ID: 778227
Sample Name: osGcfBvGVu.pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 08:45:10
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report osGcfBvGVu.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
System Summary 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 9
Public IPs 9
Private 10
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0 11
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0 11
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0 12
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0 12
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0 12
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0 12
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0 13
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0 13
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0 13
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0 18
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 18
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0 18

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy) 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF52ad0a.TMP (copy) 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy) 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF5230f4.TMP (copy) 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links 24
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230105074603Z-204.bmp 24
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages 24
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal 25
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin 25
Static File Info 25
General 25
File Icon 25
Static PDF Info 26
General 26
Keywords Statistics 26
Image Streams 26
Network Behavior 27
Network Port Distribution 27
TCP Packets 27
UDP Packets 29
DNS Queries 29
DNS Answers 30
HTTP Request Dependency Graph 30
Statistics 30
Behavior 31
System Behavior 31
Analysis Process: AcroRd32.exePID: 1840, Parent PID: 3528 31
General 31
File Activities 31
Registry Activities 31
Key Created 31
Key Value Created 31
Analysis Process: RdrCEF.exePID: 5988, Parent PID: 1840 32
General 32
File Activities 33
File Read 33
Analysis Process: chrome.exePID: 6048, Parent PID: 1840 37
General 37
File Activities 38
Registry Activities 38
Key Value Modified 38
Analysis Process: chrome.exePID: 4280, Parent PID: 6048 38
General 38
File Activities 38
Disassembly 39

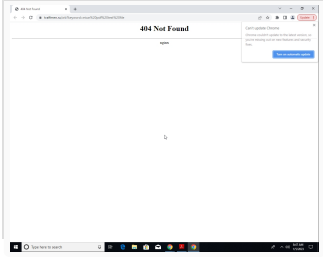
Windows Analysis Report

osGcfBvGVu.pdf

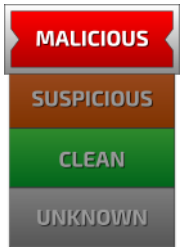
Overview

General Information

Sample Name:	osGcfBvGVu.pdf
Analysis ID:	778227
MD5:	63672c42600627..
SHA1:	df1d0775e3a8bb..
SHA256:	8f0a22d21e75b4..
Tags:	pdf
Infos:	



Detection

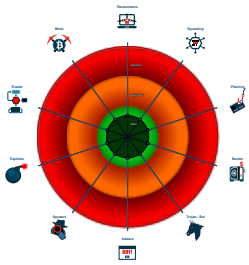


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Found potential malicious PDF (bad…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 1840 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\osGcfBvGVu.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5988 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 6048 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 4280 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1852 --field-trial-handle=1784,i,17276974344343449179,18398132625013484821,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

