447306B168002740CFEC08936247B94648AA27720890A3A8E90200BC0A3EC5077814C8EBE4F849CB36D62ACF647B457FD2B8C5D77224ED48B8AC6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..Ph..\/.....*.....A.A..Eo.....8..*.....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):	5.567988772738312
Encrypted:	false

SSDEEP:	
MD5:	A221D5A4FE55524BD37BD5F0859877DE
SHA1:	B11661269C3C3997C8E71F09338877A719334085
SHA-256:	8DBA801AF58722F5138B1728F6587720753581663391 8AA18D284E8BF9304407
SHA-512:	CB85B768495109E738684A24A7F2F10D979FE01A4D7B7F03C5B07BC5253C03F27A4961892237490736AE307F3B3E7E5FB090D3D7A2D06B2F7811D8E1134948A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...j..\/.....*..'....A.A..Eo.....J;.....7...o..a=.98l.....(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):	5.591002593953976
Encrypted:	false
SSDEEP:	
MD5:	6E98F8FC573D5B34E50EA9BB80F096AC
SHA1:	1959AD9B3B05358FAD44F4FA1DA1665213B026DD
SHA-256:	2556F3FAEF60BBF10F54BA3FDF016C969565B7064383A731A0989A59EA35F50F
SHA-512:	FCAE24096E9B00453A7D788D1BBA8318C9661358855CE78D268D6AC4A80CD9444C4CFB0A8EEC38A9FC8AC14482A4A132EB4A0350BF4D02D8712B13C371A18E 8C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..@h..\/.....*.....A.A..Eo.....3.....~..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):	5.588810987211443
Encrypted:	false
SSDEEP:	
MD5:	953F342B7AC296AAFCC350FEE55C440D
SHA1:	F5857FF4BA8480BDF2C624722600C8264A55DEE5
SHA-256:	9A0B7D15BA04B88732AA2E586EB32052EFC41447621E956CDD88B47D33B3A9AB
SHA-512:	52E9B38A04C68DE4699E26BFFD995F223E41A13BCF1FE0426784B7B76BD9F0A4A5FC015569C62B731A24AC4311DAFA2C1ADB5DF33786AB017839184E5B3A325 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...g..\/.....*.....A.A..Eo.....~]...%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):	5.609347787281982
Encrypted:	false
SSDEEP:	
MD5:	1825445B96A93E2DC0D69E49F79C710F
SHA1:	B4CE88300D7E1A0269A36741E46EDB09EB1F209C
SHA-256:	2249120BC689B45B1A8C84766DC87EDF2FD34868C7C5D38987CD4AEC10AAD0D0
SHA-512:	BC6502F2708DE8C38B7FC6A20A39E0AB9485E95F4872320E2E3F8004FF4FE6E54F6C54D4C27C57AAF85361811B573302AA3CD408370DEBD6F226387A132194B1
Malicious:	false
Reputation:	low

Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .6*m..\/.....*.....A.A..Eo.....~.n.....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):	5.541048247773875
Encrypted:	false
SSDEEP:	
MD5:	0F7CE394DF92E47B068B45304D805E29
SHA1:	BD5052C656E3B7B6516B7494EED79B106B25DA60
SHA-256:	68D3E187526F82ED67116B1B4828C86898E6555D3565E40C6D2F2C7F69DB5B8D
SHA-512:	766AD2C9136853988FE8239648780419669 9EA1956355B85B1545F9E16C65366BB04505673523349AAD138ADB4FD3EC3D4CB279DBCD8022CF5485E69B05FA30B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..,m..\/.....*.v.....A.A..Eo.....E4w.....c}.H7M=M..-.....Ix..R.I...}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
Size (bytes):	223
Entropy (8bit):	5.548113233205637
Encrypted:	false
SSDEEP:	
MD5:	9E807BF8F17CD5232D94DFC5D0E41586
SHA1:	F7DE97D38219871A35F89486110CD367325511D1
SHA-256:	C6F8C054447536AE67805EEE58F7AA72DB593559072C307DC8C66D12CB75DF83
SHA-512:	82EB84E74653FB630D9EF45F65763AD521DF732B03DED652F33F5BC92F1EBAE7DA35C1293D906943B6CBE36A1569CA1FAC515F6840093E023BA4165ECB013F1 4
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..=h..\/.....*.%A....A.A..Eo.....2.....%.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):	5.678263253038303
Encrypted:	false
SSDEEP:	
MD5:	0A9CB71D21DB65241B49B2AC91D7DCF7
SHA1:	F321737B23B8063C5536A889F05755E7F148AC91
SHA-256:	09B8CB26DCD62B139A98ADF2DAE3EA57E1F6258BB409D1D0833D6E58B7CDFF4C
SHA-512:	F94307C7B3A43D53766274F331A5AD60CCE65BB08E410F77F34145E0562A402D929916C8090CA2400D0E30A2EDEF0542702888058C5B6EB80D8B05F6C535C13A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..qh..\/.....*..z....A.A..Eo.....?.....;"./N_.,.:C..2....9L.H...3:...A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

