ID: 764046
Cookbook: browseurl.jbs
Time: 11:05:17
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

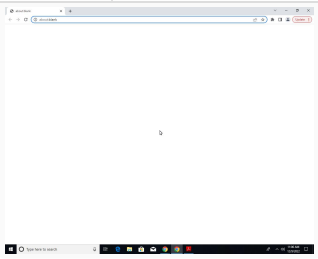
Windows Analysis Report

http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwen..

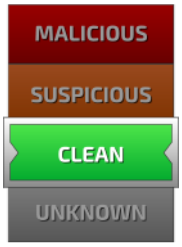
Overview

General Information

Sample URL:	http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf
Analysis ID:	764046
Infos:	



Detection

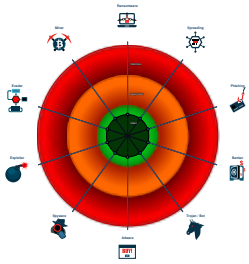


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Drops files with a non-matching file …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2224 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5932 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1640,i,10835741753073723708,5021152820849143339,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - AcroRd32.exe (PID: 6764 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Downloads\ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
    - RdrCEF.exe (PID: 6652 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
- chrome.exe (PID: 4692 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

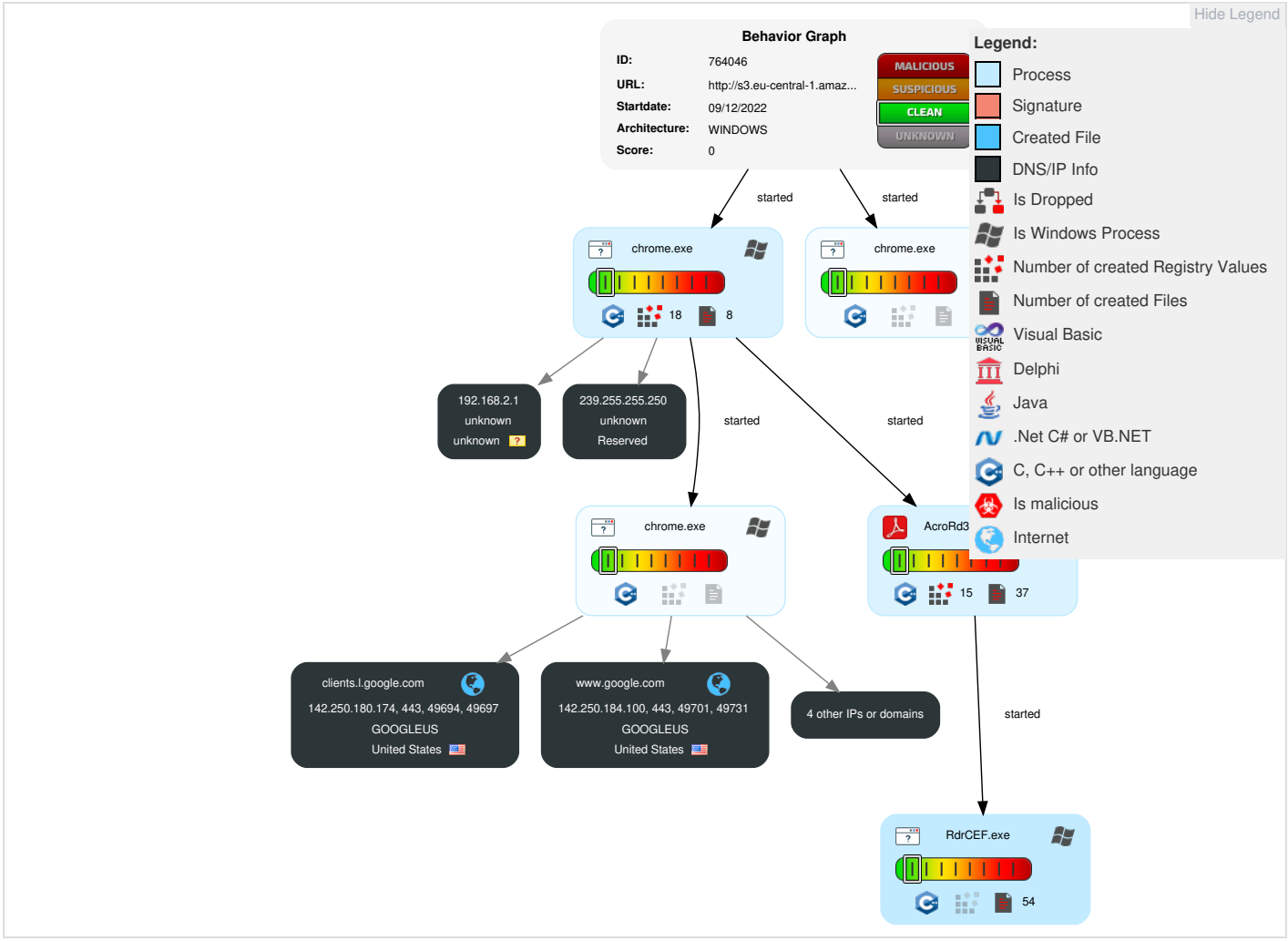
Joe Sandbox Signatures

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 3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

