ID: 651261
Sample Name:
117444687973.pdf
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 18:03:51
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

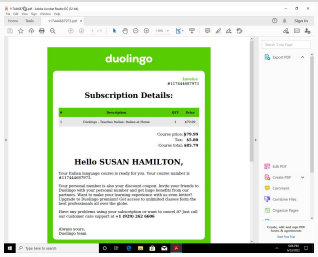
Windows Analysis Report

117444687973.pdf

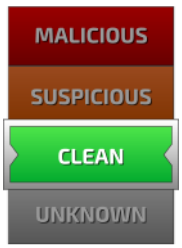
Overview

General Information

Sample Name:	117444687973.pdf
Analysis ID:	651261
MD5:	96ed08bd55e2d5.
SHA1:	8a27895e1683b0.
SHA256:	a3fbc01a305591..



Detection

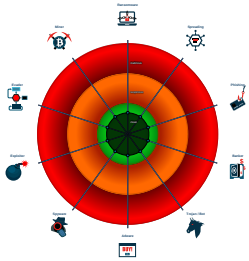


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is start
- AcroRd32.exe (PID: 6360 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\alfredo\Desktop\117444687973.pdf MD5: 0EAC436587F5A1BEF8AEB2E2381D2405)
  - RdrCEF.exe (PID: 7244 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.

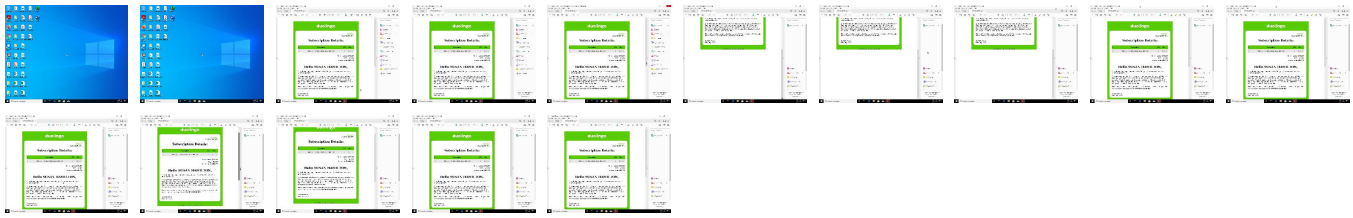
Mitre Att&ck Matrix

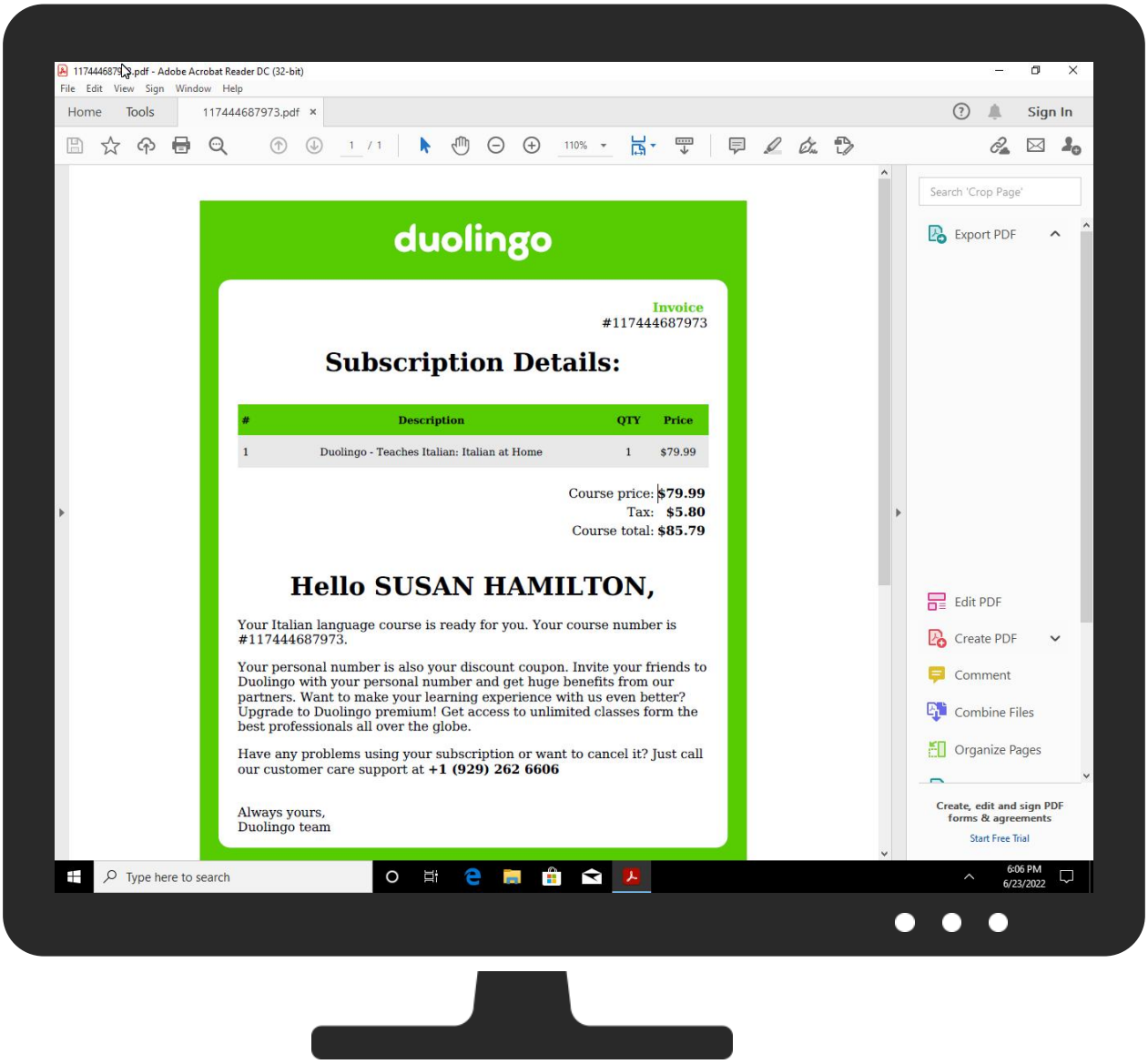
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	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	1 Extra Window Memory Injection	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Extra Window Memory Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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