Size (bytes):	208
Entropy (8bit):	5.519146008366271
Encrypted:	false
SSDEEP:	
MD5:	5518399FD9DEAD0CB04E2AD5F3C1E405
SHA1:	F6409B91B9F75BC8423509E2418623AEC3C90631
SHA-256:	26977DC4F1EB1905488E2EC87C2CD3DFEEED06262D5AFB34B54E1F28F07BA006
SHA-512:	EF8D5789C19469FF4931BC9FF178237A65189BFD17922A19B98DC1A29CFFA5381E532A4CF5B92FF307991277FDBD08395B58DA32EEC48A004B615F14D3F3BAA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .7-h..\/.....*.....A.A..Eo.....021.....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):	5.570390140234784
Encrypted:	false
SSDEEP:	
MD5:	94FC8B44C8A09A7F3D39713CD2B0CCA5
SHA1:	7840AE98B71D90E316881368F1C49DA49C1643B6
SHA-256:	5B719C45B5F13915709CE2B7E3E88327852B19478FA4BAE7B8323559D1F6B463
SHA-512:	FAB9FD5EEC2F6E923B15D21AF26732985AD5ED881E697E4AB70D0095A79278523BCFB0807268F49B130CEE08081601453BC828159E91AB4E1F2E9400E958A055
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .Cl`..\/.....*.0.....A.A..Eo.....K.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.632779666990352
Encrypted:	false
SSDEEP:	
MD5:	7BB1500E2B603741F1FB27BDF4E195CC
SHA1:	C98BC7F4DB1A625349AFF896CD8C7561A5CDFB76
SHA-256:	56D0306122EF5A4D81247A7649397013A471661D53D88F937BA29742FA31B103
SHA-512:	C67EFFA8D04833BC25FD10544F421236269C8EDB809BD28819E7C92480B275E819807DB8639DE3DC61AC732A83B049D40D3BDCC9894B704DE303C04FA110E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...m..\/.....*.9.....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):	5.566370763851544
Encrypted:	false
SSDEEP:	
MD5:	64BD552743A322BB603E79B6048A1900
SHA1:	8A1B6F51304836089B3F9441FA7457480D63EAB2
SHA-256:	55D051EA94DBADAF9B99F90F5F7574C1B7D5C6A88D8E38EA4D9781042F2F93D1
SHA-512:	C3D65382840133698DBF3957D28BC6AED56E375905D7D702B9AE76A5E915AD20548960E72E614BAF6B67106A3E2AB3D5AF35BECA56906C7F30C238312F3BE24 D

Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..P^..\/.....*..j.....A.A..Eo.....o.....L...Im.@.....E.nW...IP..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):	5.627034964733468
Encrypted:	false
SSDEEP:	
MD5:	3D99B5902E784A97DEC14388D34F6104
SHA1:	91905E2955801EB58F4904618BCC3AA09FBBB4CB
SHA-256:	DE285290C719BC0F08CD740DBC8B78FB75D78F43D268E9FD44904A308153F94C
SHA-512:	E626E76E2E8864EBA756200151FCDAED7537183DC6224C1997532BEC07FC454D25C83F9BC97ED43CA12F2D9098FCBB93871D48AE9D85D51DCC76DC741379F2 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...m..\/.....*.....A.A..Eo.....PJm...0x.x..RD...BB!@5..<..]....A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.642799744783458
Encrypted:	false
SSDEEP:	
MD5:	5B845776B2CA53D9C1CE3017E438822A
SHA1:	933F81EEC18E51DDD3F0023AD4C9B33822228262
SHA-256:	25128AC7C2C8E4A325FD0DA9881DAC76F47D8894D052FD61F14872D051E42142
SHA-512:	C7D6DC38D6A7EE8A4D8BA10D425A6618967055C5C90F509C6C61741ABDAD53138D0A351FB04A5F86FCF0614F44A08AD16AF4B05278D7A560A60564F55DA0D7 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..9C..\/.....*...&....A.A..Eo.....`.....P...#4..I....5. ..5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\e58e492b0f04240a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.620034825983163
Encrypted:	false
SSDEEP:	
MD5:	E7AA1C8F8514A5606E29CB43051EE1F7
SHA1:	5DAB3776804CB213913FA51C80D361285A7A9C0A
SHA-256:	D2EECCD1D9987B546F8FC83C9EB35B07328E84A4BAB704A507F673305E5EF897
SHA-512:	0FC397C69BBBAC33104237735D66D9A047681811B58CD1D516CF82988FF04F406394E230BB5F66F5D17ABF7B0D6FBA9D1F67078672930F40B7E255C824A13728
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/plugin.js ...C..\/.....*..&)....A.A..Eo.....`R.....E*).*^.!..C.....G..#.&)A..Y..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):	5.579438164108999
Encrypted:	false
SSDEEP:	
MD5:	DEA4FA2B13919968E53E2164FF0568FB
SHA1:	ED08F73E6EF9E5040FC7C733735B9737A8B8FCB8
SHA-256:	683FE25268F95043334C07C9BEEECE115905CC295AC696F5200EB1768AFFEC76
SHA-512:	C2647D1EEC2B70E0758EAEABEBAD7D4A50C42714EC63E2AC72BFABBAF818E9FE85D953DD0ACCE935A49B6D1208E10A61E4417A1AACA51805056709E881B16E5E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...n..\/.....*.....A.A..Eo.....#..@..k(v.8g..5.~_....]Pj.*..6.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):	5.5502009412905995
Encrypted:	false
SSDEEP:	
MD5:	AEA3D0598F27097CB92CAF9D4C5252E1
SHA1:	E32CC960FDD947A7429E1A26CE72EB5FFDB992B1
SHA-256:	1B99C0199DA7D1D29D0A084ECCDF1131FF825A54AE29727D1457A7CCC55AE375
SHA-512:	5CA093B99AF3DFA1F5F5B16B3E17BD2EF828FB229DC263F99528AEB3592C77B66A6E3E32415952EB9F1BF10672BB115688B41A428ABF61E430B29D4CA98AF5F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..sh..\/.....*._.....A.A..Eo.....5])..... ./.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):	5.577683145080395
Encrypted:	false
SSDEEP:	
MD5:	72BBB3BCC17319C12812FFF6425090C8
SHA1:	1DC77F38FC7BAC36519F6757CFFAE213F8A8E4C7
SHA-256:	7F136F79D4B3BF0A118788F1E4B177739CB6ABF89EC7645C6435BF01C1887932
SHA-512:	94300DAD7A21A2881F5773CAA5008609458DFEBD5FB80C6CC6C1516D8BEB9652797CA59D06993668D4E535003BEFDCA172D4BE3DD2FCCF6AE0AC7D10323BDCB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..2l..\/.....*..J....A.A..Eo.....3.....U...I.>P...X...x..0U.~;m.x.k.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.565924245092688
Encrypted:	false
SSDEEP:	

