ID: 778232
Sample Name:
Cancellation_418406_Dec23.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 09:01:23
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

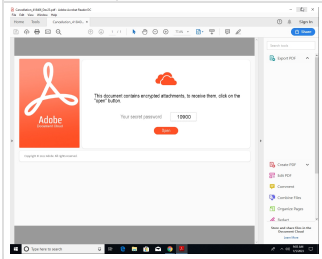
Windows Analysis Report

Cancellation_418406_Dec23.pdf

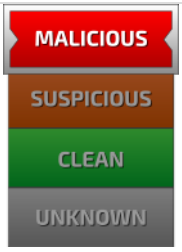
Overview

General Information

Sample Name:	Cancellation_418406_Dec23.pdf
Analysis ID:	778232
MD5:	c085bbddc02251..
SHA1:	98d3377ff32441e..
SHA256:	ca2d98108f12fb4..
Infos:	



Detection



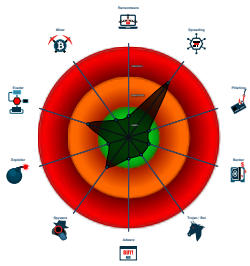
Qbot Downloader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found potential malicious PDF (bad…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected Qbot Downloader
- Clickable URLs found in PDF pointin…
- Creates a DirectInput object (often f…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Internet Provider seen in connection…
- Sample execution stops while proce…
- Creates a process in suspended mo…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 2156 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Cancellation_418406_Dec23.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5448 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 7152 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 2364 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1948 --field-trial-handle=1812,i,5445074810738567 73,15156316211615148029,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - unarchiver.exe (PID: 6076 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\Cancellation_367461_Dec23.zip MD5: 16FF3CC6CC330A08EED70CBC1D35F5D2)
      - 7za.exe (PID: 5296 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe" "C:\Users\user\Downloads\Cancellation_367461_Dec23.zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
        - conhost.exe (PID: 5312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Qbot Downloader

```
{
  "Download Url": "http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Cancellation_418406_Dec23.pdf	JoeSecurity_Qbot Downloader	Yara detected Qbot Downloader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Spreading

Yara detected Qbot Downloader

System Summary

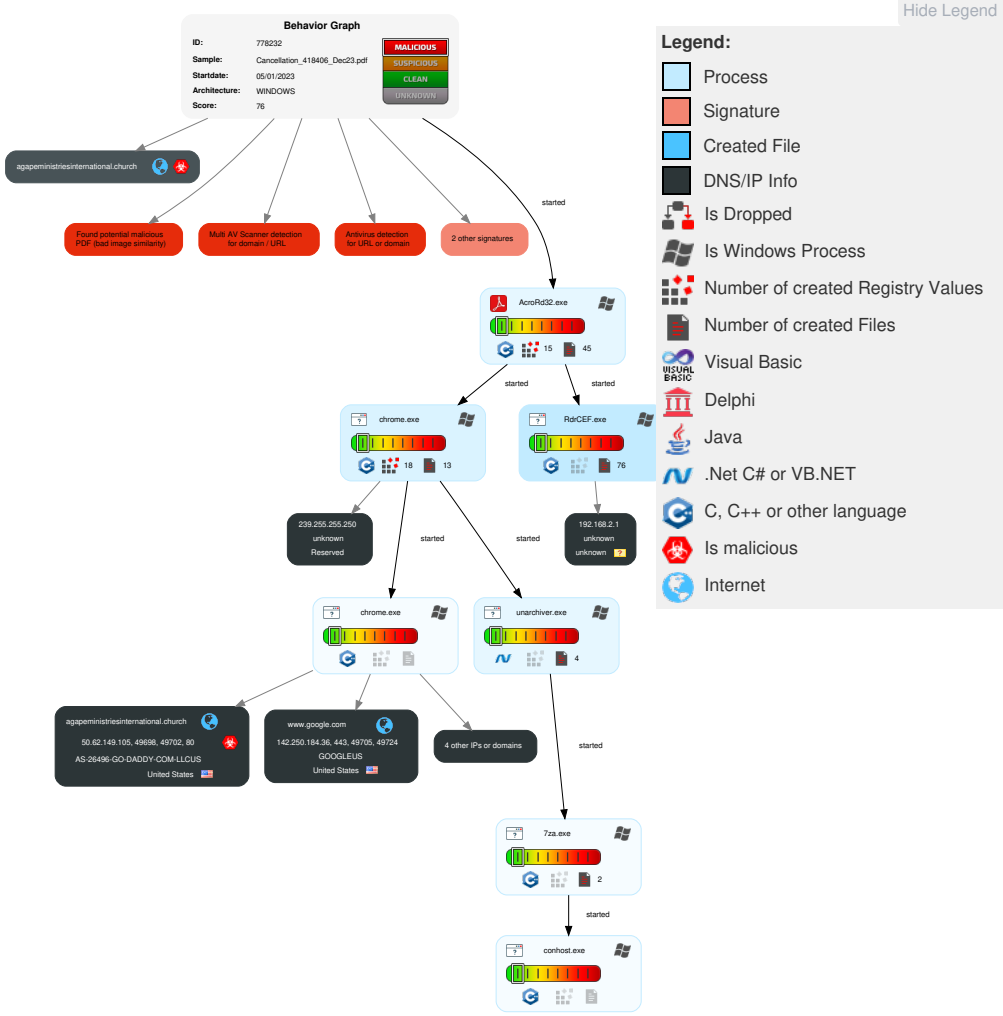
Found potential malicious PDF (bad image similarity)

Clickable URLs found in PDF pointing to potentially malicious files

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
1 Spearphishing Link	Windows Management Instrumentation	Path Interception	1 1 Process Injection	3 Masquerading	1 Input Capture	1 Virtualization/Sandbox Evasion	Remote Services	1 Input Capture	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 Virtualization/Sandbox Evasion	LSASS Memory	3 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 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)	1 Disable or Modify Tools	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 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)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

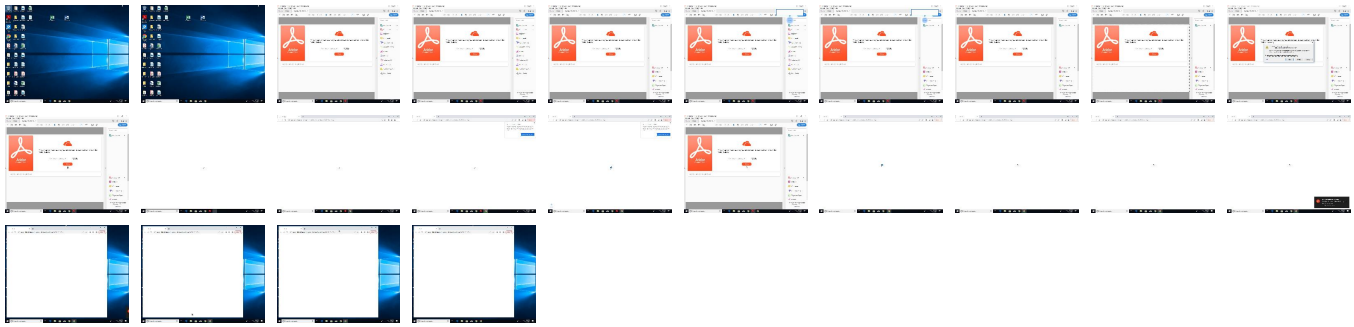
Behavior Graph

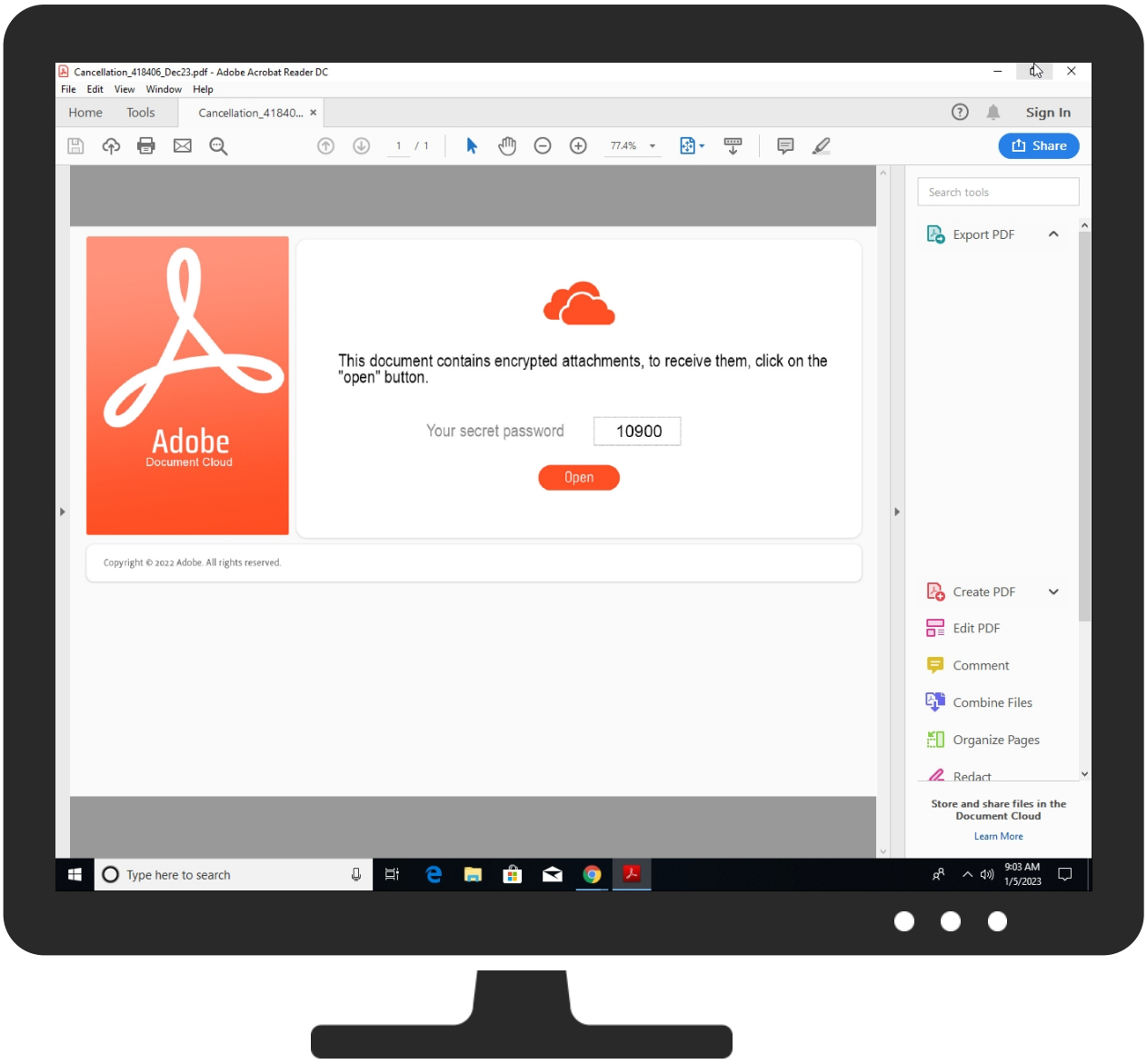


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
agapeministriesinternational.church	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip	100%	Avira URL Cloud	malware	
http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip)	0%	Avira URL Cloud	safe	
http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip	16%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
agapeministriesinternational.church	50.62.149.105	true	true	• 3%, Virustotal, Browse	unknown
accounts.google.com	142.251.209.13	true	false		high
www.google.com	142.250.184.36	true	false		high
clients.l.google.com	142.250.184.78	true	false		high
clients2.google.com	unknown	unknown	false		high

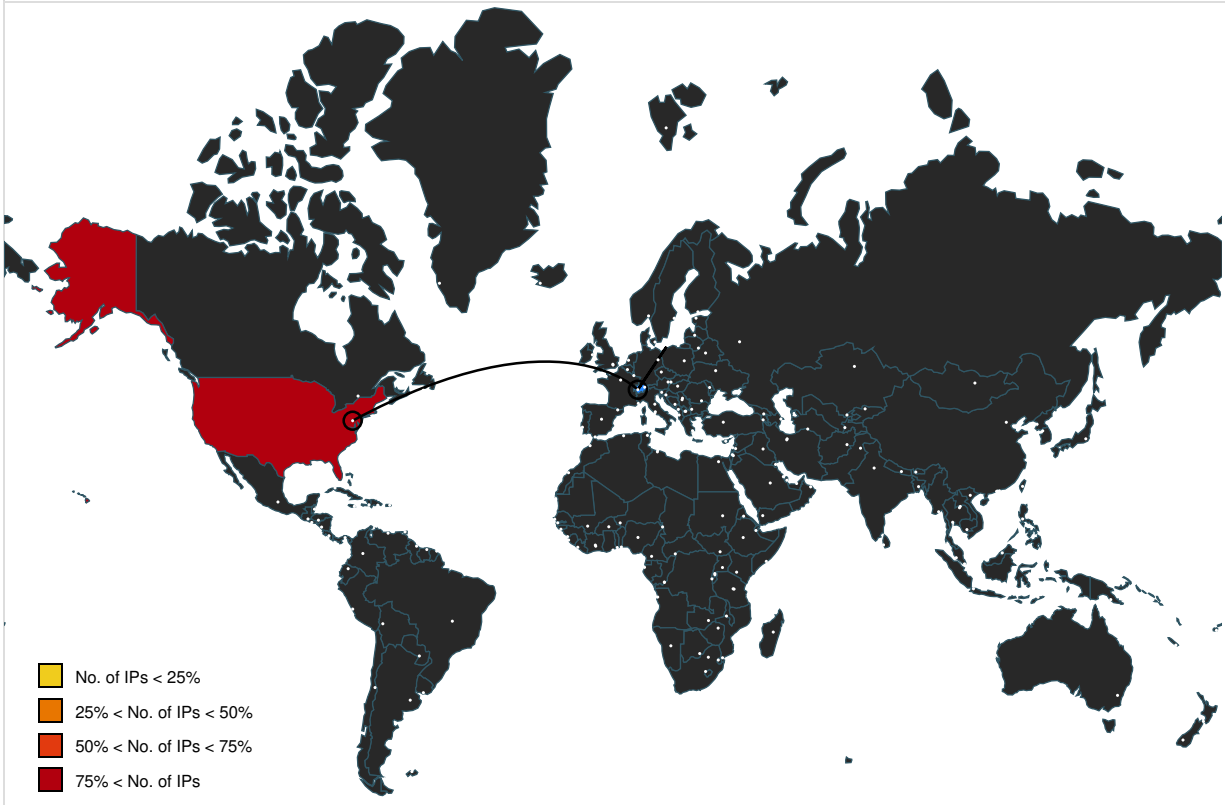
Contacted URLs

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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip)	Cancellation_418406_Dec23.pdf	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.62.149.105	agapeministriesinternational.church	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
142.250.184.78	clients.l.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.251.209.13	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.36	www.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:	778232
Start date and time:	2023-01-05 09:01:23 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Cancellation_418406_Dec23.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
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:	23
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:	MAL
Classification:	mal76.spre.winPDF@38/57@5/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Security Warning found • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.21.22.155, 2.21.22.179, 23.211.4.250, 142.250.184.35, 34.104.35.123, 142.250.184.67
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, fs.microsoft.com, armmf.adobe.com, edgedl.me.gvt1.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, a122.dscd.akamai.net, update.googleapis.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
09:02:21	API Interceptor	1x 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):	5.621995976318026
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVlfl/1lQRktyrVNBiTFJrqzOJkvP5m1:men9YOFLvEWdM9QKftvPtYvi7Z+P41
MD5:	05A8ED13DB8ACF9593227A84C5C6FF47
SHA1:	6414B2E11A5C6EDA3AEDDF90585DC7AB6AA8817E
SHA-256:	6AD07D48B525B5EBE2DE9B7C4A074C01C366CCDD01080F8F65C378B8089C4227
SHA-512:	A392B1984BB041DB20B9AC85C423966E8D67F40D5774D82B9313626CB5F428454BD88C77D5CC82CC6DE18DC7EDB1BE95C6DAF387C92F19AB2AA799C613B4AE4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..mQ..P/....."#.D5.3....A.A..Eo.....KX.....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):	5.576331272896254
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVeofl/Tk9kRktWfO98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEk5tT0jtV8Be7Ywcr1
MD5:	7F55774458FA8EA992A4750965A14D93
SHA1:	1B5B39ACACE70F1BC54D1746E2C8CC05D59E2028
SHA-256:	03A014EF976E41BDA70EBB3EE3775CDBF07AF033A808EE9DE7D3CDCEE58546B9