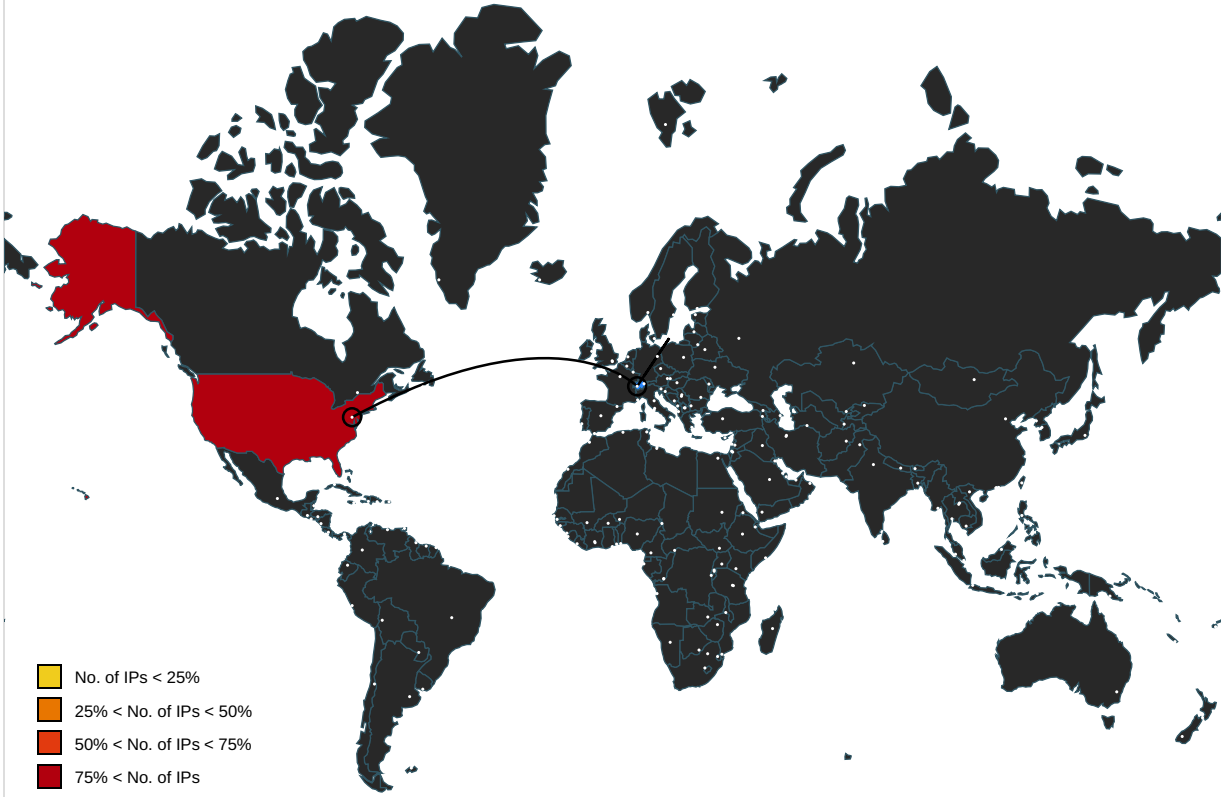
No Antivirus matches

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
104.102.28.179	unknown	United States		20940	AKAMAI-ASN1EU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651261
Start date and time: 23/06/202218:03:51	2022-06-23 18:03:51 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	117444687973.pdf
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	16
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
Detection:	CLEAN
Classification:	clean0.winPDF@11/69@0/34
Cookbook Comments:	• Found application associated with file extension: .pdf • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 104.102.28.179
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com, nexusrules.officeapps.live.com

Created / dropped Files

C:\Users\alfredo\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):	5.626165503012043
Encrypted:	false
SSDEEP:	
MD5:	DA28400DA497888DFDA948B29FAAD06B
SHA1:	BAF10E540EA2B07A8C7D2E27156D092A98EAFB70
SHA-256:	D832F8AB3154E2F563B941F9723B7382F315006D4A5614BC068C4555C964029C
SHA-512:	F19D1D590EE357FB6B2D9821FDB870C82A2B61AE3937CD7DA95A3E8EABC98CCA46868BD75069FCE7726BF49D4454C55BB0C50262FA6D6859B55EE275AFACB AF9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .7.Jq.@/.....*...IoC..A.A..Eo.....S.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

C:\Users\alfredo\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):	5.50438962986547
Encrypted:	false
SSDEEP:	
MD5:	0F323C29341AE2248A1318AAB451F356
SHA1:	6524BDF10414D8B6C5D82E9F1CCF79DFFF6C8A8C
SHA-256:	F48BAF0FA2644DBA6A859B4F894277448522E801D554F0A26FC991796AC78026
SHA-512:	87C7D40BC8A97A1263D48794D1928BEBAE8AF13ECD36B443967EE9C4A36102B7E3CEFB569ABBC573A1ED234C20A301D8CF9E83E33C8E0D978DF5DFA1F56C0 249
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .F..p.@/.....*..e.lC..A.A..Eo.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\alfredo\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):	5.572810920409399
Encrypted:	false