MD5:	295EFD63B85BA5CA9612C0A0F4FFA81F
SHA1:	92001FFEF5B255783BDE6CC05734290B8B00DE4C
SHA-256:	F8B0F397259A7FA5F5DC9AFC379BA522126BD7F2DE4863D0E4888E5123F7CC7E
SHA-512:	1B0B1DD45508B540044F49A99A9A83FB2539C4A1017327DBCC5234C9697FA51E15D651AC72367CCDEC0E0766C8E619C4458FD86DA03F0E3522B16387CB715CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...j..\/.....*.....A.A..Eo.....k....F..D..O.n;[.1m.....=..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):	5.559621898077909
Encrypted:	false
SSDEEP:	
MD5:	60C7CD5B1334B5F8E52FD8B1F3DA0234
SHA1:	458805845548D1706A327E3949DC71251F7A73B2
SHA-256:	BDC1BBFF99C43B4ECF55DF2AD18F70BDD8CB62373936B60BF5CFE6E6B6684D61
SHA-512:	A73B8CD3862C1DFD9D541DDAFB30302A7BFF07870859741EB4FB3E562D44F177FDC12755E890E9A6B25B628A57DD225B8B762E3A998CF32FCB35D4BDA28D6D DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...h..\/.....*../....A.A..Eo.....p.).....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:	COM executable for DOS
Category:	modified
Size (bytes):	960
Entropy (8bit):	5.0240786190624735
Encrypted:	false
SSDEEP:	
MD5:	E0A9EF5455BA777C9C13BB89DD3297D0
SHA1:	0CB2F7E0A98D3CBB88A0296F93F493DD3BADBDE8
SHA-256:	8DAA4D25DDF242537B24D99DB65C040BD7B003B0203CFEA02B7D083F94BFE7A6
SHA-512:	3BDCB44C2D76945DBF58B32C44F8D0EB3D8C76765D25C5F76767F8C076C9078DCAEEEFDD3CF0543E0A6DADE60F44FC59FA5D877A9FC8F9D3346024DB03EF 784
Malicious:	false
Reputation:	low
Preview:	......U.oy retne....&.....&.....;.y~A..4..."/.....*...4..."/.....9.cmvd..`.."/.....oB*..o.."/.....#...(....."/.....k7A..4..."/.....D.4...`.."/.....[.i..%...`.."/....., +..._.#.4..."/.....<...W..J..o.."/.....6<|.....o.."/.....A?.2:..4..."/.....+.{..'..`.."/.....?..7X.L.4..."/.....2q.....4..."/.....P....V.4..."/.....+.U.!..V..`.."/.....P[. q.4..."/... .....!...0.o..`.."/.....u\].q..`.."/.....~..,4>..`.."/.....&..r.4..."/.....=..(Q.x.4..."/.....4..."/.....*.....`.."/.....o..k....`.."/.....^.~..z...`.."/.....o..4..."/.....Gy.' .h..4..."/.....F..=z;..4..."/.....3....4..."/.....v...q...4..."/.....C..M....."/.....a.....o.."/.....$..+I..`.."/.....=....m....`.."/.....q..4..."/.....:..N.A...4..."/....."/.