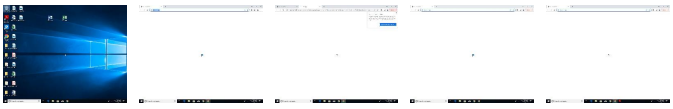
Behavior Graph

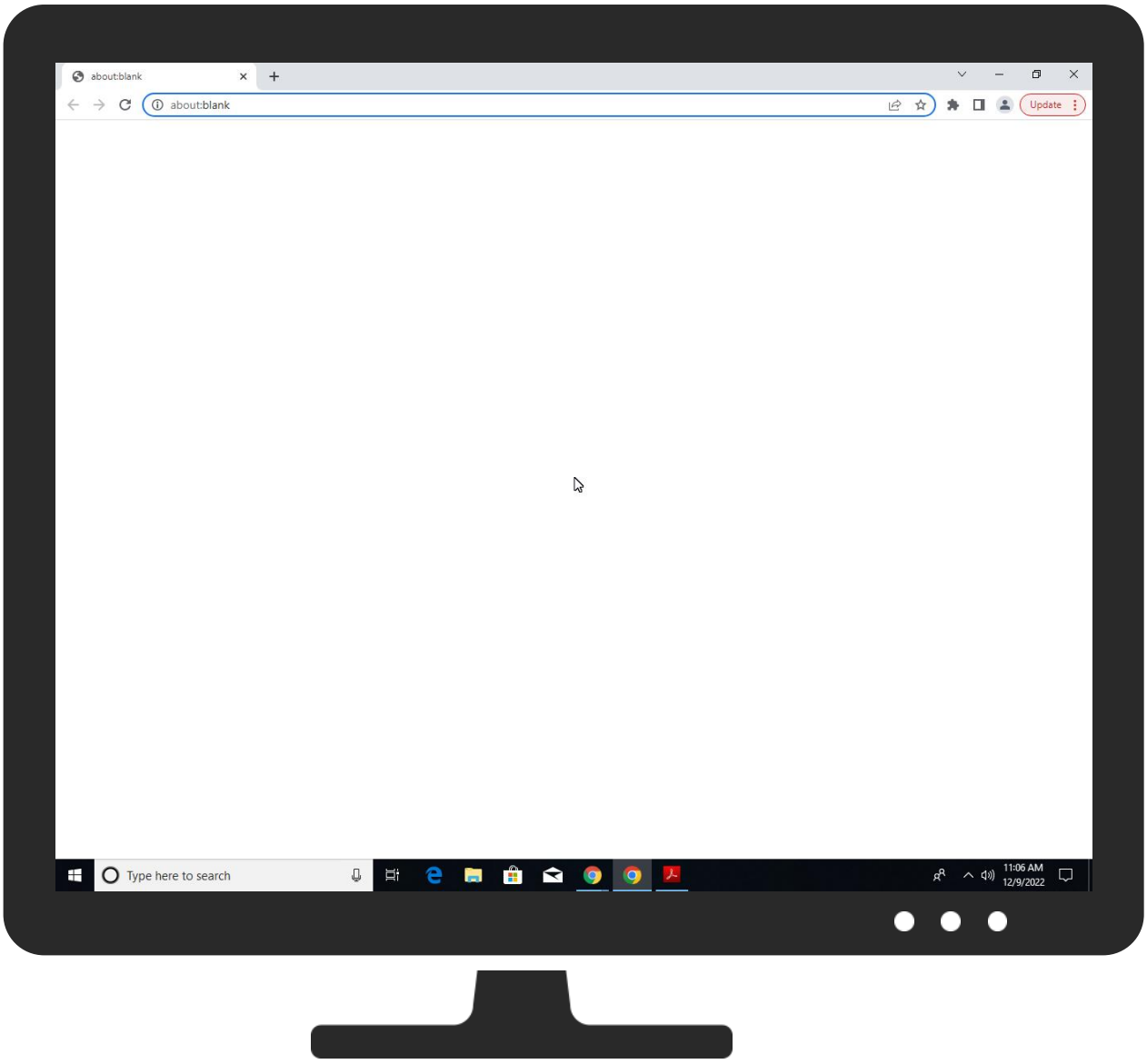


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

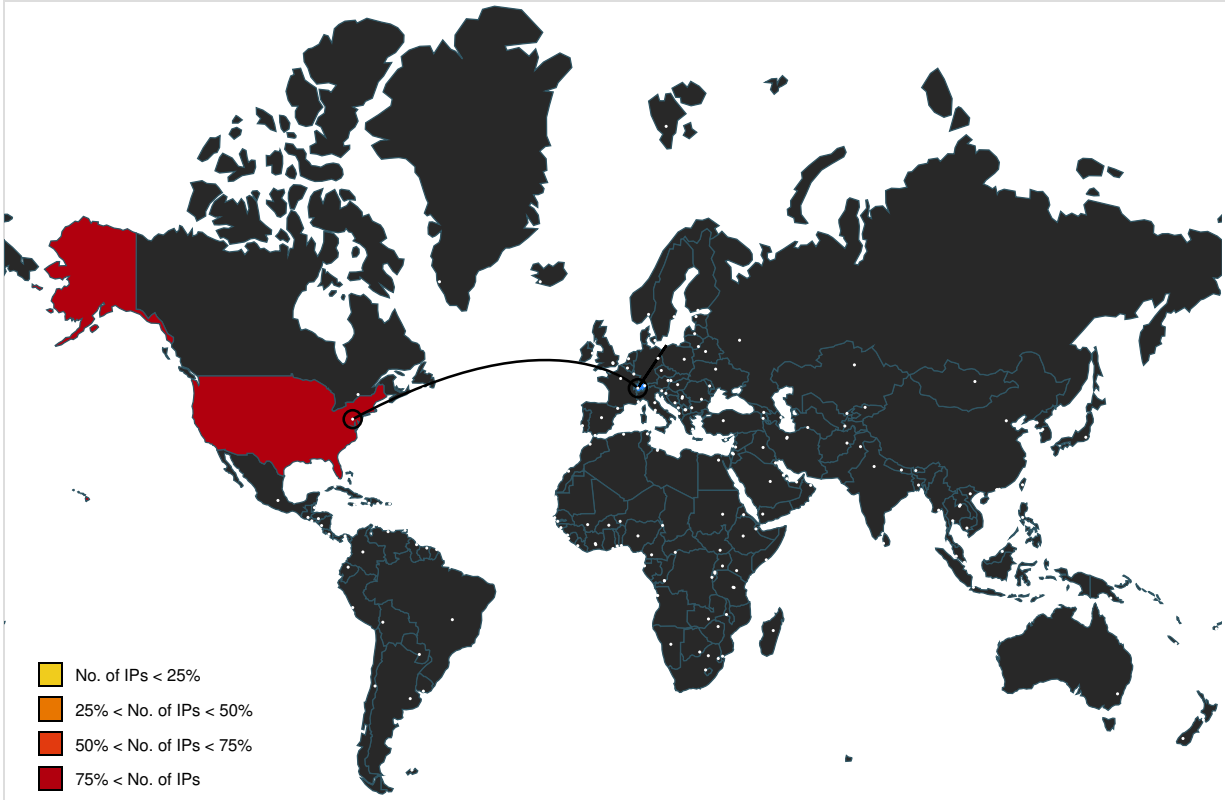
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.184.45	true	false		high
www.google.com	142.250.184.100	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
s3.eu-central-1.amazonaws.com	52.219.169.25	true	false		high
clients2.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.219.169.25	s3.eu-central-1.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764046
Start date and time:	2022-12-09 11:05:17 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@35/49@7/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 23.211.4.250, 2.21.22.179, 2.21.22.155, 142.250.180.131
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, edgedl.me.gvt1.com, armmf.adobe.com, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.net, a122.dscd.akamai.net, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, acroipm2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:06:32	API Interceptor	2x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.6159222568163845
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Q6lNn5oltVXi7Z+P41:vDRM9BlzafuZi
MD5:	7B33641428209CB54DADE8D39DB1C4D6
SHA1:	DFD364777B12414F0267166CA0897A35405306B7
SHA-256:	64AE46B32F8F6F9AEE36EF690DD055583751CBEDC75629A41CF92A9F289F316E
SHA-512:	3CB8AB9907FFCD0BA935E3B56308915589B7BFF893B60747D28CC87B2BC8023E39139431E204EFFBF0EF6200687B26840C8AE315D6E7E111AF8BEBF86A61BE4A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....M/....."#.D.>?-...A.A..Eo.....w.%.....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):	5.523039701692117
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVrulcSQ9koMkt7H1e98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkZulcx9kolt7Ho8Be7YV
MD5:	40877B6EC74554300E3AFB7561CDA0CE
SHA1:	FFE13518AC922D9DB65135404ACEB7C32F6B5B97
SHA-256:	DDE0372114C839E2A9A37D4D5A890A8353CDF8F01714121F5638C0D5ED88DBA1
SHA-512:	60AD4FA0FB3036F725CFB2787A106CA963AF8B22E9ADAC78995907ED9AA2CD2F9E536015035FEF0BB19C6908A48E47E216D4B2CDDA90E7C6096118242E57D6B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..9...M/....."#.D...,...A.A..Eo.....z..[.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.580875910527271
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhufFlhTGoltO4t/RlUoSjGY1:DyeRVFAFjVFAFDFlUaBtZlUo6
MD5:	8255BBB451E7033328B07B213709BB9D
SHA1:	9267C32061294F6DD2AD4F9ABF7E0D89D24715CB
SHA-256:	4A046C8C3E82EB56E2C2389DFC0E9AC84BE84448FA56F1180DF95884F3BDE3FD
SHA-512:	4210A1F93A5A4E806AEC33D965ED9BD66AAE52431E258D7F73FDBAA48BEFFA8457EEBDA869ABC067730C80C6E08D0384C13D3C64CA5917DEB3236F3B99C25F73
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 .....M/....."#.D'.2-...A.A..Eo.....V5.....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):	5.671486775358988
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rs1ul6koltSzuiWulHyA1:IbRkiDPl6jEjWus
MD5:	D164A6468C653DF61E59626C6C989468
SHA1:	00F553DD1CED3757C20A863F79FD061D77DCAB9B
SHA-256:	3A603743CE211987034A5DE5C8E45591B3C4B92762832423446BCE1F431DCA32
SHA-512:	BDA08D26DE13B20FA0AF6B60D5F54418EE7E23EDF573CC22BF589921D30AAC5CE2B8C9BC07AECF1522CCA7320200C91C6CFF427F323BBAA7098111588E68AD17
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 .G....M/....."#.D...,...A.A..Eo.....E.....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):	5.534321326360182
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVue+lgAnLdoltF9lcVyh9PT41:pyixRudlgA5arcV41T
MD5:	550EBAEB14A3DF7F5A6B93EFB1ADE2AB
SHA1:	2EF0BEC0103460AB2C00ED1078B0B54AE66DE3F2
SHA-256:	BE83104A07B6363EF12A09BA5E3ED01841A301661403A6D88E4104A56F417A99
SHA-512:	A8D8048CDEA5B6440771D1B10699AAA3DF37E7DCE469F4968B066B4DA40D4E4EB00B3C45129F0E01D4D7D32BB8F338B4E4EF1163FAB3DC51046B0FBAE55A4AA1
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/....."#.D..4-...A.A..Eo.....Dy.F.....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):	5.591600566739831
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQLlloGoltZV3Zll6P41:0RhkkllhaDBZ