SSDEEP:	
MD5:	B7A065F2CB0C4A95AD70A3E0728E428F
SHA1:	50F38316B0A1128C049369176EDD8A816CD5C457
SHA-256:	0EFCAC7E3E4CB89028B7D9E5009B59506D0ADB19D0100AFF4A6C10C892F390FE
SHA-512:	3F4A5224ED67A93F177A69BF79ED2E69EC166E9EFA47129D579BCDFB2E4D2721CFF2A70B6D14CC727BE2F882C65F365BA3D677EC50F807A70C551916164127D9
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 ..Hq.@/.....*.2..oC..A.A..Eo.....L. .....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\alfredo\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):	5.671056320746446
Encrypted:	false
SSDEEP:	
MD5:	C2E3A4B38BEEF9BFEC184E18B7A279F3
SHA1:	9CD4BAA4A261D58536936BA3A6A524B65FFF60DB
SHA-256:	0356396306CB42D7BEE27A2C89D647FEF3F0CF8B3F42148C0B16685D0C948B2F
SHA-512:	69D534AA4C03B89E8473E8E36ED50B66AB43D8B434042D8AAD08F165B542E6A046E529293170B62273EBFFC702538E6A5D9C9D42D77DBD5437D5C6E096CE98(A
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 .Q,.q.@/.....*.S.-qC..A.A..Eo.....&*.....8 P ..a...R..Y....7.@..2Dm{..A..Eo.....

C:\Users\alfredo\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):	5.571741757550295
Encrypted:	false
SSDEEP:	
MD5:	1AF317F5D3918C070219C14A8773A653
SHA1:	72ECA3ACF61A2D9A05DF8CBA8CAA642CDE1F4964
SHA-256:	D471B5EDDAA79B3B0F9EDF0BC9BD8ABEAFB36D5577DB2C2C67F1A99096F64E96
SHA-512:	8E88A7DF2CCAD573C5BF9C10F1FAA675589E2EFDF55F1122671520BFDAE168AAFF81C1F6FE02AC06B5EF5782368B31586CC6315CC86D1999AAF718ABBD25A74D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..}lq.@/.....*..$=oC..A.A..Eo.....k.Q.....-_..y.....O...>..1....A..Eo... .....

C:\Users\alfredo\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:	modified
Size (bytes):	216
Entropy (8bit):	5.585373816888227
Encrypted:	false
SSDEEP:	
MD5:	A058C9DB6E1D8726F6AD3F7BE974D3F8
SHA1:	ACDBAAA1D506FF5309EBA3858269B5AEE1C5BC0B
SHA-256:	63C75D7B55DB5605AD6C4F940371139FF096F2F7A5BFE918F3592FE60D090C6D
SHA-512:	DCEF133B411851F2A200697CD73FEB6963CF22956F2F0A216F7D0DC0A4D4578F5278714097556FA3563D088B589EC24AD8876F252AA38ED1D58921374C94C91D
Malicious:	false

Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .(/Gq.@/.....*....oC..A.A..Eo.....Y.....].>....uUf..N...k.....c..l.A. .Eo.....

C:\Users\alfredo\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):	5.511778751885925
Encrypted:	false
SSDEEP:	
MD5:	0F3576B44EDA2E96F6F2AA7DF064C75F
SHA1:	A0E976A6231E7EC4D56459A675F11AC63CF52E32
SHA-256:	66E2A64C56B9A74344E5375E3BA84D1FDF44AB712C1CE55F773220BA369D711A
SHA-512:	119FB67C6A75A7E6656CC957832DBADC3A881717DA18B9A223D0FA07044C62E7FD1D392C3722B2FC99C419636485E59B3022C9C18EE6F8C8691D642EC3B94E 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...Jq.@/.....*..yoC..A.A..Eo.....}Y.....c..y/L....|y.n..C/I.....X7-ne.A..Eo.. .....

C:\Users\alfredo\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):	5.52079556911055
Encrypted:	false
SSDEEP:	
MD5:	45C73E84C0D1B4E347C7246FB4847779
SHA1:	22057005E156D4E1B7711B1BACF97D8148E1D5C4
SHA-256:	2F8BF776211E0F4D634B9CDBDA30857339DA7EDBEE8D4F332DC3284D4B49DD13
SHA-512:	8F4A7B0841D1D5FBFCED6A4C6ED4633CD6B50A5A67F4AEDAE514DF9D56E3669ACC3D8B52D3432AAE3DFF1476B7C1556C3234A2E2802151D182FB6BBD33FC 6AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .W..p.@/.....*....lC..A.A..Eo.....G..`.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\alfredo\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):	5.5231811113634555
Encrypted:	false
SSDEEP:	
MD5:	C274108233E793332C2D84ECDD8D0F13
SHA1:	9E4815408C21ED9ED9CD20993C9FD2A66F406EB9
SHA-256:	BAE79935401FE04C274504AEB02CA2B63E617FB4D984831B4A092B4FCAE9585F
SHA-512:	23F7BB848F02B761FE3780D094F385CC3E485AF46108A9E6EB0B86F1C0ABBC93EA5023786DA9B55EB2E49DF9FE2C135B3E04F4002363A9919E6186C7080F3D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...p.@/.....*..y.lC..A.A..Eo.....;.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\alfredo\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):	5.566501668551465
Encrypted:	false
SSDEEP:	
MD5:	2B25AAE7034A5EE4935F2FD2AB9DB002
SHA1:	7AA44728A101920F21E70069CE5CA72F230AC5FB
SHA-256:	986E7822538828388F3334375CC059E869DA2CE3F79D50ECE80CDC2879D5C430
SHA-512:	5A5C6BE749DDFBFB89584F935DC03CF5FDDBC26C2FE4BF81688E2A259FDB0EA2328E938482429C1AB8AADFC396318E4EF479A9CCE9B878550015CDAA91E7C331
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...9O....._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/plugin.js ..1Gq.@/.....*.S?.oC..A.A..Eo.....^.....e.....@-H.>a..o..sh.5.A.x ..C..A..Eo.....