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:	COM executable for DOS
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.0240786190624735
Encrypted:	false
SSDEEP:	
MD5:	E0A9EF5455BA777C9C13BB89DD3297D0
SHA1:	0CB2F7E0A98D3CBB88A0296F93F493DD3BADBDE8
SHA-256:	8DAA4D25DDF242537B24D99DB65C040BD7B003B0203CFEA02B7D083F94BFE7A6
SHA-512:	3BDCB44C2D76945DBF58B32C44F8D0EB3D8C76765D25C5F76767F8C076C9078DCAEEEFDD3CF0543E0A6DADE60F44FC59FA5D877A9FC8F9D3346024DB03EF 784
Malicious:	false
Reputation:	low

Preview:	......U.oy retne....&.....&.....;.y~A..4..."/.....*...4..."/.....9.cmvd..`..."/.....oB*..o.."/.....#...(....."/.....k7A..4..."/.....D.4...`.."/.....[.i..%...`.."/....., +..._.#.4..."/.....<...W..J..o.."/.....6<|.....o.."/.....A?.2:...4..."/.....+.{..'..`.."/.....?..7X.L.4..."/.....2q.....4..."/.....P....V.4..."/.....+.U.!..V..`.."/.....P[. q.4..."/... .....!...0.o..`.."/.....u\]..q..`.."/.....~.,.4>..`.."/.....&..r.4..."/.....=..(Q.x.4..."/.....4..."/.....*.....`.."/.....o..k...`.."/.....^.~..z...`.."/.....o..4..."/.....Gy.' .h..4..."/.....F..=z;..4..."/.....3....4..."/.....v...q...4..."/.....C..M....."/.....a.....o.."/.....$..+I..`.."/.....=....m....`.."/.....q..4..."/.....:..N.A...4..."/....."/.

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF6ed366.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	COM executable for DOS
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.0240786190624735
Encrypted:	false
SSDEEP:	
MD5:	E0A9EF5455BA777C9C13BB89DD3297D0
SHA1:	0CB2F7E0A98D3CBB88A0296F93F493DD3BADBDE8
SHA-256:	8DAA4D25DDF242537B24D99DB65C040BD7B003B0203CFEA02B7D083F94BFE7A6
SHA-512:	3BDCB44C2D76945DBF58B32C44F8D0EB3D8C76765D25C5F76767F8C076C9078DCAEEEFDD3CF0543E0A6DADE60F44FC59FA5D877A9FC8F9D3346024DB03EF 784
Malicious:	false
Reputation:	low
Preview:	......U.oy retne....&.....&.....;.y~A..4..."/.....*...4..."/.....9.cmvd..`..."/.....oB*..o.."/.....#...(....."/.....k7A..4..."/.....D.4...`.."/.....[.i..%...`.."/....., +..._.#.4..."/.....<...W..J..o.."/.....6<|.....o.."/.....A?.2:...4..."/.....+.{..'..`.."/.....?..7X.L.4..."/.....2q.....4..."/.....P....V.4..."/.....+.U.!..V..`.."/.....P[. q.4..."/... .....!...0.o..`.."/.....u\]..q..`.."/.....~.,.4>..`.."/.....&..r.4..."/.....=..(Q.x.4..."/.....4..."/.....*.....`.."/.....o..k...`.."/.....^.~..z...`.."/.....o..4..."/.....Gy.' .h..4..."/.....F..=z;..4..."/.....3....4..."/.....v...q...4..."/.....C..M....."/.....a.....o.."/.....$..+I..`.."/.....=....m....`.."/.....q..4..."/.....:..N.A...4..."/....."/.