MD5:	C420E984F024EA6D8F5336907B7387A5
SHA1:	0748CC7275C36013B009A3992CC8060C3422B0BC
SHA-256:	FA6B5CC226E672B3297575BE7D28C247CB354D45DE33820DD94A57CE3D1E058F
SHA-512:	E706A78F62AFEBB34204FCF9CF4D575756C3914B46D724F0CFC209869EBB06D7ABBEB0686BA43FBB2E7909A02F58DFB5CDB75B38172FE90066ADE0245B6744E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..d...M/....."#.D...-...A.A..Eo.....<.....].>....uUf..N...k.....c..l.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.536951598435399
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuV5jj/lF9doMktMHljcyxMtv9G:mJYOFLvEWdGQRQOdQC/lHdoltcjD6g1
MD5:	2355A8FED952988427757A85438A6F50
SHA1:	21CE838BE16EA1B2468D0745A286183542F2B578
SHA-256:	27DD563C51A1E887601FEF4C54B5731F352D394028E96CAA4410C77B28CFD336
SHA-512:	867F3E7449147073BC7356E64AE152B5353F0A86227D79F126CBD236A00CDBEC39D96BEAD33E0F4626EF352023CAA5E2E0AD82CC17A04BCA974738FC6A61432A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .....M/....."#.D B4-...A.A..Eo.....).8.....c..y/L....|y.n..C/I.....X7-ne.A..Eo .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.534553133937308
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVel+FRCkoMkttdFlDQMWqg4nRb7om5m1:mOYOFLvECMLel+rCkoltt12uR/41
MD5:	0CD0D5CB4C80C453C78EE314B73AC68C
SHA1:	D4D30A4351EB9E39C3C324CB5FB9C58AAFA4E327
SHA-256:	9D9CD1C04E4158D438A0B557EFB7B2C9D19853FF3D101DC6F3F8B86A17E9E61A
SHA-512:	A9FA70AF0393FCE063BD5B5D0AC975726DCCAF881C6B6FF53286BD7C737711F43CC80CD40CC1F30374F9689380C2E72004020A788119545E44E676976B3F7A9(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .1V...M/....."#.D..,...A.A..Eo.....;.'8.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.532441048627083
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu0uIZKGGoltZE3by0zBUKSAA1:pRDuIZKGGaDWb
MD5:	5A625C9159C101DFF930CB88EB12BC53
SHA1:	E19BA2E1F6A7375EC043B23F07A83F5C920C5F78
SHA-256:	3F691A4D5BB059EFAD764680FFD553C631B75D88716535E08FFE2C1309642EFC
SHA-512:	CEB5E1571F9E02455CEAD10874D0B6A47FEFBA81772FD8FEEB9485B113DABC357A71723CF4D5EF3A4EE7907F5D64A35902D898D6705D80798AB0C975B27B4A52
Malicious:	false
Reputation:	low

Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .....M/....."#.D).4-...A.A..Eo.....K.Q.....Q..E.=....=h`t..t..3%A. F$..w..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.450764729626921
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvwquldCJnokoMktRtlWd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvwqulAnokolt7ks
MD5:	55DF571219E2D0E5653640E45F5DDAC9
SHA1:	358424BC1AF6CFE8BE1D86BFFEEEDCE1B80ED686
SHA-256:	723F03AD36A379BE381DFB34AECE4834A48595255265916AFF65E1397CA40EAA
SHA-512:	679E56EAADA3E383E6139F3A3A4E52133DD7928C9844582F5076690A3813558FBF63F648B7DBA65E43D1381925F8AFC2B236BD41FCE6AC3726CFC25BDA1062F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..;...M/....."#.D..,...A.A..Eo.....^Un.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.562642110688597
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLKo/lvoMktDlljUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLKolvolt5loPqVyM+e
MD5:	7F0896654F5A43CFA082D5A29CCA86B2
SHA1:	FC31232FC5507F3CAB4ED2E97A3900FBBDC17350
SHA-256:	0C6C026B556E61C06F6F8AE456470961B8B4B0A42D466D7F9DF953AB5445823F
SHA-512:	21D8DA8A299058CCD6CF13507BC12FE05917FAF1FD1B276BF2A23CBBC7898E2E0915430160DC1DAD27C17D3E4F9E341F16612EE5FDAFE6870E56B832CB35A0 14
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....M/....."#.D...,...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):	5.559046432023821
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFly4liqxfolt1lgtwSeKaT9pr1:URVFAFjVFAFTlJpabitwSeKaTL
MD5:	7A60A11927CD794649DEBEDAFFD7D810
SHA1:	F6CB5C64F2424394D710548F5797A5C0B0703035
SHA-256:	D5F42A67B6D52A6E5EB5CA231A0B71C1ADACE09E3F846A41893EEFEE0D2D2337
SHA-512:	0D4E2310C7DA1D555652837A107AA24FD163259F6128179CBECC6F23780D840DA4F106C331F17771F0528FF95EC59569941F5065DE01D9E0020307D841EAC251
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 .5....M/....."#.D..;-...A.A..Eo.....6a1. .....H...{...2../.k`..r4.C. .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):	5.488733346659401

Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXudlwoWiolt7zg11:BsR2Ese4lwoWia
MD5:	ED5737971DE752A85A72296AB9E0E252
SHA1:	F4DC4BA4EAA8CA324BBCF69F0C04AC036EA3CDD7
SHA-256:	384188AFBCA32A91B4592617A2D8CD0C4234FC42BF040DB98AB96AADC978056D
SHA-512:	2A391389FB3C8454631FDC45FA9B0B75A499F1F260485B50ABEC67CACE25A2E8D8D876A4A9E94150F0A38D01F638001CABF8AA44783A87D16D6B879E1F69672D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ..+...M/....."#.D.M3-...A.A..Eo.....VJ.....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):	5.61815825631675
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQhZll61doltELxm7OhKlvA1:RbR16mllsaCLxmJ
MD5:	4E51A17C9A96A729C965CD8534122D12
SHA1:	6E1AEC08D1282CA35450DDE7C4D81B591DFB9030
SHA-256:	44CFD507B9B3A8174AE6C738051690BE5B88947F85E242E0052CFC50B9805491
SHA-512:	54C134DD4AFF55F985035FD19811C6E77FFBBB4A50258C6F58748BF7E179D07659E2887559112E1A16720F47CA8FF4E1A5745E8A6472576F460778075610A262
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..`...M/....."#.D..-...A.A..Eo.....h%.^.....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):	5.59414365433801
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVun89lSoltFPddFt1:B2geRHRQaclSaXP
MD5:	56551CE445FF5A447B395F674857ADD4
SHA1:	02B9B77D3AC049A7C6B765424AEEDDDA361717F1
SHA-256:	DF4D6DC0732C33D5715D16C7C83D0D9D205738B19EEA8022283166A9FDF90E11
SHA-512:	0000A7363DFF668863B690A4F668918B7CD162A13AD0225FA64E229DEF1EBAA0374ABD36A0A05A9E395389055C98886F67B50296B9A203E0A6189957822361E4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..'...M/....."#.D[%3-...A.A..Eo.....@..{o]...9o|..qY....T....{ ..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.593021354449434
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVh0/XtlCqkoMktkX4EnNWQ1SUm1:mzyEYOFLvEWdrIOQJlZkoltLEt1S/1
MD5:	147D3EFA9E84499E47CC1282801D3432
SHA1:	F7C7F3E77F2C65D7E8D8B4D530D4831429DF9D23
SHA-256:	F99773D2A68FFA5A2ED2C6741CA7438011AFC66BD7E1E04F65411056F9BAAA9F
SHA-512:	C20A7E37AA7484E00FA9A7A013391C7C6BD59A5B5D42B5627763B08F5CA95911FC363A695E069248AD20BD50ADD4247D824089E46912D43B3081BAF7CAB3BED7
Malicious:	false

Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .^....M/....."#.D...,...A.A..Eo.....4.....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):	5.566774724543403
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuW2/9lYoltTqwlwrqwK+41:wRhmlYawwqGwK+
MD5:	1F1375A26AEC9F46651F8417F11CDBF4
SHA1:	84FB8C569C5212477B68A680230183AC1EE237FA
SHA-256:	D3F7B69DAD8483880DD59112965C98D96BFA8053F0A0A63878742203F9C123BD
SHA-512:	94198E3B622F3F81A8D923A2A0F73317ADF546346C21C0D02550E1734C999A576679E53DE7918B398606AADDA8CEF3C5052F6B04552B6524811D071A33A43672
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .....M/....."#.D.q.-...A.A..Eo.....I.....7...o..a=.98I.....(3. $G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.576893409180775
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuej/laoltKfO441:/RrROk/fj/lxUfL
MD5:	97205B581DA9AFC48422F738EE56AF6A
SHA1:	53B05EEEB385F15B37C1377DB3AE38268503C7D4
SHA-256:	A72E2DCE1D1BE4146D61DF7ED296F027D0ABBF7F59F31067B403AC5294CC41AB
SHA-512:	7588750CC336EBDBBD24249E7A4D9B95371D98D42C53880F0EC7C35D9166F71325643FB9BCB0CC8F41F06E45859C420640DF7563D06946474834C0F3765EC668
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 .....M/....."#.D...,...A.A..Eo.....8.J.....~..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):	5.563247075909488
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVi/9lQdoMktTffzoIN1OFPL4m1:mmDEYOFLvEWXIKlQdoltTffzV1QPLr1
MD5:	41CE1B8098D13509912653989F6E2E46
SHA1:	0A4A0B7A77CF70A80721AC6A70780E824E24202A
SHA-256:	52A28674A857D298105BC5FD9C7B4AA1638603138B1147A79C4DF3A3B4C44A8C
SHA-512:	5B0C099F774118022466BCA280D6A2098DC9A1A2232CCCB0111DB3A5525A0F7486BFD932D384B5F763FB98EAE3E2F319B124519591B365C421764217FC1534C7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .2....M/....."#.D.g.,...A.A..Eo.....C..G.....~]...%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):	5.593670915311761
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvrzul9okoMktOXlm8D6EsEJeUm1:m52YOFLvEWdMAuBiljoltuUEvsEJ41
MD5:	6D346E08B4C3FD2B89B5C6EA0075904E
SHA1:	51FF099D2F66673BEB989C126EEB9D3989D05BF2
SHA-256:	E0D1074FE7C7614AF81B192D2E4ECC17EAE576074D356917A13F6EBDACCE3551
SHA-512:	F0B0BF68AEF77302F4334E496097B0DA6C5035A7145A825C51E10DA586D0E850A735675B40F2465BE45A518EF7086E8480D6FCFEE0D8BF887114E7AFEDAB617A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....M/....."#.DJ.3-...A.A..Eo.....[.....z._a...'.v.....4p3..1.']...A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.548237652556384
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuF59lVP5oltXBt4ong1:6lJRw9lVP5aNL4o
MD5:	5D32A41FD042B70F1F6F17F1DDE791D4
SHA1:	C0E063DA99D6AABC0D9EA9A1B7ADBCC6A7FFDE03
SHA-256:	D07E47012D8EB31E36FC7315E3165E1E3F142773DB5BE6A3C3866040E1F5E74B
SHA-512:	837E4EDB35BD5134B82580AB7964A70A0AB67A65B8D80DEEBE14A4451C095163903ED7903F065AA7D33775227EF434E025F0FBD002A2470052C515870E1E8015
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .....M/....."#.DK.3-...A.A..Eo.....&n.....c}.H7M=M..-.....lx..R.l...}Rl.$q.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.590757964166745
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/luE9j/lY5oltgN16wG1:F8hRrROk/2/lJl
MD5:	9007F7391338D223F8C0E36820FCF866
SHA1:	B26BB5FDE1714E6522D201DC4A72557F1195BD9F
SHA-256:	C138F9E221E3AEE34ED0D26975CE6EAA9986071DE8770C0B1E56FA097DAD7F04
SHA-512:	09BA0D85B56EFE0CDA74F729C2668A151567BAAF50934E55C7B464D4280A6BF3F69AEB249B50297014A1DAD02AE66386C60E63336DF08D91725931D9DFDF586
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....M/....."#.D.O.,...A.A..Eo.....%.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):	5.58619921325221
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrloJUQEulECkoltDeeJli1:ehRcDulECjpeeJl
MD5:	EF9A5AD0642198D1DF3823AA400025DD
SHA1:	5D403C489BB0E046A9B8EACA33ED5F36B3027B76
SHA-256:	345D1647A865F7E347C3902B8202CE5158B4BB23886E578206DAD9153946ACD1
SHA-512:	156D5AC2711E206E69C9E3C4F9B37ABE8B38CC84E88DB374730E1A5A0165F5DAF5675DCA8366290C149344E6DE0B0A690C8AE4A8CD5281848094DFE2A3E365F

Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .#3...M/....."#.D...,...A.A..Eo.....U.....;"./N_,.:C..2....9L.H...3:...A. .Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.564866080502459
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuAj/loKoltTfzgm2d/1:0R+j/lohRR
MD5:	D33DAD7F5E9AF26FEAB7F74939DC1EBB
SHA1:	887172144240129D77F72540AE998A3C4DD58DFC
SHA-256:	647F35DD78A3576E24F149CCDB3B3B140F8864112988B20AE83657CEFA1D3AAD
SHA-512:	5DA96B43D4A0E0D5DE7812114EBE7C8B130B80E9C76A3E56539F872E453592008C1F0332B62F5FFB027DEC465F953512BDBE13C38FA88BA45B5B70B001C70A3 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .E....M/....."#.D...,...A.A..Eo.....)&.....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):	5.585043797161187
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvJ/oKtl9nL0koMktt/9tllGBiaQ562Hvp1:mAElVYOFLvEW1KlXtl9okolttHrx56uj
MD5:	43B4656847AB33EFB2B6F7DA7CA6C584
SHA1:	F49150A5EBE51CD7EE39108D4B0CF1F9997F1084
SHA-256:	E7F261B11CF0C75DE4BAAB30059AD2F42FD8494BCC40C8F09BCB0D66348AAFA4
SHA-512:	0816E0A6F38C995E4206DBE6D8A6F3EFFCA42B2A0E5CDD94543A19E1D91A994865FFF25EC63EFD877AE6F77EF007353404CB6D54630883C996F01F548B29671
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .-....M/....."#.D:..,...A.A..Eo.....Z.....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):	5.612851337520772
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvun1/lwddoltkUDLYtmOZn1:xRBJE1/lw/aPDcFZ
MD5:	5684CBB8B32B68F2AF78AEC80F83FDCB
SHA1:	A113A8C9A41C0A599A408E257CE6FB5949AB3F0E
SHA-256:	8B84892C09CD2394616775E6D86816BCCAE4477492F1333873E5538D7EBA2E2A
SHA-512:	E9BAD0F9515CFBEA38CF51489A2428E943101F95CA37DE5F38FC71EFF99FB8FC6605CFE2B34FE4905744CE3FC5C33D8ABCF5C873CAD9C554D7F9F592D15590 87
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .q-...M/....."#.D.h3-...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):	5.556716827755618
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp75j/IHdoltx8VPu1:BPHb/IHQI
MD5:	53E8FA75DE20A3B2288FC6A1CE4590B1
SHA1:	78091A9A880B80962D063B32BC71C0819EEDB0C5
SHA-256:	0E4574253E15A3E011A75F61A9F9DB7E0755DC8DBA038C1D3B707F95BA128AA2
SHA-512:	5F1139BA8D147922F9B45720A807265455314F97FBF157C0F35DB5D17A9B339610BC39789248EBBBA99959D2F159D77DC28DEA9A56A42E66B144BCF38CE4FEB
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 ..X...M/....."#.D=.,...A.A..Eo.....Pm.q.....L...Im.@.....E.nW...IP..A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.541580938239157
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QQZll9GGoltkwiM3Y1:bJRT9lIlMGa/r
MD5:	7BEA3D576F8A406BF7ACA36B73B69C10
SHA1:	F621D9BBEB77E5FAD35DA8B1FBDE1BDD730C1E5C
SHA-256:	0A98B7C369EE164A49AB7A0B7F40A80F2BA459FA78EC91C22776813B700B508E
SHA-512:	D89FB073912C73C36FE944F6125100C30675237AF21375DB8271706D01BA39BF40F59D9006F15DFB189D4CCD967A22C390A4C8745B432D7C72229FDB6D4AAE7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..c...M/....."#.D...-...A.A..Eo.....V.....M....m+lS..e.....<7.U.P8*.0K.A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.579082231795791
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQX+PtlZnLdoltImjBRCh/41:XRc9Zl3aSmDi/
MD5:	4E7E302DB1B9D1BD237B6B21B609863E
SHA1:	A6AFC1C91502D4A2D396AAA312D0AE198781F8EC
SHA-256:	9203565F9A241EC321C7E3D7B7681AD01BAA68D1176C95AF63C94D1F2D363D12
SHA-512:	CFA75923C91A2E2435862456BDBB0BD48D545F2F29C8C813C86D262ADF6EEBC53A9AD651E8F599D863C1A28F04BB6D38F2BD3AABAB45C4354A514A98FC854 7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .v....M/....."#.Di6C-...A.A..Eo.....9e.....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):	5.5785627727433305
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuUq4nQGoltiHFkULIF4r1:bs6xRkieqps7LIF4
MD5:	D2C9F80E599BCF883E40D2B3C31CEDB1
SHA1:	B37D6F04F135E0CB9AAC76BC68BE9D9079AB6B7A