SHA-512:	5A413BEF7E1445D5C3A2E6D9026B07B7450BF322AC34B4E8C4CEF7EF39D02A177955B60F40C4A8DDDF72CA3A664C1EA59098D1110F79335805EC66A13DFA74 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ..N9..P/....."#.DS.....A.A..Eo.....1.x.'.vl..*|Z..o...+.4....0..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.567684396308422
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuLm1u6OQt7XHmt/RlUoSjGY1:DyeRVFAFjVFAFXx9QFXGtZlUo6
MD5:	97CD0EFE5E2B8A3D74AEEE4842308710
SHA1:	8AA2676E49EE270AF8120524244A7BE5B58D3991
SHA-256:	3FDACB1B6DB3BC8535408C9A2598E2C9C9E6F84901CD5060A56CF2E9B9197ABC
SHA-512:	D40DC4F1773DDB3E1622493F6BBA336A01F0FE7C56A56659E9AF7AC55C99BC1314BA8EA9F92F70465F35E8EEE86277F64FCA7F02D87B2DA7743C88CAC757F5 1
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 ...O..P/....."#.D..-....A.A..Eo.....Y. .2.....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):	5.64887853183383
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsbH4A1Di9tGuiWulHyA1:lbRkiD6HH1+QjWus
MD5:	9EA125E9CF4BD143066AA72AB2D1D403
SHA1:	434C1A2C729CA4D40154E9F98FAE727767E4263D
SHA-256:	7A04211A73C7169FD4EB1FCC0D0B5B46198EAC7A4D233AC37E4F95394E1D3837
SHA-512:	7E4DEA9B51E264FE3D356B928F068C50C84D5BE07EFE1970830BC2E2D7AF1481B3C4AA6B75634A5AFAA637922BD6CF41E08C22221F60287E9CB22D010E2F1C C
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .>w...P/....."#.D.z:....A.A..Eo.....8 P..a...R.. Y....7.@..2Dm{..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.512939302571262
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuQtItiGVyh9PT41:pyixRu3EGV41T
MD5:	A17F44A872680C207579A1A086788A99
SHA1:	9119588BADE75F7BBB909798C3048D4C78C49DED
SHA-256:	1ADD7711FDD7361A04F6F0680525B5529853D3CA300BA69DF0555322800DC321
SHA-512:	37C865F8FE9EC955A5DD7E71A57D266389E0858444C294AC2005196977E79CBE631334E5D9526A61C789DC24851FB33A4ED7ACB2C5788F7945466DBA185F7C2
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..MP..P/....."#.Dk.....A.A..Eo.....(G.....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:	modified
Size (bytes):	216
Entropy (8bit):	5.612388645423502
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQo4e8Bl9t6P/73Zll6P41:0RhkMl9aDZ
MD5:	FF6F0A6F4A92165C2750003E38D98901
SHA1:	C9C78B3F5200C167C28357E2BE0DDD05A4D080CB
SHA-256:	73708B5FC326A0EF2172354612B07BB86E42C2515AD5F624344CC7BB9ED294C8
SHA-512:	B836830D4B854BF2693E5BD6E6F24718E0432E5C6DF47AF363A6C03F4D93A6B2917EF62AD013C34F7D10702BD2F06CC26E942980F8CB7D1AE528CFA0E529565
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..EJ..P/....."#.D.....A.A..Eo.....:.....].>....uUf..N...k.....c..I.A. .Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.523770318520741
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuV2ll/X59Il9k6RktNcyxMtv9G:mJYOFLvEWdGQRQOdQ7tp9Ok9tND6g1
MD5:	C8E82FEB22D90B3991337437F2948FC4
SHA1:	8691CD0E6A3068871B3233EC70C7BA714160B08B
SHA-256:	7C752F349B50EBC49C0ABE460515311ADF5CA8291298F7EBFFB4BC8197A69910
SHA-512:	B2FDCBB762EC76A2D01B4CF75F798E5E37E7EBDEB2A791852AC9A4E68DB99E54EE84335086F621ECB6EEFA34A9B949B029820CA021101D51CC3958A79BBC0 D2B
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..^P..P/....."#.D.....A.A..Eo.....g.....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):	5.5990078596133435
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVeoH/l/NKqkRktg/l/VQMWqg4nRb7om5m1:mOYOFLvECMLPt8qjtg2uR/41
MD5:	3825DDDE75117D171E71E5A458925227
SHA1:	888D0794E3A82F286534336C13E2C1BE72DAC204
SHA-256:	5A710A6D29EC4856CDBDECF5DD80C0B4E6C50D9648F8F83670AEC94661FEA8EF
SHA-512:	018C790C06BE9DA972F4AAC61CE76B1E0865C64F973A93858F7455656ECAD0AC99925A5870BC1B69F6682FD7936F088B030037495E908B6DEBC76690908AD088
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .N.9..P/....."#.D.....A.A..Eo.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.645116909414164
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu9p9tXMGm0bbsIDMGH41:XfRM75MVKsIZ
MD5:	49C5D81D91FB71BC30A6194FF1EC9511
SHA1:	CD1CF4B7CAF5310114F568DCBEFAE30B5E6BEDB9
SHA-256:	013C484B65CF375E55A8D23396A38B83215541C89C688F95620783DFFC1A9824
SHA-512:	A2386258025F2A536DCE5A8D478B85F393683FF9CDEB65AADC05A35DD55CAD7EA00EB50B94C4C7B865AF0C2CB1E1893DB6B5CF063A62232FE7A6E32A27641 37
Malicious:	false

Preview:	0\r..m.....T.....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .....P/....."#.D8Mh....A.A..Eo.....Vw.....`.....^....L>..Xa./.....C.y.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.50823459567584
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuio41atOqKjtEhby0zBUKSAA1:pRHlAQ5ahb
MD5:	95844A96114E25247A2FF70296381B8F
SHA1:	9B7C3175BEA13C18EEBF7773A2978D94304F467B
SHA-256:	6DC9AF2C8078322C1D3F029FB277C539B1EC9C81E9B14A7F9D5BAAAAA501395B
SHA-512:	BC6B9BC933D31484E0A1024A9062CA179A23158983B69EF7433A9557BAFEE6053F10C0C2925A2D7C5DBA089D5F834B2E1F546A586325C33149031865BAC742BD
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ..Q..P/....."#.D../....A.A..Eo.....N .....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):	5.464478515173832
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvrZ4Al/cbekRkt/gulWd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvV4Atcbejt/LlWs
MD5:	3B017F44D6937A232DAF337527007722
SHA1:	BF073D4A3478DEB49B19168951EB4AF5BAE00BCB
SHA-256:	846C8930FE818F33EE410564FFEE3DCF8373729EC527BACB7178BEDE5FB9988D
SHA-512:	04634D17981352204AD8D850BDF187F0447A9B3ED828B785D4EC6978C4308E2898F558111D3FB8664783569262E8FCB76D109F095A0589F3ADC5234DB4833798
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..9..P/....."#.D.....A.A..Eo.....oA.....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):	5.537214904794677
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLaOjval/JAT9k6RktxfNFtRUPqf9tsDMam:mkl9YOFLvEWsfOLaOjatEStx4PqVyM+e
MD5:	8BE056AB92C0B0E86E8B813D483AEE4F
SHA1:	57DAB50CBD799FC1602E10CAF834A0E6B7B9DA81
SHA-256:	2117ABF959441BA292E84E00F16C4EB5238A05694E58675FF05014FB198A55E6
SHA-512:	01AC1479A0393075FC49F4C16753A4A10C37CBEA13DE3F40C7A6637F5A647F7556F603279191C1EF481F9D30B95278E99859666FF58D73A98AD74CAACF4BC7C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...F..P/....."#.D.....A.A..Eo.....`z.....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):	5.592823378418027
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyDMtK5BtZtwSeKaT9pr1:URVFAFjVFAFq5BjtwSeKaTL