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_2798067b152b83c7_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.516068689456449
Encrypted:	false
SSDEEP:	
MD5:	E2480F17D9D6920A52A10A1801E2A5AD
SHA1:	85B40226979AE2042227AAFE33B29B997B21C95D
SHA-256:	DE019E51100AD8C6476969519362F6F56A25ACB9D6C2CE06B712F74DA20573A2
SHA-512:	617494E3E73DDCA04979DB3CFE31AFB95B70BE7BBB8B19E6334E085354767792E1490C2EF87FECC0943A0A2056A74149888015B87B89D6CF38E4D51504D2102E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..m..\.....*.M.....A.A..Eo.....k..J.....c..y/L....|y.n..C/l.....X7-ne.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_6fb6d030c4ebbc21_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.495888678433462
Encrypted:	false
SSDEEP:	
MD5:	61F637CA4D298E523C9892BC5D023848
SHA1:	2F95FBBA73C5F0607D2DCBA24D0CA997BA56F611
SHA-256:	15C7D928ADE324EEA1F2D933A6EB284C0C8C08673A82C07737B77EE57097E662
SHA-512:	92370EF08AEFC82B51AF0A9AA74AA0B5870B5671DF60F9B70DD86702DB9230E508BE96754AE371A17D5F6214B8587C9A3ED0EC58365D1D1AFDEBB44AC3E2E9 90
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...m..\.....*.....A.A..Eo....._.....A.o]@r..Q.....<w.....].n\....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_71febec55d5c75cd_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.575186308366446
Encrypted:	false
SSDEEP:	
MD5:	A648FD23E1BA3E4AB92379BC9C3A2130
SHA1:	35263129084F454324CAE7FA9083C162DCA1CB57
SHA-256:	49B23008B5CBB28B3830B5B88FBF7EADA532C2F915F034AE1AF89E33DE85322B
SHA-512:	1D7B91CB74064BB0CDA133E33A95F1BDDFF4C6BAE6C31C4A7E5AF138DB82346518323CD17DCF58FC3558CB459DEBBB601B811EE7C6851EE9639E07CA46FC8DE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...I..\/.....*.. ....A.A..Eo.....q.61.....@..{o]...9o|..qY....T....{..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_91cec06bb2836fa5_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.609347787281982
Encrypted:	false
SSDEEP:	
MD5:	1825445B96A93E2DC0D69E49F79C710F
SHA1:	B4CE88300D7E1A0269A36741E46EDB09EB1F209C
SHA-256:	2249120BC689B45B1A8C84766DC87EDF2FD34868C7C5D38987CD4AEC10AAD0D0
SHA-512:	BC6502F2708DE8C38B7FC6A20A39E0AB9485E95F4872320E2E3F8004FF4FE6E54F6C54D4C27C57AAF85361811B573302AA3CD408370DEBD6F226387A132194B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .6*m..\/.....*.....A.A..Eo.....~.n.....z._a...'.v.....4p3..1.']...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_927a1596c37ebe5e_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.541048247773875
Encrypted:	false
SSDEEP:	
MD5:	0F7CE394DF92E47B068B45304D805E29
SHA1:	BD5052C656E3B7B6516B7494EED79B106B25DA60
SHA-256:	68D3E187526F82ED67116B1B4828C86898E6555D3565E40C6D2F2C7F69DB5B8D
SHA-512:	766AD2C9136853988FE82396487804196699EA1956355B85B1545F9E16C65366BB04505673523349AAD138ADB4FD3EC3D4CB279DBCD8022CF5485E69B05FA30B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..,m..\/.....*.v.....A.A..Eo.....E4w.....c}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_cf3e34002cde7e9c_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.627034964733468
Encrypted:	false
SSDEEP:	
MD5:	3D99B5902E784A97DEC14388D34F6104

SHA1:	91905E2955801EB58F4904618BCC3AA09FBBB4CB
SHA-256:	DE285290C719BC0F08CD740DBC8B78FB75D78F43D268E9FD44904A308153F94C
SHA-512:	E626E76E2E8864EBA756200151FCDAED7537183DC6224C1997532BEC07FC454D25C83F9BC97ED43CA12F2D9098FCBB93871D48AE9D85D51DCC76DC741379F20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...m..\/.....*.....A.A..Eo.....PJm...0x.x..RD...BB!@5..<..]....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_f0cf6dfa8a1afa3d_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.579438164108999
Encrypted:	false
SSDEEP:	
MD5:	DEA4FA2B13919968E53E2164FF0568FB
SHA1:	ED08F73E6EF9E5040FC7C733735B9737A8B8FCB8
SHA-256:	683FE25268F95043334C07C9BEEECE115905CC295AC696F5200EB1768AFFEC76
SHA-512:	C2647D1EEC2B70E0758EAEABEBAD7D4A50C42714EC63E2AC72BFABBAF818E9FE85D953DD0ACCE935A49B6D1208E10A61E4417A1AACA51805056709E881B16E5E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...n..\/.....*.....A.A..Eo.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....

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):	293
Entropy (8bit):	5.199728777815265
Encrypted:	false
SSDEEP:	
MD5:	2D6DE0447FBC0D8422C9E1784060A57D
SHA1:	0F6ACAA8D0E9698FDBEB2CAC4F0D6CC29BC43494
SHA-256:	3889D4A09036A7EAD4ADDB7EE52572F1A036E0D2925A91B93C2C56571EC26F32
SHA-512:	7BF0F79CEFD55E7CAE3E331377CB1C30299236316A27BEA25445088EFB5556CCED9A4FEA6A939869F3A84FC05FAC9ECFA8BEBCFF7ED3C3BC5E94D22159C759C8
Malicious:	false
Reputation:	low
Preview:	2023/06/06-17:18:38.190 26c Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/06/06-17:18:38.192 26c Recovering log #3.2023/06/06-17:18:38.193 26c 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):	0.01215297344497993
Encrypted:	false
SSDEEP:	
MD5:	08F860991207E3DFBD25CEFE58D0F316
SHA1:	57255679E3C07A6E9DD989EBE7D8DBD698693B45
SHA-256:	0D4A592FE66AE27FAEDAA5340544459CD0B2C73BC39731390262CE1317D4E451
SHA-512:	E3C2FB6F2A745407C445C92A7E8620E0714992F4A91C13355FD5363F6E7DE7711C99BB97CE5F21FC4D1C786A4E5A0A60E9B76ED6FA26B7B9CA5F5D2B6A0721AC
Malicious:	false
Reputation:	low