SHA-256:	8CFEC4BBC37FA8A8E81992AE40C18D60A7A0BC30BA8022900AE7D65401338FD5
SHA-512:	F0A80F38D80352D71861F81A479D8FE83BCFD14324F324AB0EED12C3805EEF1820FE40183FC9A37F624AC3F80B6D2F49D94735105F39C229DF1EEE45617EC0C
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 ..c...M/....."#.D%..,...A.A..Eo.....P...#4..l....5 ...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.537979923769991
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvjAl/lJloMktyttPECcu1isLK5m1:mhYOFLvEWd/aFu+tlzoltyt1EN941
MD5:	A51F73BB8940A6A48821A8F79A00FE8C
SHA1:	42FA17E248417B82239277CA1D6E7F1B05D21114
SHA-256:	8FCF1DDDAECDF9A1E4B51238EB389123603A660BA5BD4D44461AE46E731CE87D
SHA-512:	90B8B6518691D27243D54F52528B4E041CE6BF848EB6E5C76795669BCB9C832BAA2D2A20219D9C09F1FF6E52EAC95084D54313C5EAEC0528744C428D78923A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .q....M/....."#.D..4-...A.A..Eo.....<.....a.f.m.i.o.p..3U5.....^...I.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.536533270628599
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQZulloltyjBMqVd3G4K41:2DRuRbllacjB9Vd2
MD5:	57DD5B475B48CCCFC671EF82014575F9
SHA1:	E60B4DDE0E45AF17C80C68BA9FBC666087666DF3
SHA-256:	521730962D09200B3F0B3C39754BDE5375643D9E275BECF8CF38756240D70794
SHA-512:	7F82BAAD36D891C87CB31389FF2EB50FD30A6B260D743FAA44A79882C25FCB7A052F12768C6E8173786FF7B81AF39E0B9AA8D2AF98E77A32BDB075CCFAD8C5 EB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .u....M/....."#.D9.4-...A.A..Eo.....9.`.....y.$..$.v5j...T...z.]..._S....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.5682582219970165
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QCPtlkKLfolthduA424r1:+RQjtlk+aLsr
MD5:	D259E423E4565354E66AA774817E7625
SHA1:	81390D60DF628244273DCA8F5CCE3CD03C9EBA19
SHA-256:	C52D05D9CEE8D141BBA56BFCF400991EF280E35894BB9FDF429CF25BFDE9A525
SHA-512:	BA4E09F9645510155198C0A4AD7793CAE0DC23EC15B541CFB7C7FE0D3EF6DA5216C24BA494E314227EFCD67FA9DC612B118469ED592CBCDFBADB1CEF781B 04E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..w...M/....."#.D./E-...A.A..Eo.....1.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5090683073698
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAubG29blkoltrll+yC8n1:xhRTZhllkaF/+7
MD5:	136DF171825EF84D65C56F034D5FCF10
SHA1:	907054E06A2C558B94C5C996345819438 70EEA0C
SHA-256:	49F8D3C7B1E741A86E763DA12332F54D9D3EE3FF6F9E40FC4707792132E8F2E8
SHA-512:	0F44396FAA9EDDCADF6E3CB213421E0F37218BF7A7FAF835FF524B6D6896B4D84B23E893EC46AA9355749C2F2142FD26E812E97AF7CB4C3AC655608761F0713
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R..........._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .....M/....."#.D*X.-...A.A..Eo.....s.j.....8.../...;.\\o....1.....+..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.601987563182256
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQfllQolt/4sLmB41:nRrROk/VSllPp4N
MD5:	8D272A2858A1DCAADFF36F5CA2BA2DE3
SHA1:	7E81488EB139935E7754E807FC4BF546AE5D9DBF
SHA-256:	02883A5DCB22FA8FFFAB3FDCFAADC9F4A7F4AB2E847C70274273DDB7A562211F
SHA-512:	F25323B435AC7CFDB42FA34C3695EA040047E159BA153714C51F2A0CE03F3FA2160E72BEDB3CE8A2035AC11B2971880EAA860E07E167B5071A816D562D2327A A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..5...M/....."#.D...,...A.A..Eo.....%.F{..... ./.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):	5.584087802070617
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuy/9j/lM5oltP6dm9741:qxRc+llM5ax6du7
MD5:	421B4ECD282BCC3CCFF39E6F8C1DC312
SHA1:	71EEE857088BF43D128DAF8B88CCAC98001B6EA3
SHA-256:	A51CE2A3A35ABB0AD6F3661AEFFC58CD21EC5D87BE294C3734B2C96AA75E0666
SHA-512:	13E236769D326013EDD0E47E51A267BD725E96980021ECD0EDF21FE4E94EF0125943884E08538A600556C0E56629925A8F31A30D6CE7DAB0478A87F121B8575D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .. ...M/....."#.D>.3-...A.A..Eo.....$S.....U...I.>P...X...x..0U.~;m.x.k.A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.565924245092688
Encrypted:	false

SSDEEP:	6:mMOYOFLvEWdwAPVuX9xtl1foltiOB6Jn1:2R1q9xtl1faw
MD5:	BA5F127416023168C9EC78D17C71567F
SHA1:	6A4D54A98B8D82A848BEB3F525A64B1A4B248E68
SHA-256:	8A754FDB18D6C1AD448C21D8B1614890E9CE9C0A885C567E6445A414898B0F9D
SHA-512:	7C65723B9F5B931710B392CEA79EC860735ED18236A351EDEA03803FA44DA0514FCAC8B52C926A9DBE3B78475DFD30657087CD97DC35B870B9F00F695C96421
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .....M/....."#.D...-...A.A..Eo.....5VS.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.61378273226241
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ8l/foltwQ//qhcsBXlh1:mxRBJQ3l3a8B
MD5:	DF1199385F5A0A26CC5383BA28D37F72
SHA1:	EBD7AAA4439F05F5148C17A4BC73806367656AB3
SHA-256:	8E5279F463A9DD9393CA2FB488886A6C4CC88727C35387F8F65246A96B08C49E
SHA-512:	681659588976E998676BD32B3EBB84DEF2236E135328FC1EBA1879295EA1274AC9C2E1166542094744FCBC7F3FBFD4854E855EEDFF76A2815C5EE2F2FD8C19D E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .[....M/....."#.D.i4-...A.A..Eo....._.....k..`..N3.... ..d..$[.....{.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.574008066506312
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQnlEioltRc3Me/1:3RrROk/sMlE5f
MD5:	815ADC8D3C1B3398FC7EAAF610A2E4CC
SHA1:	DDA80C503D19631F97E3A2B72C7B25609712B411
SHA-256:	8C70F768C711E541B77FDBFC8A4E0970FDEA27CF491B526959C74F7EBD28D48D
SHA-512:	16EF0B96ADAC4C11A8427A081ABFEFE67B95AF5FE43D59B1973E4E8631BE825E37826BA1A67AC53E0A70504D6D8E2B13E7629D22F42B9DCFFD594684C7BC28 0A
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 ..M...M/....."#.D..,...A.A..Eo.....R{.....9Q].8O.z....=. .:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.054955582893257
Encrypted:	false
SSDEEP:	12:al0UGuuajUqEWZG0uXMzl6scEYILh4ssqMd5t7eMvAsgC9qzjiuyGtZ2:aDumUq39uXMfcTXqMXlbos98ihGtZ2
MD5:	0C90E3457F036639BB7630631DAC1B58
SHA1:	F1F114BC382E113238C106AA8B54FBAB43F27F52
SHA-256:	F97B94665B768B5DAC7AF0BCB623719D5689554DDBA83C5DE4A2B14C24FC3C7E
SHA-512:	B331805D86E9837684E097EB3DB94D3F11C0D63AB697550011753347E7FBFE6D8D989FED02175EAB39504DB5E6F3E02434F02513BF23D8FDCBA03D0756173994
Malicious:	false
Reputation:	low