MD5:	F84876297A72BEB1651728C1BFBC1656

SHA1:	C3A6235941079B657A7FA71E9F18BD0D781F76D0
SHA-256:	0D817919DDD0781C329CA59BF7825F621614506EEF0BEA06D02A38809444055A
SHA-512:	979A592311103B859550302B63A4C504E702902B57D78B79C3ADBEA59159081EE0F754A1DCB1B004FB557A13EF420E28DD8261D040A1B4BDBFCE04C4CB074DD7
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .Y\P..P/....."#.D..9....A.A..Eo.....8{T. .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.542565577661833
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQWZ1iltM0t5GFCaa+41:NRMHdjZUlS0t5Gda+
MD5:	2B30A71A95636FB7EB31ABBCD30914B1
SHA1:	EBCEB28F0DABD913F71C8E970B226DB750CE72A3
SHA-256:	3ACA663CF9476B74AA3AB2974971668E9CD3D7C33D66D1D107FD167C0E3FE949
SHA-512:	05753E498D442AC0C5CE4CA1074DDA1343D0BE042426C835378B74E3016015EE6DE30C2731B1F2D7DF938E72D92683703F706613049DF436D0383091E0891A9E
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .....P/....."#.D..i....A.A..Eo.....#.g.....G.3D.....Q.g0...._.Q.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.503044010207524
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvq5Ll///RktWfJyrpYFm1:ms2VYOFLvEWdvBIEGdeXucRXKtWA11
MD5:	EAC791EA906DFF9FFFE142A9C3128082
SHA1:	1E64D921644E4255D83F8628BCF5B854D92E1CDF
SHA-256:	86A99F42FCA4331C519705EB534CDA3D56D404D6725BCD7425DB4AFB964E002B
SHA-512:	4BC2B0C9F5EB356D3BE2FE90EE03B51313034B26598DAF27FBA4D0A4A4DA47121AAD3D01C369C7F4A39AED209DC8A6235C0F3A9DB7A83DD241AEE2A110DDBED5
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...O..P/....."#.D.....A.A..Eo.....'.....A.o]@r..Q.....<w.....].n\....A..Eo .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.607762882702344
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQvkWtj7xm7OhKlvA1:RbR16Q9xmJ
MD5:	557A0AA61BDFB25AD34327FE8435751A
SHA1:	85094D987F3F984A4EC70BCC250B0DCA39A0F2C8
SHA-256:	37C4521EDF38CAF2848CEB5771D7601D8CAF1A2B6BC32B5095E17219D016439B
SHA-512:	7E4C3CF8F9A57110DDBAAD102C7EF2C807D937D2CF5D31122BF3976141BCDB44C8B10D866172EACEA0F6F6D66B4512DE946FA9681BF566FA1B069B69AC08749
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..(J..P/....."#.D.c.....A.A..Eo.....D.....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):	5.551307296605831
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuSMeQa0BtzdFt1:B2geRHRQHU
MD5:	B4A4AAF19733C12B4B33E2D15D0FCE58
SHA1:	8B163C6853DE9E60B357821A6FCFDB39D61544B6
SHA-256:	F0836551209222B402AF4FD01C08656F2E804400C03804F28148EF3C7614F234
SHA-512:	EAA75427B31C3B82E7D8E7E8C0AE2906482186D044077F650B4000DA87BA35BDDD97C06ED340942EC7BFD1FE81D4984653F9D1134AF17FDC17FB7E9A3E64F1 C
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .orO..P/....."#.D..-....A.A..Eo.....$8.....@..{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):	5.627841101631036
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVn/rmJO0kRktWtgEnNWQ1SUm1:mzyEYOFLvEWdrlOQESBtZEt1S/1
MD5:	64E8C64C6A112DC79EA38A6DA4FD9576
SHA1:	391CDCF1689D666F2CEFEC41B9CF7548C8A41B22
SHA-256:	9BDF5299BF039AEC674577CBDCC0CF2507FB7FAD9816BA7BBB943A4574CA6E7E
SHA-512:	ACCA0514DD114F827D7F875B6F9C16498FBB0D0978BA9F0B149FF03A9D4CBEDFD410124E7234E2E457E0B78D937E2A8E96FD481E975982EB50007FBE34A521C 6
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..)H..P/....."#.D.i.....A.A..Eo.....M.....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):	5.550674839202454
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvJ5t/t9kRktYEt/glwJNqww6U+5m1:mnYOFLvEWdhwyuj51t9tDClwrqwK+41
MD5:	A86CDE160790DFE274404BFE174A765A
SHA1:	18E017F5E931422390B642FE1DC41DBCDD242959
SHA-256:	9D58599A524D65AD58B5ECA39F5E95C1A0C2AC19BFBE48BD9BE04C78506F3768
SHA-512:	10BD32F3764A343D3CFF0132BCB58CE7F73B8F2618BEE067AD41C44B8B305417464976218FB8C0798867EDD5BB5A7C1FEBF8D16B5315CD4C98105F4EB0EDB9 4
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .,'J..P/....."#.D36.....A.A..Eo.....hD.....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):	5.600848952677848
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuOWltntM0fO441:/RrROk/UpC0fL
MD5:	93B8F67BA6059DA3748FD998C5DBC788
SHA1:	3E623AD93172A25C525E4A78F0EEEC53813B6F83
SHA-256:	D383312016DB941640B947688007DD211A9EF754C5BC51BD0E6F0A0B42FCB0CF

SHA-512:	72287A5E1692BA88599436FD3C8E61539054EC43D12401EFDE982F9A6FE1EDC8FB28EADA7C03A664C88A2556A44D3D3C0C80AA500B10625F3B777B8D0EB19A 6
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ...G..P/....."#.DPQ.....A.A..Eo.....^.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.588810987211443
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVs+ll/oOJRktYT3zoIN1OFPL4m1:mmDEYOFLvEWXIjtoOQtYLzV1QPLr1
MD5:	CA823AA1C7CB0DFCEA3FE712B63A557D
SHA1:	12383F1280288995D7221C890ED488C9BAA1C861
SHA-256:	9C9604A8846253EF0A3790580196374917E239BC17E42DECFC1A3A9356AEED43
SHA-512:	1384029E9CE5160BBA3103D23F9AFFB54768AF2B81EA57935C84B4056D780D2FA7C3148DF4F50446A199C22DC75B74C38065FB042F7F2C86B9C38420E2C83287
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..F..P/....."#.D.k.....A.A..Eo.....&.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.610626350115273
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvkFTHt/PLc9k6RktE0//m8D6EsEJo:m52YOFLvEWdMAuqTVPoG9tl2EvsEJ41
MD5:	0926F994DE13EDA59A7E2CFC10281BE5
SHA1:	935830D69C61C55EDA95BF974779BCBADF853CED
SHA-256:	DF223F196F3927202A76E14C1A1D8C1CFE13138118102E542A4313D748211DE0
SHA-512:	4E8D2E51BA77EFA84583E313E3D8F5D59A1F80EAD845803A8859AA8C0E7220961A7E8ED49724C0AEEFE78F1EA1847BE3D18FB8EFCC28169E07142ED01CF5B1 85
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ...O..P/....."#.DJC.....A.A..Eo.....C(.).....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):	5.583998485910321
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFveCu/jQRkt3A/OFoDb7T2/1:mYilPYOFLvEWd8CAdAuPebt3long1
MD5:	3D95B90EB0979E07AEE7E94065292E5B
SHA1:	39683F5FD739A548B0A08DD9754FD8610F730908
SHA-256:	74724B37664F439C379CEF31A267E8146BE66C16892C8E2DD3BECF8297EC106B
SHA-512:	32ECD6CED29ADBD1F4A1E323CCFF61B5750702A8AD53C8C01CFEA1BEEAB636456CDA8CF3C29105A47E6253830A5478638897FBC1857F9B5D7406619E7F171A 03
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .;.O..P/....."#.D)^.....A.A..Eo.....B.....c}.H7M=M..-.....Ix..R.I...}Rl.$q.A..E o.....