Preview:	VLnk.....?.....,..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2306061518332-201.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, cbSize 71190, bits offset 54
Category:	dropped
Size (bytes):	71190
Entropy (8bit):	1.6639863087780205
Encrypted:	false
SSDEEP:	
MD5:	4CFA3773D2E38AE2B07F0C520712BC83
SHA1:	EDED76B885B2C57142E5FAB96EB0882914BE6A8F
SHA-256:	19AD4CDA2D9A3C0B655ABF86E60D5ED902A5680D1DBDB0D80984DAE0F7F409CC
SHA-512:	FC0BAE077755ECD02320AF99D0A68496D9F327713E218A43B680DD1813EF70082C67C74B24DDF899431AFD1B2E2FBCCC06FCBDDB4583FCEB9337582A5FBEF 14
Malicious:	false
Reputation:	low
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 3035004, file counter 11, database pages 16, cookie 0x5, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.8255863633176053
Encrypted:	false
SSDEEP:	
MD5:	C310C363EE49F92B1D3663791DFFD518
SHA1:	7F202460F17285739ED8D3300996D87118E17275
SHA-256:	2D6959E7F6A62D78C861A9526F7E31382BE94D8BDC40E6584F6EAE9975C92142
SHA-512:	5EC1CF033DBEA6DA30E1E08EF5A018464BD3FBCFADC8BDA6A1EF04C8A7DAF51B87CF6775DA659CF1085329BC9A4E52DC60D8062E9484F8140965CA9E814F 753
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....O|.....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):	3.1785832930925286
Encrypted:	false
SSDEEP:	
MD5:	91812A6CA0E051A57A15C36BD351F823
SHA1:	42CEDDB1232306E68B9F278F55A3F9F68F357529
SHA-256:	11AF2D786FE0FA38F771C71CDEB778989085BCC682ADB520A9F01DD14B354E0E
SHA-512:	85AB733773A3675D7C3F8FF34FD890817E67CE884B3E9D940D44CE7CD412E1D92E61750196FE59E391E09D5A4EE2EEC7E795F43AF98C9D4480D910D891180F6
Malicious:	false
Reputation:	low
Preview:	.... .c.....A#f..... .....h..... <.....y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt21.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.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..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.6800

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.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..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt21.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	536
Entropy (8bit):	5.17576513886526
Encrypted:	false
SSDEEP:	
MD5:	4D5E3CD969F14362210F0473720C5528
SHA1:	AFD90E9888759B809F78E87D5550B601A288A0A3
SHA-256:	79D95D01FDE7FC7C890CD62734A7F203B12A5D44A56D6009D0E43E40D99682AE
SHA-512:	B10C157945432CC8944E63A28CA3420CAD0C6B87BABC77BB5437DA5E3DF0CDEB657D410F28FA61D314E86269B8D1AC5972B0792D3E78787DFCE496EEE979D 64
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:Dire ctoryHandler.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..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt21.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):	5.223243858582587
Encrypted:	false
SSDEEP:	
MD5:	3455517A7EA370FB26E41F9C0D1F2AEF
SHA1:	0A1DE15B520E538FE48BB82DC29CFF12D772EC51
SHA-256:	F29BE4937BB25A377D75F64271D1C3CB44992AEABC41F1D0ACAAF830E5FA40D5
SHA-512:	979D1BB3A39CB1AE51083612A37DF3D4C19B7830EB3D82FD8506B9A4B0B68009B67D68CD7785B3368934697E45573DABA1041E8BA881706CCE702ACA0ABCB6C2
Malicious:	false
Reputation:	low
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:85552.FileModTime:1619528014.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.6800

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.223243858582587
Encrypted:	false
SSDEEP:	
MD5:	3455517A7EA370FB26E41F9C0D1F2AEF
SHA1:	0A1DE15B520E538FE48BB82DC29CFF12D772EC51
SHA-256:	F29BE4937BB25A377D75F64271D1C3CB44992AEABC41F1D0ACAAF830E5FA40D5
SHA-512:	979D1BB3A39CB1AE51083612A37DF3D4C19B7830EB3D82FD8506B9A4B0B68009B67D68CD7785B3368934697E45573DABA1041E8BA881706CCE702ACA0ABCB6C2
Malicious:	false
Reputation:	low
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:85552.FileModTime:1619528014.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_READER_LAUNCH_CARD