Preview:	.....0..oy retne....).....T.....3.....M/.....v...q.....M/.....C..M.....k.....#...(...k.....]...I.P...M/.....6<|....P...M/.....<...W..J.P...M/.....oB*.P...M/.. .....a.....P...M/.....M/.....;.y~A.....M/.....P....V.....M/.....F..=z;.....M/.....o.....M/.....*.....M/.....2q.....M/.....Gy.'.h.....M/.....k7A.....M/. .....:..N.A.....M/.....;/.....M/.....M/.....P[. q.....M/.....,+..._.#.....M/.....J..j.....M/.....A?.2:.....M/.....q.....M/.....u\]..q....M/.....!...0.o..... M/.....*.....M/.....o..k.....M/.....^.~..z.....M/.....[.i..%.....M/.....+.{..'.....M/.....MV3.....M/.....@..x.....M/.....*)....J:.....M/.....&.S.....M/..... .+.U.!..V.....M/.....D.4.....M/.....~.,.4>.@."..M/.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.054955582893257
Encrypted:	false
SSDEEP:	12:al0UGuuajUqEWZG0uXMzl6scEYILh4ssqMd5t7eMvAsgC9qzjiuyGtZ2:aDumUq39uXMfcTXqMXlbos98ihGtZ2
MD5:	0C90E3457F036639BB7630631DAC1B58
SHA1:	F1F114BC382E113238C106AA8B54FBAB43F27F52
SHA-256:	F97B94665B768B5DAC7AF0BCB623719D5689554DDBA83C5DE4A2B14C24FC3C7E
SHA-512:	B331805D86E9837684E097EB3DB94D3F11C0D63AB697550011753347E7FBFE6D8D989FED02175EAB39504DB5E6F3E02434F02513BF23D8FDCBA03D0756173994
Malicious:	false
Reputation:	low
Preview:	.....0..oy retne....).....T.....3.....M/.....v...q.....M/.....C..M.....k.....#...(...k.....]...I.P...M/.....6<|....P...M/.....<...W..J.P...M/.....oB*.P...M/.. .....a.....P...M/.....M/.....;.y~A.....M/.....P....V.....M/.....F..=z;.....M/.....o.....M/.....*.....M/.....2q.....M/.....Gy.'.h.....M/.....k7A.....M/. .....:..N.A.....M/.....;/.....M/.....M/.....P[. q.....M/.....,+..._.#.....M/.....J..j.....M/.....A?.2:.....M/.....q.....M/.....u\]..q....M/.....!...0.o..... M/.....*.....M/.....o..k.....M/.....^.~..z.....M/.....[.i..%.....M/.....+.{..'.....M/.....MV3.....M/.....@..x.....M/.....*)....J:.....M/.....&.S.....M/..... .+.U.!..V.....M/.....D.4.....M/.....~.,.4>.@."..M/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF5769ce.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.054955582893257
Encrypted:	false
SSDEEP:	12:al0UGuuajUqEWZG0uXMzl6scEYILh4ssqMd5t7eMvAsgC9qzjiuyGtZ2:aDumUq39uXMfcTXqMXlbos98ihGtZ2
MD5:	0C90E3457F036639BB7630631DAC1B58
SHA1:	F1F114BC382E113238C106AA8B54FBAB43F27F52
SHA-256:	F97B94665B768B5DAC7AF0BCB623719D5689554DDBA83C5DE4A2B14C24FC3C7E
SHA-512:	B331805D86E9837684E097EB3DB94D3F11C0D63AB697550011753347E7FBFE6D8D989FED02175EAB39504DB5E6F3E02434F02513BF23D8FDCBA03D0756173994
Malicious:	false
Reputation:	low
Preview:	.....0..oy retne....).....T.....3.....M/.....v...q.....M/.....C..M.....k.....#...(...k.....]...I.P...M/.....6<|....P...M/.....<...W..J.P...M/.....oB*.P...M/.. .....a.....P...M/.....M/.....;.y~A.....M/.....P....V.....M/.....F..=z;.....M/.....o.....M/.....*.....M/.....2q.....M/.....Gy.'.h.....M/.....k7A.....M/. .....:..N.A.....M/.....;/.....M/.....M/.....P[. q.....M/.....,+..._.#.....M/.....J..j.....M/.....A?.2:.....M/.....q.....M/.....u\]..q....M/.....!...0.o..... M/.....*.....M/.....o..k.....M/.....^.~..z.....M/.....[.i..%.....M/.....+.{..'.....M/.....MV3.....M/.....@..x.....M/.....*)....J:.....M/.....&.S.....M/..... .+.U.!..V.....M/.....D.4.....M/.....~.,.4>.@."..M/.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2212091006332-391.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, cbSize 65110, bits offset 54
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	0.5648740687125007
Encrypted:	false
SSDEEP:	768:f000000000000000000000000000000000000000000000000000000000000000c:4
MD5:	42AC886F3F697B74D8A53773FF9E6243
SHA1:	EA28ACBDE2BA9171A485E79E60B2675217640215
SHA-256:	D3BD1B835AE1D23CEAD6256ED8D08831595DBB84AEE5E2C749443F0F6B56E133
SHA-512:	EF1F900A3EACF5D9D837656EE3CB4C339E6C33A1FFFFD69008891A022EC0DA8B91550B78628B9A16BAD6656F40A3FB86B1EBA4834ADE341C64B4EB8A390DEC5A
Malicious:	false
Reputation:	low

Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000, file counter 16, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 16
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.5676561304813363
Encrypted:	false
SSDEEP:	384:XeT9dTh9tELJ8fwRRwZsLRGlKhsvXh+vSc:mkYZsLQhUSc
MD5:	73F55AD5081EC44C0FA2722EDB6C2F5A
SHA1:	C514FECE88C9C7DC4F06189F9169AAA029EC898E
SHA-256:	93326556D1B9F0BFA386614CED82C8B4CCAEA6E8224281B8686237F4BCAA9777
SHA-512:	750B8282D61AEE8C0A8D1C26C939C3BD61CB242DF05B5CCDF84197D5A5FCF633C44BC8CC2B496B7DB6584936ADFD6BCE7DEB4CEE22BCF7B5797934407248 85D
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.3185248830252903
Encrypted:	false
SSDEEP:	48:7MeT2iomVQYom1Cuiom8Vom1Nom1Aiom1RROiom1Com1pom19iomVKiom4SRqQl8:7ICguOhhCKsN49lVXEBodRBkl
MD5:	09D865EB6DE36EA4944FEE68C127C4DA
SHA1:	3D954B7F09A2D67CDC1C9AA20658ED4E2FA75393
SHA-256:	2AA453C6D1D99C333EDCE7B6056CE0C26176AB19D23ECA484B25A7942D9BC4B8
SHA-512:	035BFEFAD2241CCB8230F53358D0F19E1B0372F1F40A1D9D27C27A2AFFF0D6A3919DF6605C944B6627609676026CB00160DCB1692252B917BA7E90C5614D618F
Malicious:	false
Reputation:	low
Preview:	.... .c.....P..... .....W....<.W.L...y.....~..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZbRK43hLbuTmMsMh7TgSBFTqYyu:J0GpiyVFihbRK4xLCCZMh9qK
MD5:	BFC1D46DC3AB8D7B3BFE4B4F708DA23C
SHA1:	19B2B7B1270D3BF7CAAA624249F87D383B023FA8
SHA-256:	16CAEC3AD77EAA056FF54AD407CF49EAA1E8FE25C918ECEC46A2CD08F37F355A
SHA-512:	BE1BC8571B179631C587E5D2B80D7632118DCA3C1948F823441D16320482CC57ED4648EF72B83BA0159B93E3135A8F33CD672C651BAE949988557DF92BFCFF8
Malicious:	false
Reputation:	low

Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narr ow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial .L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\Downloads\21f6f8e2-c457-4f9e-b65e-185755c07296.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.7, 35 pages
Category:	dropped
Size (bytes):	3730
Entropy (8bit):	6.498082419952405
Encrypted:	false
SSDEEP:	96:yiV4vdML05/LhnjbPowaO/3uDnmDo9MjGehJZ3yoj0weLNy5N9yx3lNYpwYK9ZJU:yiVsML05/LhnjbPowz/9DZjGehJNyosQ
MD5:	DDC105DFB8D596DC678D15703388BA79
SHA1:	83E1F0A7508D9258E8ECA65CF5CD6C8AAEFF494A
SHA-256:	BB83417447802FFF62121971017F348B190E60E19337F23D1029DA2C80632C7B
SHA-512:	3F8C3990915B927262C540FAD20357E6F81E43F5BBD8B265FA1205A02A1EF28E1F955C0806B634B34EC31EB1EABAFBCA4AC24D1CD1F130BA48573D05313D2D C
Malicious:	false
Reputation:	low
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 213 0 R/Outlines 130 0 R/MarkInfo<</Marked true>>/Metadata 1747 0 R/ ViewerPreferences 1748 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 35/Kids[3 0 R 16 0 R 22 0 R 24 0 R 26 0 R 28 0 R 30 0 R 33 0 R 34 0 R 35 0 R 36 0 R 37 0 R 38 0 R 39 0 R 40 0 R 42 0 R 48 0 R 50 0 R 52 0 R 56 0 R 59 0 R 62 0 R 63 0 R 64 0 R 65 0 R 66 0 R 67 0 R 70 0 R 71 0 R 72 0 R 73 0 R 74 0 R 75 0 R 77 0 R 81 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/ProcSet[/PDF/Text/I mageB/ImageC/ImageI] >>/MediaBox[0 0 595.25 842] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 882>>..stream..x....o.0...#.?.1........n.G.n .a..k).(...i..wgRV ..M..+.\..|....{.L..Q...C.....tD..a.{V.....)....e..%..RS..S.....~+..s.ie..1..A_..U.. '..}....$#/.Jz....N..[.....

C:\Users\user\Downloads\ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.7, 35 pages
Category:	dropped
Size (bytes):	1293208
Entropy (8bit):	7.958630832443152
Encrypted:	false
SSDEEP:	24576:jge3HoEj4GZ+YobvYuV7xSI+OroaF0I65Pdqs4egD/:8kH2GobQuVNSI30I65PdbuL
MD5:	D7B65868F43D1D3D867B0223C4D60ECB
SHA1:	371137A2E55B48ECB6C5F076C392854E592A528B
SHA-256:	FC0D0652E22AFEC12B7F73638036B1A22909BA0114BDBC5F78980180A2358899
SHA-512:	09145209278AA6ED3439D71E009AF1D4863489A9F69523D5A8CAB1A13DE16E4E9015AC440F4C5B4687393629C76F18506748F1B59005F64FF158822263D49FD3
Malicious:	false
Reputation:	low
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 213 0 R/Outlines 130 0 R/MarkInfo<</Marked true>>/Metadata 1747 0 R/ ViewerPreferences 1748 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 35/Kids[3 0 R 16 0 R 22 0 R 24 0 R 26 0 R 28 0 R 30 0 R 33 0 R 34 0 R 35 0 R 36 0 R 37 0 R 38 0 R 39 0 R 40 0 R 42 0 R 48 0 R 50 0 R 52 0 R 56 0 R 59 0 R 62 0 R 63 0 R 64 0 R 65 0 R 66 0 R 67 0 R 70 0 R 71 0 R 72 0 R 73 0 R 74 0 R 75 0 R 77 0 R 81 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/ProcSet[/PDF/Text/I mageB/ImageC/ImageI] >>/MediaBox[0 0 595.25 842] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 882>>..stream..x....o.0...#.?.1........n.G.n .a..k).(...i..wgRV ..M..+.\..|....{.L..Q...C.....tD..a.{V.....)....e..%..RS..S.....~+..s.ie..1..A_..U.. '..}....$#/.Jz....N..[.....

C:\Users\user\Downloads\ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PDF document, version 1.7, 35 pages
Category:	dropped
Size (bytes):	1293208
Entropy (8bit):	7.958630832443152
Encrypted:	false
SSDEEP:	24576:jge3HoEj4GZ+YobvYuV7xSI+OroaF0I65Pdqs4egD/:8kH2GobQuVNSI30I65PdbuL
MD5:	D7B65868F43D1D3D867B0223C4D60ECB
SHA1:	371137A2E55B48ECB6C5F076C392854E592A528B
SHA-256:	FC0D0652E22AFEC12B7F73638036B1A22909BA0114BDBC5F78980180A2358899
SHA-512:	09145209278AA6ED3439D71E009AF1D4863489A9F69523D5A8CAB1A13DE16E4E9015AC440F4C5B4687393629C76F18506748F1B59005F64FF158822263D49FD3