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):	5.575019062802048
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVIJ/2oKPWFv6ll/fgnnkRktnEOe28WIJLA:mY8nYOFLvEWdrROk/luwltqtEN16wG1
MD5:	1C1C09775D89160E3A7B6F61C8E20FF9
SHA1:	8019387BCB63D8091D68D2456C94281132FE4679
SHA-256:	1524F3BE3F93029528B9C62B04F50D4B8FC1445D6F41916343CFEC6865021BE2
SHA-512:	0E7F507F4CE4ED44FF1EB0F722B5B46F9D64515194655C4DA4195B97CD53ED83AF3DAA60CF54EC3264152A0423C90733955CF1976427401876378 00DA1B67635
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .K.G..P/....."#.D.E.....A.A..Eo.....}S.....%.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):	5.668873581676798
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVytoF//pzcqkRktrlePmJt:mLrnYOFLvEWdrloJUQFaVdjtxeeJli1
MD5:	D5EAB93751AC1B7A61F8E96AC211EF3F
SHA1:	FB8C7EA8C0F710DB3676D39A69E9F31A99BB2E76
SHA-256:	F6E3414FB2014966D04477625B51E19DEF36D3DA5A0B3DD8B49C85B1800325C8
SHA-512:	D1AB12BD803A180ADA820E3B2047A2953280633350C4C468C396807B04EFBF4FCB900D225D0FA71C50747B13F5FDBEBC2B442F07DD368E5111CB07181C04DA8 6
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..+H..P/....."#.D.....A.A..Eo.....Z.....;"./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):	5.5612368136651344
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuDVta2rIStD/xzgm2d/1:0R5VEEISV/xR
MD5:	7A6974EF458ABA31509126F8638D6F99
SHA1:	4B009AE03A7892EDBEEE77710D429C6BD3B63154
SHA-256:	BDD7527EDB021F834BFC94CA96B150B49D17B5B19B5C7C8B5CE1FFB95E4AA70B
SHA-512:	299EABF847D9BB30B390AF6688C5DB965AA889412EBA34320D1BA1040082288D8FC6E7EEB6B28F2B875929BB580A2F23E15952796B32B0C878CF7D3CF5D3A68 D
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ...G..P/....."#.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):	5.606320392905866
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvJ1+//YjI9JRktO1GBiaQ562HvpMm1:mAElVYOFLvEW1K4e/9Qtix56uvp1
MD5:	11399BA6433E5D2C6EAF25C0B93DB932
SHA1:	E081C102177D38FA90F9B475AC0EBCF0B66C7AC2
SHA-256:	537B0A06834A3FA7E046914387CC53C3AE93EBB3B3D1BD2393D72ACF63CC82E5
SHA-512:	8870BA6EDCF9560D6CBA7F4ED13F523FD32305F65A5ADBD7BD59736BFA907DC20917409441B70BF492999839BE3343EF851EC3ABF838C8A53EC327332D546A5 7
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .*.<..P/....."#.D.....A.A..Eo.....+.2.....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):	5.651471255775399
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvusvesAHlSt8UDLYtmOZn1:xRBJDeTDcFZ
MD5:	18D937FA69EE6EE16DE14487BE3D0F24
SHA1:	407556B89EFFBE80AB5D16BB78A31FFB2CBAC769
SHA-256:	2A58B426FC93AFD55F466FC88043755A89597C11A04A8BCC6DC7D60DB81A963C
SHA-512:	EA1873AE9199D6F8A51BFD6CFDAC39270D03AF9A304DA801EA24E7D8770F4C21AD603D55FC5CEAB2DDA1F37A312EE4E5330AB9772E5B5A65B504716A10D92EEA
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...O..P/....."#.D.%.....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):	5.598506873098588
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvxZfl/2hylQRkt3llFpSKGi:msRPYOFLvEWla7zp7Kt2ElPtt8VPu1
MD5:	B36CE60DABAE5C2C68ABCDF537B399A7
SHA1:	42511E2604CBA44236ADDDEA87BC8BE6A6FABA3F
SHA-256:	2761E6588D371710329B839163392855342C66187D477C9DF92FA1E768EB60FB
SHA-512:	5669770560C2AA4D98EF50C45881DEE87BBA91F9FE50BBEFB0C4F6B940CB4B836D3D1DE64F0B576B14D62DC0C481797C5AEA08E0FEDBBC2B9574ED89B638CE87
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .`.9..P/....."#.D.....A.A..Eo.....g1m=.....L...Im.@.....E.nW...IP..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.572894941037124
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVa//k9kRktJXl96F4XVAZ+8cV3I:mKPYOFLvEWdENU9QFltgwiM3Y1
MD5:	6C25D187D5522309902319CB0F2E04D1
SHA1:	D9B972270373BA977C08081B584FE4C196A91246
SHA-256:	1DF97D65306F71A7EA7C4668387B6C2DCEE3E26A39D2CAD26E399BEB72AF6686
SHA-512:	18B8DBD480501564B45FF1908935E3B506ED8F0CE71666EA3526966314EDE66A9C312D98C58B67EDE51F68FE4BE857A7B689CA3E6790294FB737CDE46430D6DC
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..*J..P/....."#.Dh.....A.A..Eo.....Qr.f.....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):	5.600545661828051
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQzAtRtCijBRCh/41:XRc9CcQiDi/

MD5:	42EA06B4F1B3D20D423F50E4781590C8
SHA1:	13D2FBF2085C500E4DB01F1D42FFA12569556A59
SHA-256:	25A3ED04D8F2358B9398C02966857B2CAECC4F9FAC7C48C3C7E6373304CE59E9
SHA-512:	0BBF27F3903CFE74D5C38BB9DB49215D1735A93D747C16A1122254578194BF9BA1799C3BF90E9415D16A3B22E72593C25EB8DBC9BC243B4AB347FAA94EF8827 2
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .Z]P..P/....."#.D..>....A.A..Eo.....(}.....PJm...0x.x..RD...BB!@5..<..] ....A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.559487569468151
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuqYVvttXl/l/kULlF4r1:bs6xRkirx3lt/7LlF4
MD5:	8C236DEE20477DDEAAB43674564AB50C
SHA1:	D225A033A89420C2E72776A2FA62AB55BF2CF840
SHA-256:	EFB50A6265C9B2646BF5CB846B5BE985770D9D80AC5191764B0041EDF8432271
SHA-512:	C4F46CF317C1D891F13612D01CB0D3A2A4C121ED6A084A28715D26BCD2BF724664C282B48782C56A2A879D8F773B680ED82ACDA136205A337F5B101B621A4C6
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .x....P/....."#.D[.'....A.A..Eo.....".K.....P...#4..I....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):	5.485797221682207
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvwal/dIXRktx91ECcu1isLK5m1:mhYOFLvEWd/aFuBtdIStJEN941
MD5:	2F6BB997FD2E326A5BBA37709986B17F
SHA1:	F0F1C8B3B50B1B0B74B9C137C3761BF23763870C
SHA-256:	01F38D7684A5BE497D1AB19C954BBC641B4D0BB18F59A07EE14FE2F89C2E4EB1
SHA-512:	0F6477D5D962E0B0A5A8EB7E1D763C04A18D8EEE83794A610E2FC49527AC24DD3F8474053A2C84DF9D13EE66970BB4966F95969B55739DC8CAA76DD9B1E41C B
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...Q..P/....."#.De./....A.A..Eo.....I%.....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):	5.51662120596477
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQF0lAt2StQBMqVd3G4K41:2DRuR20isSKB9Vd2
MD5:	8F8E284399A3C4CAEB29BF6033B0E4CA
SHA1:	BF5C22998C8B0346DEC0F95CFB57861EC31D12E9
SHA-256:	EE20292A9285CFA7B3DE1B28B303C798EC73E415C1925B02E6A029C3FA3F9C42
SHA-512:	704C8D0583137B2FBCB1798D881EBE77A96115536D350DCC0B4EDCDA315EEA9E7FE9BB153211B855C1B4E09DE45D4B7EA3D3A0C8CF44D71B6DAEA3BBEE10 C812
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...Q..P/....."#.DP.....A.A..Eo.....!.r.....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):	5.557649370956887
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QGltcotFlIDuA424r1:+RQXpxsr
MD5:	BA906F3502DB77FDB33FFDF846683B72
SHA1:	C6512A55A493082989422EF9B86F8375ECB53472
SHA-256:	DC1965981BAC7469337DD483732E9F782BFF3CC490A6151AA8EFB0ECD1C6A013
SHA-512:	00B130E788E8547B13475664683B4E6181EA18C949AC8280EA180AA0EBD9B0B789EBFB1C0D5542563660402EA871948512AEC55E199E287BA6E942625E82E59A
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..tQ..P/....."#.D..?....A.A..Eo.....#..@..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):	5.58392873454031
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFv//1L9kRktgl7Ag2iHio/Mm1:moXXYOFLvEWdENUAul1L9tbyC8n1
MD5:	8D55D63C5CCBDF76D54A3A7B6D0B2DD4
SHA1:	957F82EE76A16B889A5E24EEBAB3828324946918
SHA-256:	EF5290A9633E5934007A8E556FB7A22465938D5C0BA493D70EC4A9638957F1AC