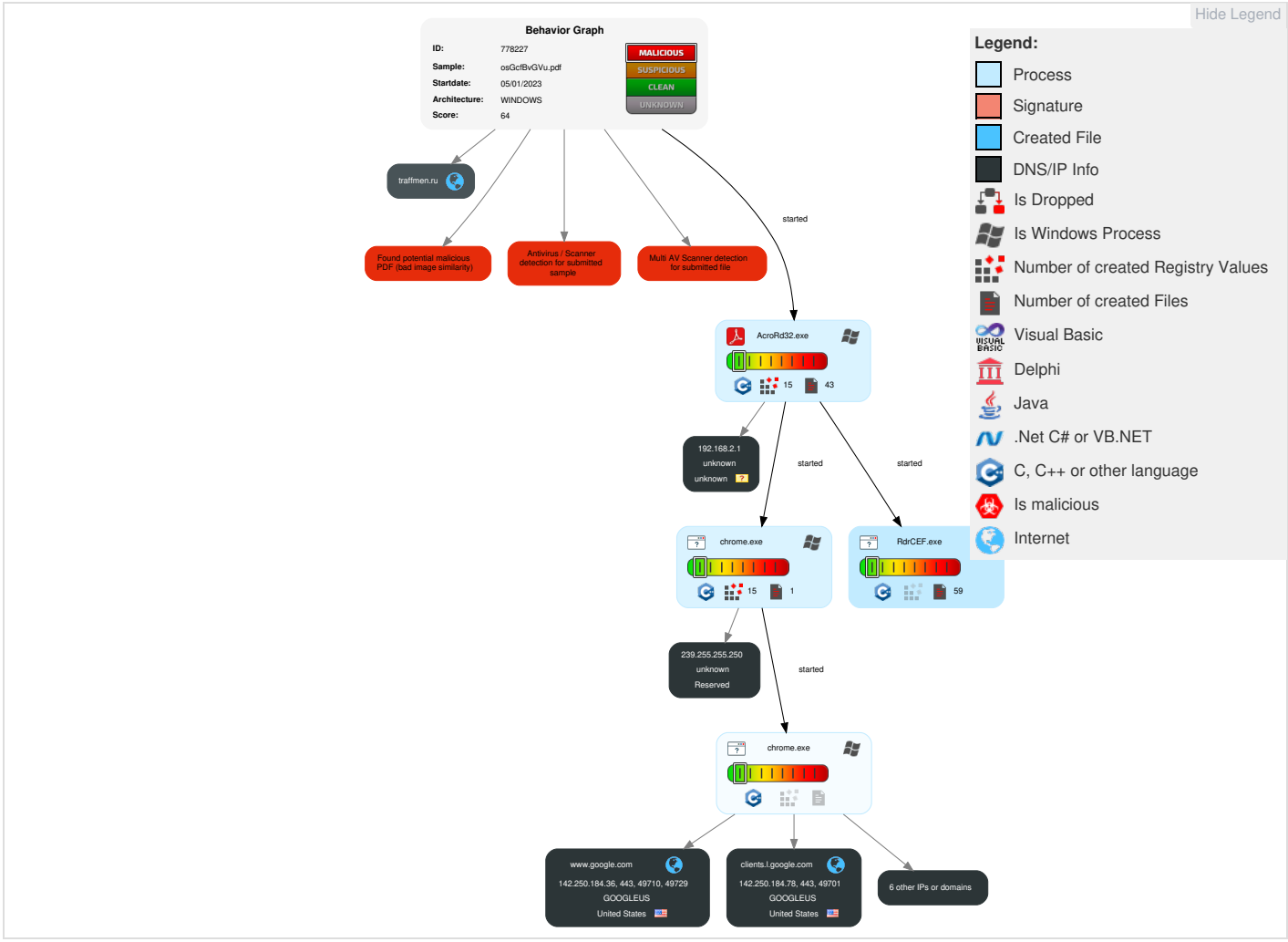
System Summary

Found potential malicious PDF (bad image similarity)

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 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	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)	Obfuscated Files or Information	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)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