C:\Users\alfredo\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):	5.523898193587867
Encrypted:	false
SSDEEP:	
MD5:	510E9C782D78118805F9EF978AA978D6
SHA1:	527C5C7F5242EB19CE200C0BFD7FD056D4BF2011
SHA-256:	14C240BC2685FCA86205B82394877F2B69D00BFCE2473B6EDB4518D675380061
SHA-512:	F9AF7383D7C3F6F82EF610CBD5259B93B8D9BCAFBA3FCFB41795077C4FB8E7B629E3D12897EDB967AC295D99A3D47C8403E668A6075FBCAE68B7C97E592A5D80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...Cq.@/.....*..?.nC..A.A..Eo.....V.....q.O...j...._y..L^z...?..@N..A..Eo.....

C:\Users\alfredo\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):	5.58564571479297
Encrypted:	false
SSDEEP:	
MD5:	CA7C113BE9832BE8982E436E22D40A4F
SHA1:	83F06C2028162B9F0A7A362430BB9D9EF6DEBD28
SHA-256:	2373765510D23B7D8DE501EBD468EF0C3B49F0DA4D9FD0BF687C64AF6AE2D521
SHA-512:	C63B13580BFD42BF8E5B3B1053E0708DBCD0909744B903D7EE9B92408572BEF50F32DE9B77EE8C2945AC635A24B6EB70D9B19051B373471839F4DB8A18B7C484
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 ..~Iq.@/.....*...oC..A.A..Eo.....dT.....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\alfredo\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):	5.592054274455178
Encrypted:	false
SSDEEP:	
MD5:	41238B9CB19C1F16237679CE3B0D92A2
SHA1:	037E31FC66C2D16712D3AFF732A03F7825FE9AE1
SHA-256:	DC5C3E27DCCAA3C3CC89401BED63FD074A229A883047717EE4FF7B891C135FC1

SHA-512:	C7F484E602C3E9ABFD3EEE08868A9425EA55959D49D45D0781BBEE53E69ABC83B924FB4423126E3150EE4EFDC7BB365696612918018BC818089F0070C1CA1AE A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....."....._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/selector.js ....q.@/.....*.\..qC..A.A..Eo.....-..6.....8U-....a=...`#..VT.k.....A..E o.....

C:\Users\alfredo\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):	5.506436367955655
Encrypted:	false
SSDEEP:	
MD5:	B5A8A3194025275DAFC2821892247620
SHA1:	C47A51215D89EE514948D73548F423416EEA7B22
SHA-256:	6CB9A886E9B6080596339B112FB90105F062332CB3040C7C8712EBF93106B274
SHA-512:	58D6659BBF943B8B711DC21EAA4B9EB83373B7EC3602DB0EE4E47EA1834341121E8BDE81CFC7DC3142DC2C032A70DE9C4929A49173C510C319E4EC1FC359D 0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...Hq.@/.....*.3.$oC..A.A..Eo.....K.....A.o]@r..Q.....<w.....].n\ ....A..Eo.....

C:\Users\alfredo\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):	5.625632390001536
Encrypted:	false
SSDEEP:	
MD5:	B8D865A8AB531BDE8662EBFD1B46D1CD
SHA1:	A2D905129E967123F25F3BEBFAEB8704059A0AD5
SHA-256:	2186D2467702B8B3B8B6AC8FA58F4833337ED7A0B25EA708A6584840BA2CFECC
SHA-512:	6D9AB805913AEA07F2C6439DDABC2299509218EBDB7A100C7C90D2167A6E8FF7FBA7120641F3585951BD60457C28AAC0FB748F856389EE857697110509BE1D08
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..,Gq.@/.....*....nC..A.A..Eo.....4T].....Tw.....(..b...EO....9.A..Eo..... .....

C:\Users\alfredo\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):	5.5660153679222315
Encrypted:	false
SSDEEP:	
MD5:	AC9D775152AE387F586D31A897EA345A
SHA1:	21BB3BB8E9DE216C952AF5F66A6BF81FA54D9606
SHA-256:	9B96B6A2368B046BE1BC08A9B8CF2CB7308FA3C29E4C0D18EEA3C23C27D05401
SHA-512:	12A2B03C303AFE26081F14BAD1286168D3A5C8FDFABCA7CC03F6501E3FA4AB3BE40E69E2DD01348884B2D91A080DE66254B563CEB056FCD1214BAA564A1A4E 37
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...Hq.@/.....*...1oC..A.A..Eo.....(C.....@..{o]...9o|..qY....T...{ ..u.b..A..Eo.....