SHA-512:	BA80E4AC60F54D990BE4A2991447AAF3529E543375F1C5837D81CF1A0ACDC2878C1ADA41919679290DF9B9AF960262C77A90A86C2247E92003D1CB1DC13FCA0
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .C.I..P/....."#.DB.....A.A..Eo.....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):	5.596994789210489
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVlJ/2kKLuVc//kcG9kRktvE/sYWmYk5m1:mQZYOFLvEWdrROk/VQPa9tvE/sLmB41
MD5:	88AD3D637A4C91DFA2C03F846E38F919
SHA1:	9068B8C973A9202209D90DCA60ACBC79B7943F3D
SHA-256:	F20574E1CAD077A8DE728FEB5431A67D635A10BD1ADCA09EE2F7CC73AF5B6493
SHA-512:	6A69C903812702DDDFC6AE0AC2082EE4F0C7D6CA439EED3D7CF4BBE06F620B17CEB8B0889F788260BF97EBEF549D28F5AC0D429ED0C7799C138DB42EA7242CC6
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .k-H..P/....."#.D.....A.A..Eo.....e..... ./.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):	5.565040183022998
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuyT4eSEtJ5dm9741:qxRcEEEf5du7
MD5:	BFB1E0BFD547650E0D8D2C598E14AAB1
SHA1:	11356D8D7377419AD0FC11A0B6E546037B9CA638
SHA-256:	AC020FB74E120DCE276617FE93E184DF0170BB2F5CDCBCEFC4516B841C7BE548

SHA-512:	DC12A24801E1A11900C078021D81C3ECD6A2C381824FF08F6C852544D99CDEF19908A54ECDA8256A4FF054492C629393202A58DCF1A9F2766042DC09AFBA7B1
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...O..P/....."#.D..-....A.A..Eo.....\.....U...I.>P...X...x..0U.~;m.x.k.A..Eo .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.601439502435024
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvwHt/+LkRktD//2B6shoq+Nem1:mMOYOFLvEWdwAPVuI1+PtD/OB6Jn1
MD5:	62FF3FEE75D6A47F2029EBD8410C365F
SHA1:	23CCB236A8B6C6D7F5B76D21C739D2F6E0DFA0A1
SHA-256:	BA1DA14D79DD90839078685DB5061B5CA3D85740AC10E57611D8B7704B3680E4
SHA-512:	954A0940F1AC6B7DDA4432715265F7642A69956EAB979229093387E105A7F001E75C8DE86D4110E51C0EBE5AFB9ED4C3001ED70CE4689FB483B5DAD9FB5649B5
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .b.I..P/....."#.D.....A.A..Eo.....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):	5.63835904638504
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQXq+ltKISBtTl/AhcsBXIh1:mxRBJQEUI63/4B
MD5:	ACDAA9AB84DF748F3E332D8EB23FA2FD
SHA1:	078D843B39A851E5E3FE399E017BCC634AD26705
SHA-256:	5C877B08292E9E402A0E64EA2E85AC5D82BF9A6BBB96DD0EAA0254A56B778267
SHA-512:	18FAD91D215A2EB31E6683206B69F1302B6F9DE5701696FE1A027E76EBC7FD84BB6627E4C2A09277C7843D82EEBBDC99EB1C1318DACBBDAAA05839E96D33404
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .Y.Q..P/....."#.D.-/....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):	5.5998858495321455
Encrypted:	false
SSDEEP:	3:m+l4kC8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKjXKLuVFAt/lAk6Rktn3Rlc3OK:msPYOFLvEWdrROk/RJUQZlPtrc3Me/1
MD5:	D0420A713C4C78DE127E5B6DF1F9A6DC
SHA1:	294EA17FD838BE667076B5A0933373A4B8ACC41E
SHA-256:	DA54A544204AA54FC9C73FEC67C42518EB3E6E4764A1F211EF64BCA5F93F4632
SHA-512:	DE0D42EDD2AEE317BB7A313A79858A43261D4AD948E68609A27A684F0DD04C7B7EA6F50738B1A4EC92AA325DEDD42FF7FCC3C72232F32055EB26E2581617B4C5
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...H..P/....."#.D%.....A.A..Eo.....}.....9Q].8O.z....=..:.N.{....N{.A..Eo.....

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

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

Size (bytes):	1080
Entropy (8bit):	5.029059890152802
Encrypted:	false
SSDEEP:	24:X4vPA5OnT9AMqOua0R5im8ZD/EX8hKx/61BW:CPpnTWgY8REXIZ8A
MD5:	B891934DBE6EB934EB98792AE7607A9D
SHA1:	F779156AEC614CC860306DEA05F7EDF2CF149B86
SHA-256:	7E74212BE3DEEC52C4BBF57A6883EC1FE28C22DFA0BF20A59829249EBE1B5913
SHA-512:	0AC0E0855746236159D84079AC959B1923A2584CE6C271DDC4DB77D2F36E198341AEC64CE8D73DD867A759FEA1AA4BFD87E10D810DD0C08CA06264C0C3325F 3
Malicious:	false
Preview:	0...6...oy retne....+.....V.....*...LH..P/.....;.y~A...9..P/.....oB*..9..P/.....#...(...A_./.....D.4..LH..P/.....[.i..%..LH..P/.....k7A..LH..P/.....]... I..C...P/.....2q.....LH..P/.....P....V..9..P/.....!...0.o.LH..P/.....P[. q.LH..P/.....3....LH..P/.....v...q....9..P/.....a.....9..P/.....C..M.....A_./.....,+... _.#.LH..P/.....<...W..J..9..P/.....J..j....LH..P/.....6<|.....9..P/.....qi.K.L.9@|..P/.....K..JM.gb@|..P/.....C...P/.....F..=z;..LH..P/.....o..LH..P/.....Gy.'. h..LH..P/.....:..N.A...LH..P/.....LH..P/.....:/....LH..P/.....A?.2:...LH..P/.....q..LH..P/.....u\].q.LH..P/.....o..k...LH..P/.....*....LH..P/.....^.~..z.. LH..P/.....+.{..'.LH..P/.....@..x..LH..P/.....*)....J:.LH..P/.....&.S.....LH..P/.....MV3...LH..P/.....

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):	1080
Entropy (8bit):	5.029059890152802
Encrypted:	false
SSDEEP:	24:X4vPA5OnT9AMqOua0R5im8ZD/EX8hKx/61BW:CPpnTWgY8REXIZ8A
MD5:	B891934DBE6EB934EB98792AE7607A9D
SHA1:	F779156AEC614CC860306DEA05F7EDF2CF149B86
SHA-256:	7E74212BE3DEEC52C4BBF57A6883EC1FE28C22DFA0BF20A59829249EBE1B5913
SHA-512:	0AC0E0855746236159D84079AC959B1923A2584CE6C271DDC4DB77D2F36E198341AEC64CE8D73DD867A759FEA1AA4BFD87E10D810DD0C08CA06264C0C3325F 3
Malicious:	false
Preview:	0...6...oy retne....+.....V.....*...LH..P/.....;.y~A...9..P/.....oB*..9..P/.....#...(...A_./.....D.4..LH..P/.....[.i..%..LH..P/.....k7A..LH..P/.....]... I..C...P/.....2q.....LH..P/.....P....V..9..P/.....!...0.o.LH..P/.....P[. q.LH..P/.....3....LH..P/.....v...q....9..P/.....a.....9..P/.....C..M.....A_./.....,+... _.#.LH..P/.....<...W..J..9..P/.....J..j....LH..P/.....6<|.....9..P/.....qi.K.L.9@|..P/.....K..JM.gb@|..P/.....C...P/.....F..=z;..LH..P/.....o..LH..P/.....Gy.'. h..LH..P/.....:..N.A...LH..P/.....LH..P/.....:/....LH..P/.....A?.2:...LH..P/.....q..LH..P/.....u\].q.LH..P/.....o..k...LH..P/.....*....LH..P/.....^.~..z.. LH..P/.....+.{..'.LH..P/.....@..x..LH..P/.....*)....J:.LH..P/.....&.S.....LH..P/.....MV3...LH..P/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF4cd3b9.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.029059890152802
Encrypted:	false
SSDEEP:	24:X4vPA5OnT9AMqOua0R5im8ZD/EX8hKx/61BW:CPpnTWgY8REXIZ8A
MD5:	B891934DBE6EB934EB98792AE7607A9D
SHA1:	F779156AEC614CC860306DEA05F7EDF2CF149B86
SHA-256:	7E74212BE3DEEC52C4BBF57A6883EC1FE28C22DFA0BF20A59829249EBE1B5913
SHA-512:	0AC0E0855746236159D84079AC959B1923A2584CE6C271DDC4DB77D2F36E198341AEC64CE8D73DD867A759FEA1AA4BFD87E10D810DD0C08CA06264C0C3325F 3
Malicious:	false
Preview:	0...6...oy retne....+.....V.....*...LH..P/.....;.y~A...9..P/.....oB*..9..P/.....#...(...A_./.....D.4..LH..P/.....[.i..%..LH..P/.....k7A..LH..P/.....]... I..C...P/.....2q.....LH..P/.....P....V..9..P/.....!...0.o.LH..P/.....P[. q.LH..P/.....3....LH..P/.....v...q....9..P/.....a.....9..P/.....C..M.....A_./.....,+... _.#.LH..P/.....<...W..J..9..P/.....J..j....LH..P/.....6<|.....9..P/.....qi.K.L.9@|..P/.....K..JM.gb@|..P/.....C...P/.....F..=z;..LH..P/.....o..LH..P/.....Gy.'. h..LH..P/.....:..N.A...LH..P/.....LH..P/.....:/....LH..P/.....A?.2:...LH..P/.....q..LH..P/.....u\].q.LH..P/.....o..k...LH..P/.....*....LH..P/.....^.~..z.. LH..P/.....+.{..'.LH..P/.....@..x..LH..P/.....*)....J:.LH..P/.....&.S.....LH..P/.....MV3...LH..P/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.22106866932705
Encrypted:	false

SSDEEP:	6:kOjYepcN+q2PWXp+N2nKuAl9OmbnIFUtjjYe9XZmwJjYeA3VkwOWXp+N2nKuAl91:kOU1IvaHAahFUtjUg/JUv5fHAaSJ
MD5:	2E7001C32D3007C69E1C881132991D74
SHA1:	338148D453B6A9D517C67D0050824085F35DE07C