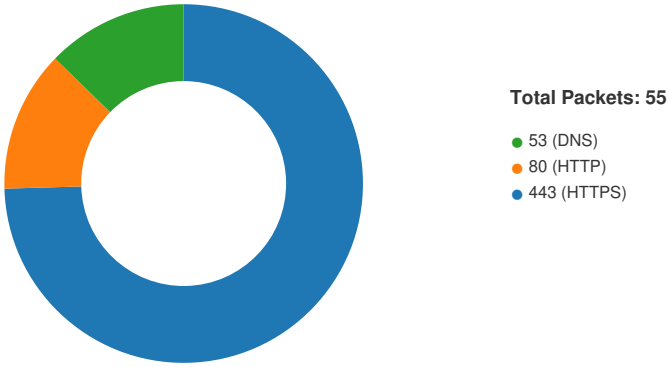
Malicious:	false
Reputation:	low
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 213 0 R/Outlines 130 0 R/MarkInfo<</Marked true>>/Metadata 1747 0 R/ViewerPreferences 1748 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 35/Kids[3 0 R 16 0 R 22 0 R 24 0 R 26 0 R 28 0 R 30 0 R 33 0 R 34 0 R 35 0 R 36 0 R 37 0 R 38 0 R 39 0 R 40 0 R 42 0 R 48 0 R 50 0 R 52 0 R 56 0 R 59 0 R 62 0 R 63 0 R 64 0 R 65 0 R 66 0 R 67 0 R 70 0 R 71 0 R 72 0 R 73 0 R 74 0 R 75 0 R 77 0 R 81 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/MediaBox[0 0 595.25 842] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 882>>..stream..x....o.0...#.?.1.....n.G.n .a..k).(...i..wgRV ..M..+.\..|....{.L..Q...C.....tD..a.{V.....)....e..%..RS..S.....~+..s.ie..1..A_..U.. '..}....$#/.Jz....N..[.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:17.721559048 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.721641064 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.721731901 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.722579956 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.722620010 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.722685099 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.723705053 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.723747015 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.723808050 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.724040985 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.724081993 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.724147081 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.724725962 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.724776983 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.724879026 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.724905014 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.725248098 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.725279093 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.725450993 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.725475073 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.849877119 CET	443	49696	142.250.184.45	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:17.879705906 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.882530928 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.890572071 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.920546055 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.923548937 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.930785894 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.930838108 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.932554960 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.932735920 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.936098099 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.936263084 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.944539070 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.944582939 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.945208073 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:17.945230007 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.946103096 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.946209908 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.948276043 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:17.948430061 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:17.948580027 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:17.948648930 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:18.024632931 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:18.230916977 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:18.231051922 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:18.866000891 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:18.866072893 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:18.869571924 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:18.869654894 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.287492037 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.287512064 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.287795067 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.288083076 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.288144112 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.288275957 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.288312912 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.288356066 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.288391113 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.288446903 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.288469076 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.288497925 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.288523912 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.288671970 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.288701057 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.288734913 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.331237078 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.331363916 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.331401110 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.331621885 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.331731081 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.333884001 CET	49697	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.333921909 CET	443	49697	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.335935116 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.335973024 CET	443	49693	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.354101896 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.354237080 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.354316950 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.380414963 CET	49696	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.380460024 CET	443	49696	142.250.184.45	192.168.2.4
Dec 9, 2022 11:06:19.398720980 CET	49698	80	192.168.2.4	52.219.169.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:19.426714897 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.426778078 CET	443	49694	142.250.180.174	192.168.2.4
Dec 9, 2022 11:06:19.435705900 CET	49693	443	192.168.2.4	142.250.184.45
Dec 9, 2022 11:06:19.441450119 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.462388992 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.462467909 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.462776899 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.481657028 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.526727915 CET	49694	443	192.168.2.4	142.250.180.174
Dec 9, 2022 11:06:19.534967899 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535037041 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535093069 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535151005 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535161018 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.535197020 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.535204887 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535260916 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535306931 CET	49699	80	192.168.2.4	52.219.169.25
Dec 9, 2022 11:06:19.535316944 CET	80	49699	52.219.169.25	192.168.2.4
Dec 9, 2022 11:06:19.535371065 CET	80	49699	52.219.169.25	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 11:06:17.134203911 CET	56572	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:06:17.136765957 CET	50911	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:06:17.153112888 CET	53	56572	8.8.8.8	192.168.2.4
Dec 9, 2022 11:06:17.155781031 CET	53	50911	8.8.8.8	192.168.2.4
Dec 9, 2022 11:06:19.305644035 CET	64167	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:06:19.322478056 CET	53	64167	8.8.8.8	192.168.2.4
Dec 9, 2022 11:06:20.310089111 CET	56807	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:06:20.329188108 CET	53	56807	8.8.8.8	192.168.2.4
Dec 9, 2022 11:06:20.332818031 CET	61007	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:06:20.358411074 CET	53	61007	8.8.8.8	192.168.2.4
Dec 9, 2022 11:07:20.375962019 CET	52437	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:07:20.403656006 CET	53	52437	8.8.8.8	192.168.2.4
Dec 9, 2022 11:07:20.406656027 CET	52825	53	192.168.2.4	8.8.8.8
Dec 9, 2022 11:07:20.423614025 CET	53	52825	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 11:06:17.134203911 CET	192.168.2.4	8.8.8.8	0x1b24	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:17.136765957 CET	192.168.2.4	8.8.8.8	0x8577	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:19.305644035 CET	192.168.2.4	8.8.8.8	0x6905	Standard query (0)	s3.eu-central-1.amazonaws.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:20.310089111 CET	192.168.2.4	8.8.8.8	0x6bb4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:20.332818031 CET	192.168.2.4	8.8.8.8	0xa15e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:07:20.375962019 CET	192.168.2.4	8.8.8.8	0x5be4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:07:20.406656027 CET	192.168.2.4	8.8.8.8	0x758b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

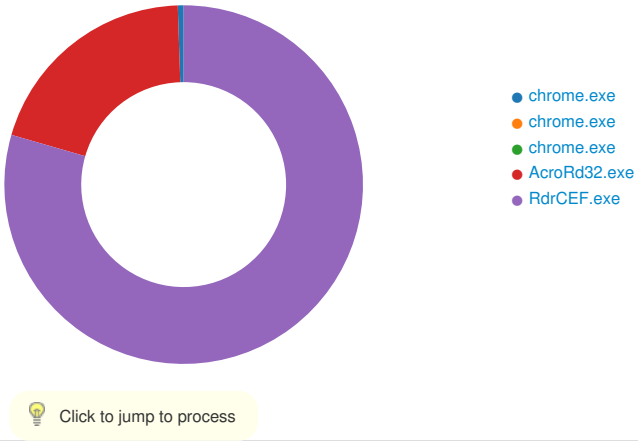
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 11:06:17.153112888 CET	8.8.8.8	192.168.2.4	0x1b24	No error (0)	accounts.google.com		142.250.184.45	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:17.155781031 CET	8.8.8.8	192.168.2.4	0x8577	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 11:06:17.155781031 CET	8.8.8.8	192.168.2.4	0x8577	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:19.322478056 CET	8.8.8.8	192.168.2.4	0x6905	No error (0)	s3.eu-central-1.amazonaws.com		52.219.169.25	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:20.329188108 CET	8.8.8.8	192.168.2.4	0x6bb4	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:06:20.358411074 CET	8.8.8.8	192.168.2.4	0xa15e	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:07:20.403656006 CET	8.8.8.8	192.168.2.4	0x5be4	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Dec 9, 2022 11:07:20.423614025 CET	8.8.8.8	192.168.2.4	0x758b	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- s3.eu-central-1.amazonaws.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **2224**, Parent PID: **4728**

General	
Target ID:	0
Start time:	11:06:13
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5932**, Parent PID: **2224**

General	
Target ID:	1
Start time:	11:06:14
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1640,i,10835741753073723708,5021152820849143339,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4692**, Parent PID: **4728**

General	
Target ID:	2
Start time:	11:06:15
Start date:	09/12/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://s3.eu-central-1.amazonaws.com/fiae/Beispiele/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: AcroRd32.exe PID: 6764, Parent PID: 2224

General	
Target ID:	3
Start time:	11:06:19
Start date:	09/12/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Downloads\ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf
Imagebase:	0xd0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1065C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	12AE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	11EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-221209100633Z-391.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1983C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1psdso_vbye37_5bs.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	4	11EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rhhnjad_vbye38_5bs.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rg3vbxo_vbye39_5bs.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R27frjz_vbye3a_5bs.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1xp7dvl_vbye3b_5bs.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	11EA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	11CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	11D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	11D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	11D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	DEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	DEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	DEA55	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Downloads/ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	ProjektdokumentationFachinformatikerAnwendungsentwicklung2021AndreasKretschmann.pdf	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	12DF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	12DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 6F 77 6E 6C 6F 61 64 73 2F 50 72 6F 6A 65 6B 74 64 6F 6B 75 6D 65 6E 74 61 74 69 6F 6E 46 61 63 68 69 6E 66 6F 72 6D 61 74 69 6B 65 72 41 6E 77 65 6E 64 75 6E 67 73 65 6E 74 77 69 63 6B 6C 75 6E 67 32 30 32 31 41 6E 64 72 65 61 73 4B 72 65 74 73 63 68 6D 61 6E 6E 2E 70 64 66 00	success or wait	1	12DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 32 31 32 30 39 31 31 30 36 33 32 2B 30 31 27 30 30 27 00	success or wait	1	12DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	1293208	success or wait	1	12DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	35	success or wait	1	12DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	12DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	12DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	12DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	12DF69	RegSetValueExW

Analysis Process: RdrCEF.exe PID: **6652**, Parent PID: **6764**

General

Target ID:	4
Start time:	11:06:27
Start date:	09/12/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0x1190000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	12859E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	4	12983E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	41	1298447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	110	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	12	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	8	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1087	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	30	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	5	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	12859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	2	12859E2	ReadFile
unknown	unknown	4096	success or wait	1	12859E2	ReadFile
unknown	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	12	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	10	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	27	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	30	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	44	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	27	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	10	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	2	12859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	9	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	10	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	143	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	134	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	97	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	3	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	84	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	8	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	162	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	75	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	2	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	6	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	15	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	4	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	1	12859E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	1	12859E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	12983E5	ReadFile

Disassembly

No disassembly