C:\Users\alfredo\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):	5.57544430450037
Encrypted:	false
SSDEEP:	
MD5:	32BAA6575CF1D765C583F21EAB538E43
SHA1:	BCD31629E1DC71A395CCCBEC431E16268DB7C713
SHA-256:	398D0D7ADA0996250D1809B4ADD3539EF83EBB3A7C1A375E37209B8550431EE8
SHA-512:	065B8098D85AFF939CD4D2887DF77FEF9A6E8E8ADAEC95D8D330975A2F197C00A8A82B3043A3FF6FF60794E539DBE46802A216D618D3E8296DCD58D5F5B6C06
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 ....q.@/.....*...nC..A.A..Eo.....Wg.....-..... 5p9o..k#.}..6(..*A...A..Eo.....

C:\Users\alfredo\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):	5.597911861351602
Encrypted:	false
SSDEEP:	
MD5:	FC415E76C7AC68A7D5D27097F8F9AC6B
SHA1:	8E399D5B16BE9782C52D3227161F39BA8618CDE3
SHA-256:	DC01E5F896CE2E08B5AED901E6C7AFC50DA079C14E382AFB0E17630F32FEF8D2
SHA-512:	95188069A77E8D1F96196B3A59CA0EBAFAF8727023EA1FBD9C463A048648C227F23078148C379AFFCF8D4A84093E1AD95C85E68592FF2F7B4DADCD9C3CFCE11
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...r.L...._keyhttps://rna-resource.acrobat.com/static/js/plugins/unified-share/js/selector.js ...Fq.@/.....*.X;.nC..A.A..Eo.....y.....U.....&.Y|.. . .&.....A. .Eo.....

C:\Users\alfredo\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):	5.561649489866961
Encrypted:	false
SSDEEP:	
MD5:	919F421C2535794C6D90260270916B38
SHA1:	51A367AA42305E794C7E91DF8CA212992AFECA54
SHA-256:	4C44C1014515A682CB77A5E55B0C86FB0FA883E7837355BEA142F6D12245CA46
SHA-512:	66BC9EB894399538207278AB7EDBD5B3D498D4B2611C13D24C9CD831E052D9E72106F6999EB4F71FC12A54820D0FE790C9ADE50927789B0F7A69F10AFEBDEA84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...Dq.@/.....*....nC..A.A..Eo.....*7.....t\a.....x5.'OuE.C..@.....x..A..Eo..... .....

C:\Users\alfredo\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):	5.572486249762836

Encrypted:	false
SSDEEP:	
MD5:	362B7C1CB779A93E80A63DA259FC36F4
SHA1:	E6F3E85A52A82259E895707C89B5E82E063A2B2E
SHA-256:	1632304D191EFC1E195F754AAB388188D5272A6D8DA3C91111CB926962048851
SHA-512:	A0553424DCA2AD970DA6DCE36AE8F075B3FB15BD9E3B0D0101EB1C226B7D59CBE1A1E58E7DFEA34652ABFC75F519EC32CB16F4A2F9050714096B540CFF285D3D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..}Fq.@/.....*.B.nC..A.A..Eo.....<.....7...o..a=.98I.....(3.$G.A..Eo.....

C:\Users\alfredo\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):	5.569894972335396
Encrypted:	false
SSDEEP:	
MD5:	806789C4E3738356A6B925CD970A3EB5
SHA1:	3B8AB7F06E1A254E25408418DA0380F50CCF809B
SHA-256:	64020EF0AFFF7FAADDCBECBE2F51FA9507128C68F50E06D5FE9D89A89D6EFAB9
SHA-512:	D724E1CB0AEDF6D330AA2F1923A0A763E739778C303EE0F2DDEF1BD6B084AD93E1C86832A21B1CC5D5BFC5C4CDBE65DB42DB043E241E875E26A46F1CEA62D1D9
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 ...Dq.@/.....*..{.nC..A.A..Eo.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\alfredo\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):	5.567305610867357
Encrypted:	false
SSDEEP:	
MD5:	DBA49325776872FBA468CD3055879D70
SHA1:	C5EBDC95A0818AB0CE8836CA5461B7CB5A7F57B7
SHA-256:	00ABADA15374EB6D4E520852E958AD794B5C5D144A6157F6A741561A034F8662
SHA-512:	2239471AD0EDE510ADD242257EDC8BE674C3616AA83B77E4195CD39646CD7768CAA05EC7DF6D4B3CBF1AE87A1D8B2ACA8E6920BA0A833E7F0DB7D3D98442B15C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...Cq.@/.....*.j3.nC..A.A..Eo.....h.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\alfredo\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):	5.635280471118943
Encrypted:	false
SSDEEP:	
MD5:	B2C85F3C9F4B7671985E154CA74A421C
SHA1:	C0EAB15EA83C6A7B26995E8C8146EC6EE63DD2D8
SHA-256:	733C1D1A8AC388E90021E16FAB3DDD0DEB146B63281E9C0E48EB180F11572423
SHA-512:	91D5F740426917625BD20B9413CB27D552EF7CCB164407B7FF3894EC0E22A42696819FFF3C87F362BBFE16B2079D8428FB3053FD199311645129B761B29FE940
Malicious:	false

Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .[.Iq.@/.....*....oC..A.A..Eo.....}.....z._a...'.v.....4p3..1.']...A..Eo..... .....

C:\Users\alfredo\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):	5.5511575480425135
Encrypted:	false
SSDEEP:	
MD5:	852D248D492921F54790DDAD928D179C
SHA1:	4B8A12C819E71A0BD5A682D917F8A4F5F39DFA78
SHA-256:	C2624FB6ECF2688AFE3DA45B5522A62D8CC8020639FB5EA72DDF07AF2C9B0EFC
SHA-512:	0F810288FBEF955D7F09D2FC55785A0DAAE6E97B0FD0CE64D6E4645D6DE182FC3CC07FF292C39A89450C9F02328CE71D6D63267120194550F6E71BE966A8E55
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..{Iq.@/.....*....oC..A.A..Eo.....c}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo .....