SHA-256:	8A4B5C463EB52B3DA59E4E0110015640EF7B72BBB79BC35C7408F0451BF951F3
SHA-512:	84120307564F598C410000072EC2A4DDE7BF2F9695F064531A9325FEC0FBD66EF48896B17CD4A5B6DB04F768FCBF50D6B39F44484DB4E46516606ED5D3184A5D
Malicious:	false
Preview:	2023/01/05-09:02:26.340 728 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-09:02:26.350 728 Recovering log #3.2023/01/05-09:02:26.351 728 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.22106866932705
Encrypted:	false
SSDEEP:	6:kOjYepcN+q2PWXp+N2nKuAl9OmbnIFUtjjYe9XZmwJjYeA3VkwOWXp+N2nKuAl91:kOU1IvaHAahFUtjUg/JUv5fHAaSJ
MD5:	2E7001C32D3007C69E1C881132991D74
SHA1:	338148D453B6A9D517C67D0050824085F35DE07C
SHA-256:	8A4B5C463EB52B3DA59E4E0110015640EF7B72BBB79BC35C7408F0451BF951F3
SHA-512:	84120307564F598C410000072EC2A4DDE7BF2F9695F064531A9325FEC0FBD66EF48896B17CD4A5B6DB04F768FCBF50D6B39F44484DB4E46516606ED5D3184A5D
Malicious:	false
Preview:	2023/01/05-09:02:26.340 728 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-09:02:26.350 728 Recovering log #3.2023/01/05-09:02:26.351 728 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF4c4c2a.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.22106866932705
Encrypted:	false
SSDEEP:	6:kOjYepcN+q2PWXp+N2nKuAl9OmbnIFUtjjYe9XZmwJjYeA3VkwOWXp+N2nKuAl91:kOU1IvaHAahFUtjUg/JUv5fHAaSJ
MD5:	2E7001C32D3007C69E1C881132991D74
SHA1:	338148D453B6A9D517C67D0050824085F35DE07C
SHA-256:	8A4B5C463EB52B3DA59E4E0110015640EF7B72BBB79BC35C7408F0451BF951F3
SHA-512:	84120307564F598C410000072EC2A4DDE7BF2F9695F064531A9325FEC0FBD66EF48896B17CD4A5B6DB04F768FCBF50D6B39F44484DB4E46516606ED5D3184A5D
Malicious:	false
Preview:	2023/01/05-09:02:26.340 728 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-09:02:26.350 728 Recovering log #3.2023/01/05-09:02:26.351 728 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.010978819626460943
Encrypted:	false
SSDEEP:	3:ImtVdXb+j4x9pPlXlpyPll//zVrzlltD0lGQZ7XEZhGIeIHdP4/X:liVtg4x9pdM//hFwl570ZhdeIG/
MD5:	E36F8F81D3C03F6AAF7D768706B7673F
SHA1:	EECE93F9E417717892E50F6A159516DD76C255B0
SHA-256:	C6E687FF9677244574F37AD2877726DF64E5BAADDA2ABE8C4759BDE8344E44F2
SHA-512:	0582ADCFA1A09095D4482C9A61475C8B77FF444BF2655DE4F6583BBB2699A054BBB2292DE2741FEEB27AFE0835B0B48F476418EE1A666DE20CA146D1EB4390A4
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230105170223Z-212.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 164 x -115 x 32, cbSize 75494, bits offset 54
Category:	dropped
Size (bytes):	75494
Entropy (8bit):	2.4020228028982116
Encrypted:	false
SSDEEP:	192:zyAByfgu8b4OcFX3EhrFgACR3PUNesB3CRcj0M9VGCf9iuseJDhQBehvv3rvvPJr:zyAByY6rfAYfUNBxRpJFc6V4/I8aHr
MD5:	D67CF064FC7C7ABA560E46285869AEEE
SHA1:	6D641177A756D9794095224A6B5B30FCE45BEEC8
SHA-256:	924E28444D2BB3939F59D6C770E979CAA612C14F33097B31FBA6C513DF3494AE
SHA-512:	235AFDCA6196A55217D9FE0FCDBCFFD31A7D6AA3EAAF169DBF79AB475FE9197B5C0124D104F3F83E7438C3EF64E930578B20727C6E801D120ABFE335F5AA1D63
Malicious:	false
Preview:	BM.&.....6...(..... ....

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 12, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 12
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.564715552600696
Encrypted:	false
SSDEEP:	384:3el9dThatELJ8fwRRwZsLRGlKhsvXh+vSc:ykYZsLQhUSc
MD5:	B15E8A8F33A5601830E856D5573DF225
SHA1:	A120DEB8D7DE2770921B5B26B9479D7BB124DBBE
SHA-256:	F52C1FC60D6D4C9123ED057BBFC32FA46A56B5595E1C2241388913C7E01CCD21
SHA-512:	9A55432D8AD36DEEF09BB4C5AF61DE9C26A2936A55F921463940F8E910AB100B5B531F03BE53B89C367884C0064176469C565984AD795AAEEB2CA136AD67534
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.284607295536086
Encrypted:	false
SSDEEP:	48:7M/om1CSiomeiom2om1Nom1Aiom1RROiom1oom1pom1jZiomVsiomgLqQlmFTIFv:7RSVOhnCsLN49IVXEBodRBk8
MD5:	A520C13D5593D1E7086D723EAB60B232
SHA1:	097223BD3549317F09FA926183CAC9960A2F8FF2
SHA-256:	78F75B8E967FD72B85D045446DC89259E2EF6950156A6399FD044E7AB3230A97
SHA-512:	8116921775C1B018AE5BA04A3E10BDDA9DE6B20A9CD27FB1B4E433DF1BFCC746AF2D7DD313BAD3286B6560B98139588308F8BB4F2F80A91B32DE662DFBCCFA50
Malicious:	false
Preview:	.... .c.....Z.>..... .....s..... .L.s.y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.2008	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443

Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Temp\unarchiver.log

Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	5.0863149791147855
Encrypted:	false
SSDEEP:	48:zFJbGYGbYGYGpiGbfGYGp3FkGbeG0FkGQGNGYGYGmHGYGNGYGmbP1+EEEEEEEEEY:x8MjKU9Q
MD5:	8A8E8565CCAA246BA9B71598B7038E38
SHA1:	27578ACD6D50E313A3BA1F5DB05EF479F0F9CF8B
SHA-256:	C783A44B81D1DEE63B86D0B1C036889E1DF5686A911785BBB9AC5F35AA32AFEC
SHA-512:	E7DBC97A56628ED6CA7F5B456AC31C1BC6C79DBF8ECF1B1D3E375F3C197FE2B4F8CC6476B2453A4D9551186EAAF83395A4E628FFA171130E724A0E4A79AF20CC
Malicious:	false
Preview:	01/05/2023 9:03 AM: Unpack: C:\Users\user\Downloads\Cancellation_367461_Dec23.zip..01/05/2023 9:03 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe..01/05/2023 9:03 AM: Received from standard out: ..01/05/2023 9:03 AM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..01/05/2023 9:03 AM: Received from standard out: ..01/05/2023 9:03 AM: Received from standard out: Scanning the drive for archives:..01/05/2023 9:03 AM: Received from standard out: 1 file, 801520 bytes (783 KiB)..01/05/2023 9:03 AM: Received from standard out: ..01/05/2023 9:03 AM: Received from standard out: Extracting archive: C:\Users\user\Downloads\Cancellation_367461_Dec23.zip..01/05/2023 9:03 AM: Received from standard out: --..01/05/2023 9:03 AM: Received from standard out: Path = C:\Users\user\Downloads\Cancellation_367461_Dec23.zip..01/05/2023 9:03 AM: Received from standard out: Type = zip..01/05/2023 9:03 AM: Received from standard out: Physical Size

C:\Users\user\Downloads\Cancellation_367461_Dec23.zip (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	801520
Entropy (8bit):	**7.999770193882168**

Encrypted:	**true**
SSDEEP:	24576:wlDW7aQ9CEKLN0rvLPFMDcebEvbm37vcYep11QJ/6dP/z:MDWtKZ0+DczS3TcYefQJ/uP/z
MD5:	26097A602D65D1CC7E47D2A5E5D32895
SHA1:	78868EA9BD5CA1E5B591303C964C74CAC18F76EC
SHA-256:	9D4DD3EFB6149DA52E080EC9E91F1E64C5D0656F488FA78DCD6CE638EE75BA0B
SHA-512:	6BFD8ECCB1C7CE62B06F54728781ECC100389E129A98D831F3FE20DD79BD65CDDE2D91764993624161F906936672A0839790FEBAF86019B8A10BDC26D83D2D 1
Malicious:	false
Preview:	PK.....U....B:....j.....Cancellation#J58.isoya...B.do.....;..\.....lk.).w..]..%....a...?.....j..)f...t..|...-....p..[..47...:..l....8./.ZI.L.Q8...v..E....h...6s.G..P. ../.....D.W8..@.g....-...M.. }..hU..@.2.+y...D(..m..,.....M.\..k....l..l.....Z..4....1a.....s.....IA%....<.v.....BU..na.....Z~../H>.P....Z.g..)..b.,1.:..D?..M.x.F.~..Z..w%r'.e..zq6.2...9.v.r.@.a.7.....h.FP....[,.S. 7N.jO.ZI.(U(...).Qt.#...t ..nE..q...Yo.<..q....q.@...(...7..7!..z.D7...k....d.m...W.N}.V..v.0Ds..L.!.`U....}."......\.g..'..V.#.m...k..Y6+&..i..8..6..H.y@.....::.G..4.t....{....h..;dS.i.....j6.g...{ Bl...b`...!#.Ol@.{...v_z.[.e.!....TW.A.[...P`.....+.g.k....:..*.xh...1'...|.....~:.`...._.N|.6.".X^NY.#.aU..{p.../zZ".9.o.\GI....X..d.b.*K.@;..P..F/j{.}N?.x...\!..|...>.T!.ctp.2@-...aU..5S.. n.i.........}...xQ....%.x....i...1...~...!....>.GU.p....X.....w..%..../*.....Z.;.wI...li.3...?Tddl'.D..uf.Io..@....7x...R.....).....U!...n..1.x#I7.M....].....N.&..