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.332717847961966
Encrypted:	false
SSDEEP:	
MD5:	4771061A5575A21EDD10516110D5D489
SHA1:	979762E618479EC2F856D049772E005C8F06E0ED
SHA-256:	15DA84FBAF7A66868BE6ECBA8E5CC5E178C325A58505C393500EE9B0CB7C4046
SHA-512:	2B884F7BC71881DEE819FD9048054C47C5460D740C4505B52E53373290D125653F05C80A0DCC0DC554F4389A1AAAF9F76C9028B0CEC87ECA5E41EE9AD594E5F
Malicious:	false
Reputation:	low
Preview:	{"analyticsData":{"responseGUID":"e6cafb2f-fe58-44bb-ac74-e46d3e09e190","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"expirationDTS":1686242997844,"statusCode":200,"surfaceID":"DC_READER_LAUNCH_CARD","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Banner

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1395
Entropy (8bit):	5.779126765157096
Encrypted:	false
SSDEEP:	
MD5:	B1494493CF2E4DA08F17BC375A61BFC9
SHA1:	283635E25A009A8A117E9A0819337F75C8C1A42F
SHA-256:	986F2A685A7223BE5FE051243092B47B2AF0911476D53175C0576AD6D02A4E03
SHA-512:	AEC090E166215045A77A94E92A40563C0FC7014887B5874F4C5F47D61773C18C08587409F657216D2362D895282E26C72C33C7C712E773CA78ACF9D13A5A7C78
Malicious:	false
Reputation:	low
Preview:	{"analyticsData":{"responseGUID":"e6cafb2f-fe58-44bb-ac74-e46d3e09e190","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"expirationDTS":1686242997844,"statusCode":200,"surfaceID":"DC_Reader_RHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_RHP_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"57802_176003ActionBlock_0","campaignId":57802,"containerId":"1","controlGroupId":"","treatmentId":"d0374f2d-08b2-49b9-9500-3392758c9e2e","variationId":"176003"},"containerId":1,"containerLabel":"JSON for Reader DC RHP Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVIIDctRGF5IFRyaWFsIiwiZ29fdXJsIjoiaHR0cHM6Ly9hY3JvYmF0LmFkb2JlLmNvbS9wcm94eS9wcmljaW5nL2VuL3NpZ24tZnJlZS10cmlhbC5odG1sP3RyYWNraW5naWQ9UEMxUFFMUVQmbXY9aW4tcHJvZHVjdCZtdjl9cmVhZGVyIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zIjp7ImZvbnRfc2l6ZSI6IjEyIiwiZm9udF9zdHlsZSI6IjMifSwidGl0

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_Reader_RHP_Retention

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	287
Entropy (8bit):	5.277499229496728
Encrypted:	false
SSDEEP:	
MD5:	31F88F2BC23942676C9A8E123C2E8504
SHA1:	5B0750B5E3B0C058097A8BAD0DB745A51F236B13
SHA-256:	3C3E100567E858B0407D996B51CE64D7F8A4C2770B3509898E9BDDCBA15035DD
SHA-512:	69827366066D767875389909166D5BD95B9AA33B4647897889DC7E8D2F2C931FB8B01EF17E2CB02B11BFF2FDA7F35B14286236BBBBF67E8573C1CE8BB502A962
Malicious:	false
Reputation:	low
Preview:	{"analyticsData":{"responseGUID":"e6cafb2f-fe58-44bb-ac74-e46d3e09e190","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"expirationDTS":1686242997844,"statusCode":200,"surfaceID":"DC_Reader_RHP_Retention","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\Edit_InApp_Aug2020

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	782
Entropy (8bit):	5.372211768511718
Encrypted:	false
SSDEEP:	
MD5:	9B350D92971BCA097A9A945C128F208B
SHA1:	D62FE7065A9768A19654B0CAE2FB57B289F5749A
SHA-256:	67C7861E52C37D7A8E98E56AFAF3E875AB9A1C6179F6E39FC97A3B3B141478FC
SHA-512:	8587D890827B54E1EF9E6AC41C7A4C91EF18891A56D8AABD201C5271D4FEE09D71AE402D3969F56E526C49A0D13F24CD93E5012ADE2B15DD4EA3FF2CDBB6AD4
Malicious:	false
Reputation:	low
Preview:	{"analyticsData":{"responseGUID":"e6cafb2f-fe58-44bb-ac74-e46d3e09e190","sophiaUUID":"2CA8C5A6-154C-4669-80E9-F31A8F7EFE55"},"encodingScheme":true,"expirationDTS":1686242997844,"statusCode":200,"surfaceID":"Edit_InApp_Aug2020","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"Edit_InApp_Aug2020"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"20360_57769ActionBlock_0","campaignId":20360,"containerId":"1","controlGroupId":"","treatmentId":"3c07988a-9c54-409d-9d06-53885c9f21ec","variationId":"57769"},"containerId":1,"containerLabel":"JSON for switching in-app test","content":{"data":"eyJ1cHNlbGxleHBlcmltZW50Ijp7InRlc3RpZCI6IjEiLCJjb2hvcnQiOiJicm93c2VyIn19","dataType":"application\/json","encodingScheme":true},"endDTS":1735804679000,"startDTS":1686064722868}}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data

Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	
MD5:	DC84B0D741E5BEAE8070013ADDCC8C28
SHA1:	802F4A6A20CBF157AAF6C4E07E4301578D5936A2
SHA-256:	81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06
SHA-512:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB1
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	767
Entropy (8bit):	5.084745834001999
Encrypted:	false
SSDEEP:	
MD5:	6057FB3B94FC61E3A67A3D75DD8F79F7
SHA1:	FAA2D0D1A1F35B36D8DC6F76DFFA11B390135C93
SHA-256:	87F9CFE937292D24C7AF06BE4C9243003A268474201C8FBCA7FEAB0B0940E338
SHA-512:	7C4FC7C756243EA9B1997D1F83167E6520B354F395CF3B12516F756F19E10D2C4A2A3BCEFFBF2775EF9A682CCA32C44F8E1ABCE216ABE9A9C7717EA7B74A0B24
Malicious:	false
Reputation:	low
Preview:	{"all":[{"id":"Edit_InApp_Aug2020","info":{"dg":"656354c4c302dfc95224158957051883","sid":"Edit_InApp_Aug2020"},"mimeType":"file","size":782,"ts":1686064723000},{"id":"DC_Reader_RHP_Banner","info":{"dg":"d217e69a5fc43c3488b2d8e38274e16d","sid":"DC_Reader_RHP_Banner"},"mimeType":"file","size":1395,"ts":1686064723000},{"id":"DC_Reader_RHP_Retention","info":{"dg":"af6b6022768c5e45ade38e2ea9067fce","sid":"DC_Reader_RHP_Retention"},"mimeType":"file","size":287,"ts":1686064723000},{"id":"DC_READER_LAUNCH_CARD","info":{"dg":"d7dfd95ba217fbe2a0389949160657c3","sid":"DC_READER_LAUNCH_CARD"},"mimeType":"file","size":285,"ts":1686064723000},{"id":"TESTING","info":{"dg":"DG","sid":"TESTING"},"mimeType":"file","size":4,"ts":1686064711000}],"g_info":{"Version":"0.0.0.1"}}

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):	40393
Entropy (8bit):	5.5182337348115755
Encrypted:	false
SSDEEP:	
MD5:	61EA86BAFDFD593A35D14DD35C278562
SHA1:	0BD901E23B108F1B38143DF16E3FB4B9A08B5E56
SHA-256:	B67921812A03D15DC38B91C8B739D0AFFB7C775265567FEC82FA40B5FA1153EA
SHA-512:	BD1DD87F4D02151986F6A92D5BAAAA72D23ABF26CC44C30914F6672A09F68D07AC8670AD0D9ED9F3E95340F2C0DCFA34738DF1D45E3FBB6E307B7E49C462AD0
Malicious:	false
Reputation:	low
Preview:	4.241.93.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:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-BoldItalicMT.P:Arial Bold Italic.L:$....."F:Arial.#.91.FID.2:o:.....:F:Arial-Black.P:Arial Black.L:-....."F:Arial Black.#.103.FID.2:o:.....:F:Bahnschrift.P:Bahnschrift Light.L:&.....,.....F:Bahnschrift Light.#.

Static File Info

General

File type:	PDF document, version 1.4, 1 pages
Entropy (8bit):	6.226053647029973
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Electronic Invoice Print.pdf
File size:	26088
MD5:	63dcc6758eddaff4e86c7de6bde70e67
SHA1:	9a52ed2a5c8e3810f00f7cec70cc030e7627ce8a
SHA256:	8f30bb76174ce3b486d58e29eec5bb24b863dd8fe2719c6c69a2321e9f949dcb
SHA512:	72928aba170f6b4d6587fc9cb454b12db444a888e7bb66e6b4274e9b475a12cdb46da79f429c897f01665b48445c0aae1ece47e5702eb9dc66bf2f3b98f97e56
SSDEEP:	384:IdpdXx47C/liqnvKX5E7pj8+ufRnMJ9VeiJxxKucuhY:l/M7m3sZnobJhcGY
TLSH:	C4C25B1AF719CD45F4D46635E0E8F28A833AB74097E33A43709C4702BF666B98C4E297
File Content Preview:	%PDF-1.4.%.....6 0 obj.<< /Type /Page /Parent 2 0 R /Contents 7 0 R /Resources << /ExtGState << /a127 << /ca 0.4980391 /CA 0.4980391 >> /a255 << /ca 1 /CA 1 >> >> /Font << /F1 3 0 R /F2 4 0 R /F3 5 0 R >> /XObject << /img8 8 0 R >> >>/Group << /

File Icon

Icon Hash:	62cc8caeb29e8ae0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	6.226054
Total Bytes:	26088
Stream Entropy:	6.192190
Stream Bytes:	24173
Entropy outside Streams:	5.072495
Bytes outside Streams:	1915
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	12
endobj	12
stream	2
endstream	2
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview
8	020f1f6b2b130f1c	f19a6ced32a17078f335b2a546657b3c	