C:\Users\alfredo\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):	5.554435697484638
Encrypted:	false
SSDEEP:	
MD5:	E88514395417D152FD360A2F04C65B0E
SHA1:	2F60F306BA564FEF174972EA91E496247E11A3C7
SHA-256:	3FF95A4F17A03465E92CAE3589409EE79036EE01392C46F01058A5DCA477C9DD
SHA-512:	7B1093BF356687CEFC36BB552569CA7C62E0D0D579E49540A0FB786106C4A4D3B2D885A9B92DB8C8E57E9106640E69FB6D21BCE07E36954D6A138DEBF876CA E6
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...Dq.@/.....*.^i.nC..A.A..Eo.....%.k.SZ..~W... ..:)'B..ad.....A..Eo.....

C:\Users\alfredo\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):	5.650563090926141
Encrypted:	false
SSDEEP:	
MD5:	348080C1FF6AABECB2380CA68764B198
SHA1:	92FAF2A69ED806D35CCA6417C7CD24DCFC870BF6
SHA-256:	BAF8BE6B0AE1D65F3CE96C031A6080729E70D252AE39A1E5009E9CB439EC4254
SHA-512:	A8606D4F8674A6C4E0E13FE182CB3676A4DF0E18FD7BEAE2AF81EB471F5DDB619D9ED77F44DAFA2525B04B41BB86ADA4952AB3FBA2DCE8646E4C77518EC41 41D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...Dq.@/.....*.5..nC..A.A..Eo.....|c{.....;''./N_.,.:C..2....9L.H...3:...A.. Eo.....

C:\Users\alfredo\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):	5.551621429049748
Encrypted:	false
SSDEEP:	
MD5:	9688A1DEB0569E7704900CDE7C37EBBF
SHA1:	3B706A2E46F1B9A5D8F89BDAECC376AA1E4B580F
SHA-256:	3FD14D5036408A20607EE0CF608A897F01505B1485323696471919CCC38A1817
SHA-512:	E8AE312D5C74171D7DECF45044B3FF7A0DACAC9B5B71BF25B6D395E680EB8907C05163E97F2D5C79A1FAE49569A4B4E06E13EE4ED7A8CEAF79FB1E8BA098A668
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...Dq.@/.....*.S..nC..A.A..Eo.....p].....Z.Z}Q..4.o....0+..[[..n:*..U.W.A..Eo.....

C:\Users\alfredo\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:	modified
Size (bytes):	188
Entropy (8bit):	5.574405499288846
Encrypted:	false
SSDEEP:	
MD5:	723E7B93943A9B78580CAB1F96BD0C3E
SHA1:	BCFB3E5423D9FB9E203FE478ABECE2CC423D22AD
SHA-256:	EA3E5D5E7C92699352CA8DD5BF55CABFDE2878AF44D545880FBB213F12AD5E05
SHA-512:	8EF5ED9238EA50C629D2D14E4A6B304B3C42CE41BCBAC5BE8AF1953E14EF6FB21EE6CE1B4EA5F8ADF1DD15D411D834AA1F0D2AE625C8CF7A2EE1CB6F477ED4AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .G..p.@/.....*.y..nC..A.A..Eo.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\alfredo\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):	5.586050695027736
Encrypted:	false
SSDEEP:	
MD5:	901763421F7FBA293D124898C68C97EA
SHA1:	E5E881569BC830B08A258C92D6D7CCB3A9C390DA
SHA-256:	EE5A69A9E8D80D927730DAFF024CF484A3ADC7E7CC1BBC1D36DC6AA32E68DDD3
SHA-512:	81E515F8649573E88C0435C9DD361413B40306A1FBB6E024755E5FE0D55B3A829E6E8717E7ADEA5821A7D391E2ED3D5DDF08592B6E89B99E1CFB0572907613C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...lq.@/.....*.k..oC..A.A..Eo.....4.bo.....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

C:\Users\alfredo\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):	5.56416984704249
Encrypted:	false
SSDEEP:	
MD5:	AEFC8D297D2FFB0C6F9FECDEABAC70F5
SHA1:	771B884305CA7D34A7BA81109FD08FE617F1636F
SHA-256:	A4E8E59B3DA977956774C196236B55D3CEB0E53D1DF0C5FCE32638B66EBF73DF

SHA-512:	6174C2B57E766C8E7BFB0D1FB32251C1030AEAAFAE62FB639088613AA723EC3A1538839A2DBC9FE2AE25276408B6474EC5B85CBCD61F5F86D1B39B293DBC2A79
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.@/.....*...lC..A.A..Eo.....!R.m.....L...Im.@.....E.nW...IP..A..Eo. .....

C:\Users\alfredo\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):	5.601025784280503
Encrypted:	false
SSDEEP:	
MD5:	31DAF861713C79928FFD72A2CF81D546
SHA1:	9247692C62E62A156621405F934A30F61D81007A
SHA-256:	157F02F5A987D89425196D3A55FA8DA486E49C9F759711BA9295442730AE56B4
SHA-512:	0C717C149223147D00B9D5F83BF6D8390DB221D4BB303175AFCBB35FA53F6BAF735613A4550B262BF5D9426C51261B3087F664660FA521843FAE0073DDC70B35
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .M.Jq.@/.....*.{.WoC..A.A..Eo.....9.....PJm...0x.x..RD...BB!@5..<..]. ...A..Eo.....