C:\Users\user\Downloads\Cancellation_367461_Dec23.zip.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	801520
Entropy (8bit):	**7.999770193882168**
Encrypted:	**true**
SSDEEP:	24576:wlDW7aQ9CEKLN0rvLPFMDcebEvbm37vcYep11QJ/6dP/z:MDWtKZ0+DczS3TcYefQJ/uP/z
MD5:	26097A602D65D1CC7E47D2A5E5D32895
SHA1:	78868EA9BD5CA1E5B591303C964C74CAC18F76EC
SHA-256:	9D4DD3EFB6149DA52E080EC9E91F1E64C5D0656F488FA78DCD6CE638EE75BA0B
SHA-512:	6BFD8ECCB1C7CE62B06F54728781ECC100389E129A98D831F3FE20DD79BD65CDDE2D91764993624161F906936672A0839790FEBAF86019B8A10BDC26D83D2D 1
Malicious:	false
Preview:	PK.....U....B:....j.....Cancellation#J58.isoya...B.do.....;..\.....lk.).w..]..%....a...?.....j..)f...t..|...-....p..[..47...:..l....8./.ZI.L.Q8...v..E....h...6s.G..P. ../.....D.W8..@.g....-...M.. }..hU..@.2.+y...D(..m..,.....M.\..k....l..l.....Z..4....1a.....s.....IA%....<.v.....BU..na.....Z~../H>.P....Z.g..)..b.,1.:..D?..M.x.F.~..Z..w%r'.e..zq6.2...9.v.r.@.a.7.....h.FP....[,.S. 7N.jO.ZI.(U(...).Qt.#...t ..nE..q...Yo.<..q....q.@...(...7..7!..z.D7...k....d.m...W.N}.V..v.0Ds..L.!.`U....}."......\.g..'..V.#.m...k..Y6+&..i..8..6..H.y@.....::.G..4.t....{....h..;dS.i.....j6.g...{ Bl...b`...!#.Ol@.{...v_z.[.e.!....TW.A.[...P`.....+.g.k....:..*.xh...1'...|.....~:.`...._.N|.6.".X^NY.#.aU..{p.../zZ".9.o.\GI....X..d.b.*K.@;..P..F/j{.}N?.x...\!..|...>.T!.ctp.2@-...aU..5S.. n.i.........}...xQ....%.x....i...1...~...!....>.GU.p....X.....w..%..../*.....Z.;.wI...li.3...?Tddl'.D..uf.Io..@....7x...R.....).....U!...n..1.x#I7.M....].....N.&..

C:\Users\user\Downloads\f1db83af-6dc2-44be-ad08-ad1b8f6a393d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	12426
Entropy (8bit):	7.986045610697938
Encrypted:	false
SSDEEP:	192:wQq1Fv+lodYd9vhN+W7rHGeZfn2BR/zPAfo028LiuOUlOiCo6r+XR7raexT4qR6E:/q1uFJE0tB4ZzMX95OUU9sdeOT7tjJn
MD5:	D09E144A7ED978AF106E813070C6DC12
SHA1:	DD127F78FB8FE3C55876927E6BDA8A3D9FA64CD3
SHA-256:	DFBDA2E1C8DFD9AB61E6E0522699E498499FBD6CAD02ABE3D90E51CACB2D2AC5
SHA-512:	1C15B50BB02885F72D99E997A2F86DDF83CAF12F2AE9E56704188DB302DB696A127D28EF5242B24D0AD9CB18B6F595707189C3A23D3335E0BD2CD544E84BD5 B
Malicious:	false
Preview:	PK.....U....B:....j.....Cancellation#J58.isoya...B.do.....;..\.....lk.).w..]..%....a...?.....j..)f...t..|...-....p..[..47...:..l....8./.ZI.L.Q8...v..E....h...6s.G..P. ../.....D.W8..@.g....-...M.. }..hU..@.2.+y...D(..m..,.....M.\..k....l..l.....Z..4....1a.....s.....IA%....<.v.....BU..na.....Z~../H>.P....Z.g..)..b.,1.:..D?..M.x.F.~..Z..w%r'.e..zq6.2...9.v.r.@.a.7.....h.FP....[,.S. 7N.jO.ZI.(U(...).Qt.#...t ..nE..q...Yo.<..q....q.@...(...7..7!..z.D7...k....d.m...W.N}.V..v.0Ds..L.!.`U....}."......\.g..'..V.#.m...k..Y6+&..i..8..6..H.y@.....::.G..4.t....{....h..;dS.i.....j6.g...{ Bl...b`...!#.Ol@.{...v_z.[.e.!....TW.A.[...P`.....+.g.k....:..*.xh...1'...|.....~:.`...._.N|.6.".X^NY.#.aU..{p.../zZ".9.o.\GI....X..d.b.*K.@;..P..F/j{.}N?.x...\!..|...>.T!.ctp.2@-...aU..5S.. n.i.........}...xQ....%.x....i...1...~...!....>.GU.p....X.....w..%..../*.....Z.;.wI...li.3...?Tddl'.D..uf.Io..@....7x...R.....).....U!...n..1.x#I7.M....].....N.&..

Static File Info

General

File type:	PDF document, version 1.3, 1 pages
Entropy (8bit):	7.795798037764297
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Cancellation_418406_Dec23.pdf

File size:	186639
MD5:	c085bbddc02251986f1fd8b84c5a404e
SHA1:	98d3377ff32441e24baa96f1d0fd83190e274c22
SHA256:	ca2d98108f12fb407cb0e1778febc9ff453ebbd8888e3b184cb8b9993775b5d8
SHA512:	02fef8a38f843cec18a6ca0e80cbb1ee23659534bab963d7ef0e8b522c2de1787666bfa4970c4d34d701ec4f652ba8bc583adca517fe5679e9d985bd2a3da59c
SSDEEP:	3072:fQcfk8aPgtSyiVLFkckuQMPhB20K8HR9hYDdfddlRCFwfkFPWN50kNSFHFUmV8N1:W8nwhFkZuvPDiYqdfddlVjbr03UmVruv
TLSH:	3504E0CCB13B76BFE8B77BB3A562835D374F6525732E6687088992A4C301F42D4510AE
File Content Preview:	%PDF-1.3.3 0 obj.<</Type /Page./Parent 1 0 R./Resources 2 0 R./Annots [5 0 R]./Contents 4 0 R>>.endobj.4 0 obj.<</Filter /FlateDecode /Length 59>>.stream.x.3R..2.35W(.*T.01.32U0.BSKS=S C..@A.@..H!9WA..P.%_!... 4...endstream.endobj.5 0 obj.<</Type /Annot

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.3
Total Entropy:	7.795798
Total Bytes:	186639
Stream Entropy:	7.794817
Stream Bytes:	185459
Entropy outside Streams:	5.173523
Bytes outside Streams:	1180
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	8
endobj	8
stream	2
endstream	2
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/URI	2
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview

ID	DHASH	MD5	Preview
6	66f76b6664006000	fde72814e2e16d5b1a82d3b7cf0921d8	

Network Behavior

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:03:45.665621042 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:45.666202068 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.666264057 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:45.666347027 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.667125940 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:45.667155981 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:45.667221069 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:45.681859016 CET	49702	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:45.682480097 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.682548046 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:45.683199883 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:45.683228016 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:45.806641102 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:45.813993931 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:45.814045906 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:45.815979004 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:45.816091061 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:45.823188066 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:45.823334932 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:45.823719978 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:45.839335918 CET	80	49702	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:45.839426994 CET	49702	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:45.854161978 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:45.854439020 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.854484081 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:45.855062008 CET	443	49699	142.250.184.78	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:03:45.855139017 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.855910063 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:45.855979919 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:45.980948925 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:46.144690037 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:46.144759893 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.144988060 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:46.145015955 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.145217896 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.145606995 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:46.145653963 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.145747900 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:46.145764112 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.146033049 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.192888975 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.193018913 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:46.193053007 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.193342924 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.193413019 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:46.195028067 CET	49699	443	192.168.2.3	142.250.184.78
Jan 5, 2023 09:03:46.195064068 CET	443	49699	142.250.184.78	192.168.2.3
Jan 5, 2023 09:03:46.214713097 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.214826107 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:46.214858055 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.215186119 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:46.215260029 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:46.216869116 CET	49701	443	192.168.2.3	142.251.209.13
Jan 5, 2023 09:03:46.216905117 CET	443	49701	142.251.209.13	192.168.2.3
Jan 5, 2023 09:03:48.063569069 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063642025 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063687086 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063714027 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063734055 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.063755989 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063781023 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063797951 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.063807964 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063849926 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063875914 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063901901 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.063932896 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.063934088 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.063934088 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221364021 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221400023 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221451044 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221481085 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221508026 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221533060 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221560955 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221589088 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221616983 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221647024 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221652985 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221652985 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221652985 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221652985 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221652985 CET	49698	80	192.168.2.3	50.62.149.105

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:03:48.221673965 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221702099 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221729994 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221733093 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221759081 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.221882105 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.221882105 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.379358053 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379399061 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379429102 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379458904 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379489899 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379523039 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379523039 CET	49698	80	192.168.2.3	50.62.149.105
Jan 5, 2023 09:03:48.379549980 CET	80	49698	50.62.149.105	192.168.2.3
Jan 5, 2023 09:03:48.379580975 CET	49698	80	192.168.2.3	50.62.149.105

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:03:31.990242004 CET	57840	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:03:32.011425972 CET	53	57840	8.8.8.8	192.168.2.3
Jan 5, 2023 09:03:45.622262001 CET	60625	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:03:45.626640081 CET	49302	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:03:45.626899958 CET	53975	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:03:45.643832922 CET	53	60625	8.8.8.8	192.168.2.3
Jan 5, 2023 09:03:45.645402908 CET	53	53975	8.8.8.8	192.168.2.3
Jan 5, 2023 09:03:45.652929068 CET	53	49302	8.8.8.8	192.168.2.3
Jan 5, 2023 09:03:48.831399918 CET	60582	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:03:48.851125956 CET	53	60582	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:03:31.990242004 CET	192.168.2.3	8.8.8.8	0x58c	Standard query (0)	agapeminis triesinter national.church	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.622262001 CET	192.168.2.3	8.8.8.8	0xf0a5	Standard query (0)	agapeminis triesinter national.church	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.626640081 CET	192.168.2.3	8.8.8.8	0x7cc1	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.626899958 CET	192.168.2.3	8.8.8.8	0x9e81	Standard query (0)	accounts.g oogle.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:48.831399918 CET	192.168.2.3	8.8.8.8	0xd046	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
Jan 5, 2023 09:03:32.011425972 CET	8.8.8.8	192.168.2.3	0x58c	No error (0)	agapeminis triesinter national.church		50.62.149.105	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.643832922 CET	8.8.8.8	192.168.2.3	0xf0a5	No error (0)	agapeminis triesinter national.church		50.62.149.105	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.645402908 CET	8.8.8.8	192.168.2.3	0x9e81	No error (0)	accounts.g oogle.com		142.251.209.13	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:45.652929068 CET	8.8.8.8	192.168.2.3	0x7cc1	No error (0)	clients2.g oogle.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

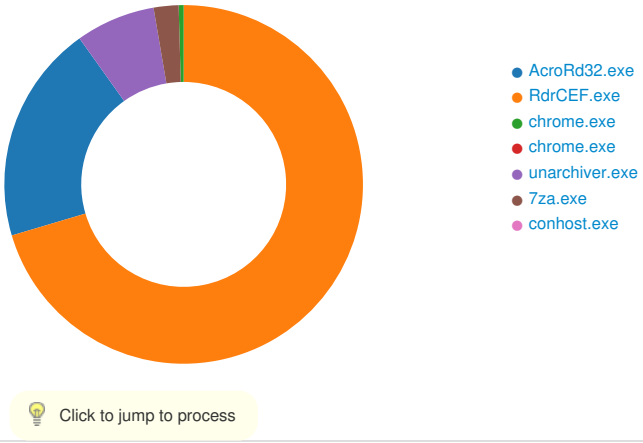
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:03:45.652929068 CET	8.8.8.8	192.168.2.3	0x7cc1	No error (0)	clients.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:03:48.851125956 CET	8.8.8.8	192.168.2.3	0xd046	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- agapeministriesinternational.church

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: **2156**, Parent PID: **3452**

General

Target ID:	0
Start time:	09:02:15
Start date:	05/01/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Cancellation_418406_Dec23.pdf
Imagebase:	0xc40000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	C8CF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	C8D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	C8D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	C8D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	C8D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	C4EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	C4EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	C4EA55	RegCreateKeyExW
\Device\HarddiskVolume4\Users\user\Desktop\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	C8D41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	C8D41D	NtCreateKey

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	C9DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/Cancellation_418406_Dec23.pdf	success or wait	1	C9DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	Cancellation_418406_Dec23.pdf	success or wait	1	C9DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	C9DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	C9DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 43 61 6E 63 65 6C 6C 61 74 69 6F 6E 5F 34 31 38 34 30 36 5F 44 65 63 32 33 2E 70 64 66 00	success or wait	1	C9DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 33 30 31 30 35 30 39 30 32 32 32 2D 30 38 27 30 30 27 00	success or wait	1	C9DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	186639	success or wait	1	C9DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	C9DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	C9DF47	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	C9DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	C9DF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	C9DF69	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	C9DF69	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 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	C9DF69	RegSetValueExW

Analysis Process: RdrCEF.exe PID: **5448**, Parent PID: **2156**

General

Target ID:	1
Start time:	09:02:21
Start date:	05/01/2023
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:	0x13c0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	14B59E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	30	14C83E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	118	14C8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	220	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	22	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	14B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	14B59E2	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	16	14B59E2	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	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2153	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	7	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	14B59E2	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	4	14B59E2	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	4	14B59E2	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	4	14B59E2	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	end of file	4	14B59E2	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	4	14B59E2	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	4	14B59E2	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	8	14B59E2	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	4	14B59E2	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	4	14B59E2	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	4	14B59E2	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	2	14B59E2	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	2	14B59E2	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	14B59E2	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	3	14B59E2	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	3	14B59E2	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	4	14B59E2	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	24	14B59E2	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-files\js\plugin.js	unknown	4096	end of file	4	14B59E2	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	24	14B59E2	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	4	14B59E2	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	56	14B59E2	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	4	14B59E2	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	60	14B59E2	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	4	14B59E2	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	88	14B59E2	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	2	14B59E2	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	4	14B59E2	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	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	55	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	59	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	14B59E2	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	20	14B59E2	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	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	14B59E2	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	19	14B59E2	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	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	239	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	285	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	14B59E2	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	266	14B59E2	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	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	49	14B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	14B59E2	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	194	14B59E2	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	2	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	32	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	14B59E2	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	2	14B59E2	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	2	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	2	14B59E2	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	2	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	14B59E2	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	7	14B59E2	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	3	14B59E2	ReadFile
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	14B59E2	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	2	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	5	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	14B59E2	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	2	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	11	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	14B59E2	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	12	14B59E2	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	3	14B59E2	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	253	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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\css\main-selector.css	unknown	4096	end of file	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	23	14B59E2	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	3	14B59E2	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	2	14B59E2	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	3	14B59E2	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	486	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	2	14B59E2	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	3	14B59E2	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	3	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	3	14B59E2	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	6	14B59E2	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	3	14B59E2	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	224	14B59E2	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	3	14B59E2	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	18	14B59E2	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	3	14B59E2	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	47	14B59E2	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	3	14B59E2	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	15	14B59E2	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	3	14B59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	3	14B59E2	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	3	14B59E2	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	6	14B59E2	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	3	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	23	14B59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	14B59E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	14C83E5	ReadFile

Analysis Process: chrome.exe PID: **7152**, Parent PID: **2156**

General

Target ID:	11
Start time:	09:03:42
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://agapeministriesinternational.church/blog/Cancellation_367461_Dec23.zip
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF6146AA143	RegSetValueExW

Analysis Process: chrome.exe PID: **2364**, Parent PID: **7152**

General

Target ID:	14
Start time:	09:03:43
Start date:	05/01/2023
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-US --service-sandbox-type=none --mojo-platform-channel-handle=1948 --field-trial-handle=1812,i,544507481073856773,15156316211615148029,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: unarchiver.exe PID: **6076**, Parent PID: **7152**

General

Target ID:	15
Start time:	09:03:50
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe "C:\Users\user\Downloads\Cancellation_367461_Dec23.zip
Imagebase:	0x640000
File size:	12800 bytes
MD5 hash:	16FF3CC6CC330A08EED70CBC1D35F5D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Local\Temp\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	F0A67F	CreateFileW
C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	F0AA8D	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	0	84	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 6f 77 6e 6c 6f 61 64 73 5c 43 61 6e 63 65 6c 6c 61 74 69 6f 6e 5f 33 36 37 34 36 31 5f 44 65 63 32 33 2e 7a 69 70 0d 0a	01/05/2023 9:03 AM: Unpack: C:\Users\user\Downloads\Cancellation_367461_Dec23.zip	success or wait	1	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	84	77	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 66 67 74 34 61 6c 63 30 2e 75 68 65 0d 0a	01/05/2023 9:03 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe	success or wait	1	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	161	50	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	01/05/2023 9:03 AM: Received from standard out:	success or wait	18	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1421	31	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	01/05/2023 9:03 AM: Get files	success or wait	1	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1452	37	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 31 0d 0a	01/05/2023 9:03 AM: Nbr of files: 1	success or wait	1	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1489	89	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 4e 6f 20 66 69 6c 65 73 20 68 61 76 65 20 62 65 65 6e 20 75 6e 61 72 63 68 69 76 65 64 20 28 69 6e 76 61 6c 69 64 20 61 72 63 68 69 76 65 20 6f 72 20 75 6e 6b 6e 6f 77 6e 20 70 61 73 73 77 6f 72 64 29 0d 0a	01/05/2023 9:03 AM: No files have been unarchived (invalid archive or unknown password)	success or wait	1	F0A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	1578	35	30 31 2f 30 35 2f 32 30 32 33 20 39 3a 30 33 20 41 4d 3a 20 43 68 65 63 6b 20 57 65 62 64 61 74 61 0d 0a	01/05/2023 9:03 AM: Check Webdata	success or wait	14	F0A9C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
\pipe	unknown	1024	success or wait	2	F0A9C3	ReadFile
\pipe	unknown	1024	pipe broken	1	F0A9C3	ReadFile

Analysis Process: 7za.exe PID: **5296**, Parent PID: **6076**

General

Target ID:	16
Start time:	09:03:51
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe" "C:\Users\user\Downloads\Cancellation_367461_Dec23.zip
Imagebase:	0x1220000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fgt4alc0.uhe\Cancellation#J58.iso	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	12263B0	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\Cancellation_367461_Dec23.zip	unknown	1024	success or wait	1	122686E	ReadFile
C:\Users\user\Downloads\Cancellation_367461_Dec23.zip	unknown	131072	success or wait	1	122686E	ReadFile
C:\Users\user\Downloads\Cancellation_367461_Dec23.zip	unknown	4	success or wait	1	122686E	ReadFile
C:\Users\user\Downloads\Cancellation_367461_Dec23.zip	unknown	4	success or wait	1	122686E	ReadFile

Analysis Process: conhost.exe PID: **5312**, Parent PID: **5296**

General

Target ID:	17
Start time:	09:03:51
Start date:	05/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Disassembly

No disassembly