C:\Users\alfredo\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):	5.57856277274333
Encrypted:	false
SSDEEP:	
MD5:	54920A4E80FF6BE5DE072C9D6A9C9BB9
SHA1:	7F7D18BCB8A6286BD2E50C18BCAC5F0268F1F543
SHA-256:	D0DB99385DCB05BDD691B79E030AC2736B291980CE76290B25E006B74BC2332A
SHA-512:	C5465EE91F95A724C9230D5717C28AE6AE96F1CDD65CBC97F6C967D13EDAA4FF70F2896E3821D69D7B133C130F2030032A6C32A347AAF66707443CD5E05C7A6
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 .bO.q.@/.....*....qC..A.A..Eo.....t.....P...#4..l....5. ..5..).w.. .h.~..A..Eo.....

C:\Users\alfredo\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:	modified
Size (bytes):	210
Entropy (8bit):	5.623629528374418
Encrypted:	false
SSDEEP:	
MD5:	2A698A246C1900463C25BD2F8FFC6204
SHA1:	DAA872D67FA6323D6C17BD734138E0A5803768F4
SHA-256:	71C2B2CF9262B1E89410A741477E25920DB8E337068AB6478B322C40A337C137
SHA-512:	4F104B5B6327B68F8331E47C6EDB6033D10E81DE162BFDED28764636C50826C8B3B47AD9C5C2B9C3265137703B63AA5BD93BB5633457054F5B1F4E4684A4A023
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/task-handler/js/plugin.js ....q.@/.....*.z.!qC..A.A..Eo.....[{.....E*).*^.!..C.....G..#.&)A..Y..A..Eo.. .....

C:\Users\alfredo\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):	5.539099897159177
Encrypted:	false
SSDEEP:	
MD5:	5F8B956DA4123E299796AA394D033D54
SHA1:	5FDBFC729C23089E8782771EAEACC487463C8CC0
SHA-256:	04DC287367B80FADB451D4B7C582AE9FC4F85AF4E685B6997F05991C064311F7
SHA-512:	84E9112E7679853E2BAFD64D217111A1699FEF903F7C5AD987E76DEA583CBCCCB493E900F3674D69D361B156946ED4A0365B2A8F97E4CE512E37B83940F656F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...Jq.@/.....*..vcoC..A.A..Eo.....0|D.....#..@..k(v.8g..5.~_....]Pj.*..6 .A..Eo.....

C:\Users\alfredo\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):	5.57187434131776
Encrypted:	false
SSDEEP:	
MD5:	82DD905448A3B9747617ECF1C16EC9E8
SHA1:	25C9ACF51868741F7BC7101CD023EE484E45A124
SHA-256:	B37D2137571EF73184117B8F3E030E5F3D087BD0A61CA7820683FAFEDD515534
SHA-512:	BA2280DB818CBD9BA70E03B6E918C867421942C3554D78ED0468202389FC49CC36361A55D61435C50178E738FAB81CB753668B3AF9757EB2D5BAEE43AA88BAE 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .u?Eq.@/.....*...nC..A.A..Eo.....D..... ./.ev.....N~..6.b.....$.j ;:C...A..Eo.....

C:\Users\alfredo\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):	5.551556062137431
Encrypted:	false
SSDEEP:	
MD5:	E67C99A7EBE3E3B185C93D0DE63A4FED
SHA1:	B626FB823D5465B76C7EBDF9D8D988F3FD060C60
SHA-256:	C7796BA9777A66A696CE9A5B60D5C1141FB351AA19B0A6473C40192F3498A143
SHA-512:	0B61F72C658914C3287643926452887323DAD5E75E905D46C98BE7C1AC8FA3B98738C732B9F7B4296CA0F4ABE715CB8A81232C595CB67519B37BE084C2A54D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ./.Hq.@/.....*.k,.oC..A.A..Eo.....1.....U...I.>P...X...x..0U.~;m.x.k.A..Eo .....

C:\Users\alfredo\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):	5.552419894591888
Encrypted:	false
SSDEEP:	
MD5:	C1FD80F911A4924D5F1149FAB03D88C6

SHA1:	8FBE171B0FB5C070E056AAFD4559F359F01B357C
SHA-256:	3B3451E35A5F55B83D5FEBA235DAB1BCCF243DC943EED6546FC987762E299F50
SHA-512:	21F60EC36FC9E5B23F5448119C0786EA4A890B7590C5FE5420007CF29CEF020FC378324D91599C65108365F7CA1BBD2DFD68B5B43E14434621696622C42785DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .#|Fq.@/.....*....nC..A.A..Eo.....?.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\alfredo\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):	5.5517259811490485
Encrypted:	false
SSDEEP:	
MD5:	5648318FDAEEE970B5AAE427A6D109BD
SHA1:	10F81CDBF3B345405975984169992CC3A3138E5D
SHA-256:	486474866676C435ADCBBF6C6894F6D1C304D31838B1128AF1534E55DBDCFFBB
SHA-512:	4AB9024DE49D3862B2D0C5D3EFBFCF142600C31ECF4D97FDABF0C8CB6C951B8E04AAB9A9CA2E32CCD9494F1718447A8A858E81E8C24E5483D3B591BE8A5C4 956
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 ./AEq.@/.....*....nC..A.A..Eo.....Y.....9Q].8 O.z....=..:.N.{....N{.A..Eo.....

C:\Users\alfredo\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:	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>..`.."/.....=..(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\alfredo\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\alfredo\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_0786087c3c360803_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.516042623495834
Encrypted:	false
SSDEEP:	
MD5:	2FE9A44CA4D38130BB45A962867A11E9
SHA1:	57F745C1905A23458134EF78A75CE4E8F6AE66FF
SHA-256:	A7F8F75BEFB29AAAB2C349483EEE99443E4680E4FACCB2C733B06277C2B681AE
SHA-512:	3B7DEC2F403335D7A204F8FB5BABA347BF6B77504E6701F184E45DC7C22DDE3E9CE5F115CEC432683960A17E0AD0992E7E763FBD1DFDD380CABA9C85753B3 E90
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...%p.@/.....*.k'.jC..A.A..Eo.....).I!.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\alfredo\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_2a426f11fd8ebe18_0_1 (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.534707440594758
Encrypted:	false
SSDEEP:	
MD5:	D90E2076FB830F45A3AE54661126EE38
SHA1:	0D86D2D98F89E35A1E4A3AAA8BD23A6C130D8BEE
SHA-256:	EC3F1C204F80AD650320D4057EC2E1F383C827D00EBA830AF83B21CDA061DC7C
SHA-512:	0148CCBAC52E5D15E74972B9CD8C18AAB504399B31A811B1DF894EA63F0B93C30E60CC1EB2605DBD791230B1AFABF4654189C4BB349F8D67CA61B11941F9D8 81
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..N&p.@/.....*..-.jC..A.A..Eo.....i.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\alfredo\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_bba29d2e6197e2f4_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):	5.565897467784671
Encrypted:	false
SSDEEP:	
MD5:	2C4354E8C183396B81BD8447345EE8B6
SHA1:	59E5BD018E1A0E570728EBCC2E816985FB4B2AE9
SHA-256:	D43D6F660BE37900EDF7CEE92CE897E4D242B3B7BC6BBBF84603440E135E624D
SHA-512:	5D8C5EFB3FF9B9F6D5A8D93BEFDFCE042AE5F67793D2128578827260A80FE98B62C78F11FCE858695D5C4F213010A29424A2404853963D09D50C5826C513973C
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 .QQ&p.@/.....*.%\.jC..A.A..Eo.....F.....L...Im.@.....E.nW.. .IP..A..Eo.....

C:\Users\alfredo\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-220624010436Z-228.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped

Size (bytes):	65110
Entropy (8bit):	1.4939441991910587
Encrypted:	false
SSDEEP:	
MD5:	249BD7F9D6D76D9DB85A6B4104C00999
SHA1:	2841302449FABE4C3AEDE58BB135D94105E99E50
SHA-256:	2E055688383127A8033A9CAB89E1537691E4895124FA83BB5D3EA57799A03909
SHA-512:	4B9E125A965EE6FFA8D5F4E0789CA8DA4E6EE00AEF5FF157C339375C019E000D48058BCBDBDEC7EA0DF2534B36C04CC447E8FFBDA2391133A5D2AE23CFA6E A11
Malicious:	false
Reputation:	low
Preview:	BMV.....6...(...k...h..... ....

C:\Users\alfredo\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:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB 1
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\alfredo\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	138
Entropy (8bit):	4.63862852024164
Encrypted:	false
SSDEEP:	
MD5:	42E7BD718F1F49CF158C740E50234FD9
SHA1:	89F4BA84FF0947F8B35BB4067F83FFDEF64C26C5
SHA-256:	CBE7B0337F3CCD0CFF792111046212CD3E61CAFF9611007D917AFB2EA038B110
SHA-512:	B6E4308AB5EBDD193F123480BA353AF99AEF092CCC75D42415C30A82ECB19BBC2686DAF43A4A2549738BF6420B001105F48029BFE58C7DBA69FD5797E55C6B AB
Malicious:	false
Reputation:	low
Preview:	{"all":[{"id":"TESTING","info":{"dg":"DG","sid":"TESTING"},"mimeType":"file","size":4,"ts":1656032674000}],"g_info":{"Version":"0.0.0.1"}}

Static File Info

General

File type:	PDF document, version 1.4
Entropy (8bit):	7.824082577928637
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	117444687973.pdf
File size:	25838

MD5:	96ed08bd55e2d5588c91ca0c2d8a6e64
SHA1:	8a27895e1683b0a798dca34c6c68381c03497390
SHA256:	a3fbc01a305591bb448ccec9a0bb5e0014e54659c0fe41ac9fff4bf11198b7ff
SHA512:	3dfaec3bc38ca9a81ce698d026f6d9f85ef8eecfc83a2bff1d99480768eac9b6d015c546bb3b8ae9a14668eafcccad09e37db438681b8aa4211436f0e7dfcc16
SSDEEP:	384:/IKijI6UJGoZnWrvN98eiPyZrL42DqB82DbADLXgglGLUA2CUSbT3+8nLqa3jAXm:/33ZnWePyZrLRLvlGLUbOTZt3KaHVtX
TLSH:	99C2D1048D844D9DFCCB6B81592239CA84EC718746C492D371B54B4AFD5BF489713ADF
File Content Preview:	%PDF-1.4.%.....1 0 obj.<<./Title ()./Creator (...w.k.h.t.m.l.t.o.p.d.f. .0...1.2...5)./Producer (...Q.t. .5...1.2...8)./CreationDate (D:20220623005211+02'00').>>.endobj.2 0 obj.<<./Type /Catalog./Pages 3 0 R.>>.endobj.4 0 obj.<<./Type /ExtGState./SA true.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.4
Total Entropy:	7.824083
Total Bytes:	25838
Stream Entropy:	7.958897
Stream Bytes:	22293
Entropy outside Streams:	5.131333
Bytes outside Streams:	3545
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	24
endobj	24
stream	7
endstream	7
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