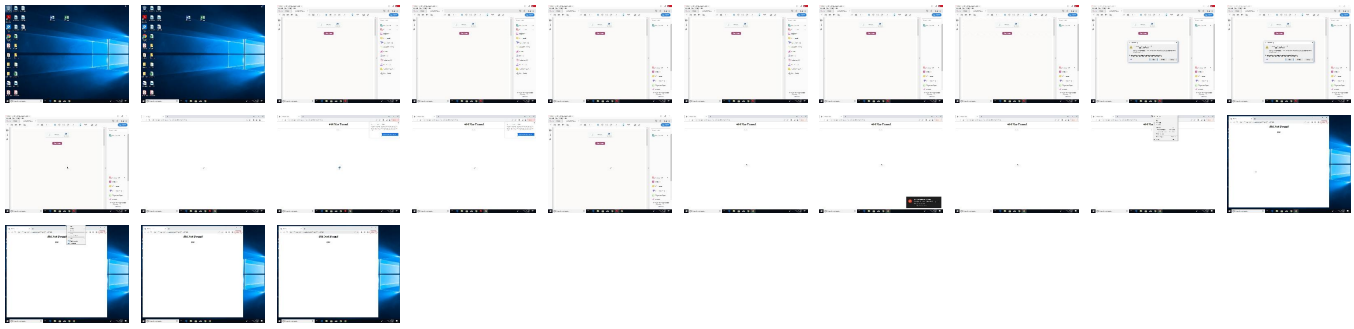
Behavior Graph

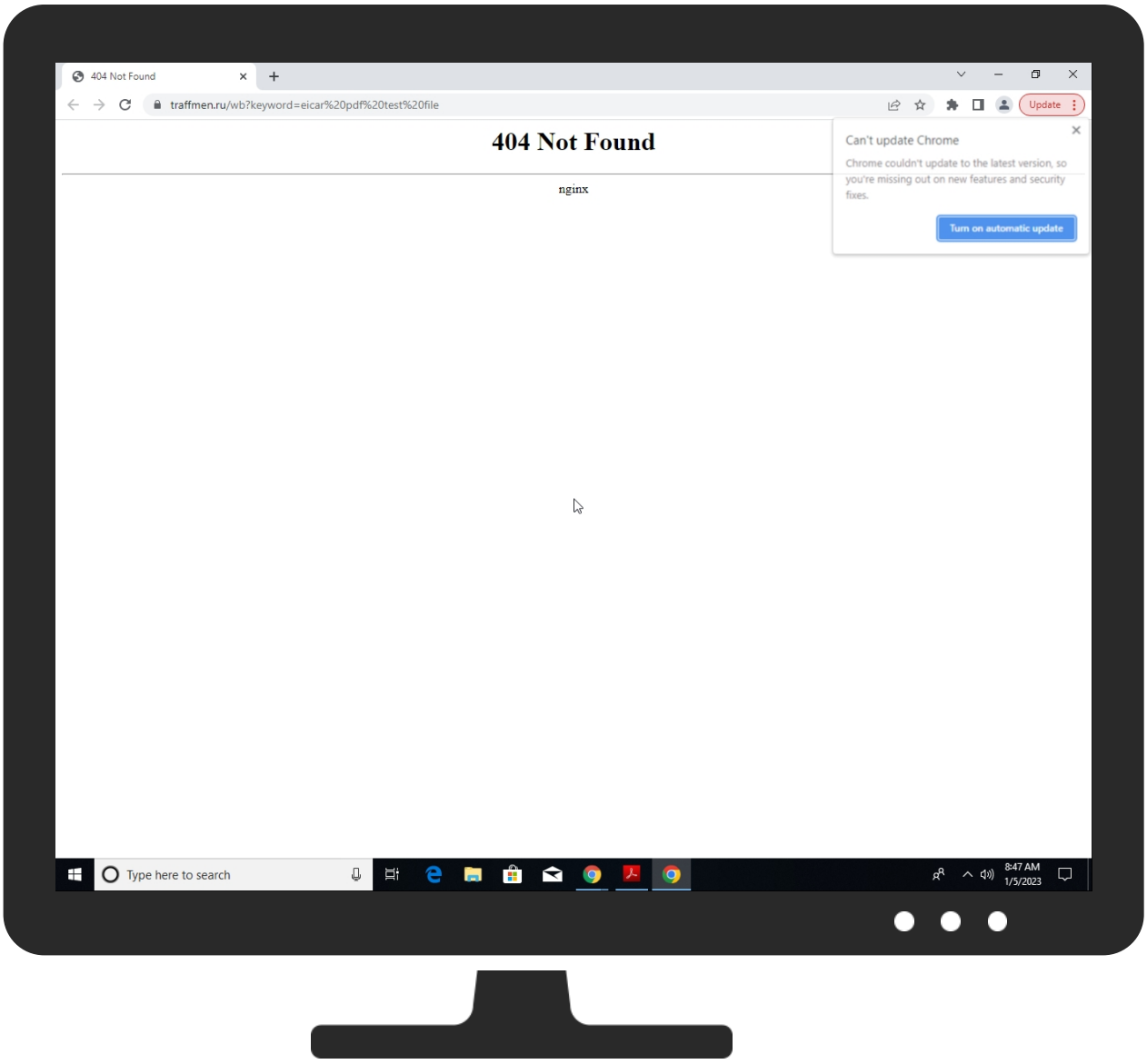


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
osGcfBvGVu.pdf	26%	ReversingLabs	Document-PDF.Trojan.Heuristic	
osGcfBvGVu.pdf	16%	Virustotal		Browse
osGcfBvGVu.pdf	100%	Avira	HTML/Malicious.PDF.Gen	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
traffmen.ru	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn-cms.f-static.net/uploads/4498392/normal_5faf04625de48.pdf)	0%	Avira URL Cloud	safe	
http://https://static.s123-cdn-static.com/uploads/4451565/normal_5fc4be3b76a1c.pdf)	0%	Avira URL Cloud	safe	
http://https://static.s123-cdn-static.com/uploads/4489441/normal_5fc8b59e7613e.pdf)	0%	Avira URL Cloud	safe	
http://https://cdn-cms.f-static.net/uploads/4381737/normal_5f9c867fda2cc.pdf)	0%	Avira URL Cloud	safe	
http://https://traffmen.ru/favicon.ico	0%	Avira URL Cloud	safe	
http://https://cdn-cms.f-static.net/uploads/4376874/normal_5fa0c5cb1b909.pdf)	0%	Avira URL Cloud	safe	
http://https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file)	0%	Avira URL Cloud	safe	
http://https://static.s123-cdn-static.com/uploads/4479223/normal_5fc8ecf96736d.pdf)	0%	Avira URL Cloud	safe	
http://https://cdn-cms.f-static.net/uploads/4365599/normal_5f9abc7d2f1a4.pdf)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	142.251.209.13	true	false		high
traffmen.ru	172.67.186.133	true	false	• 3%, Virustotal, Browse	unknown
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

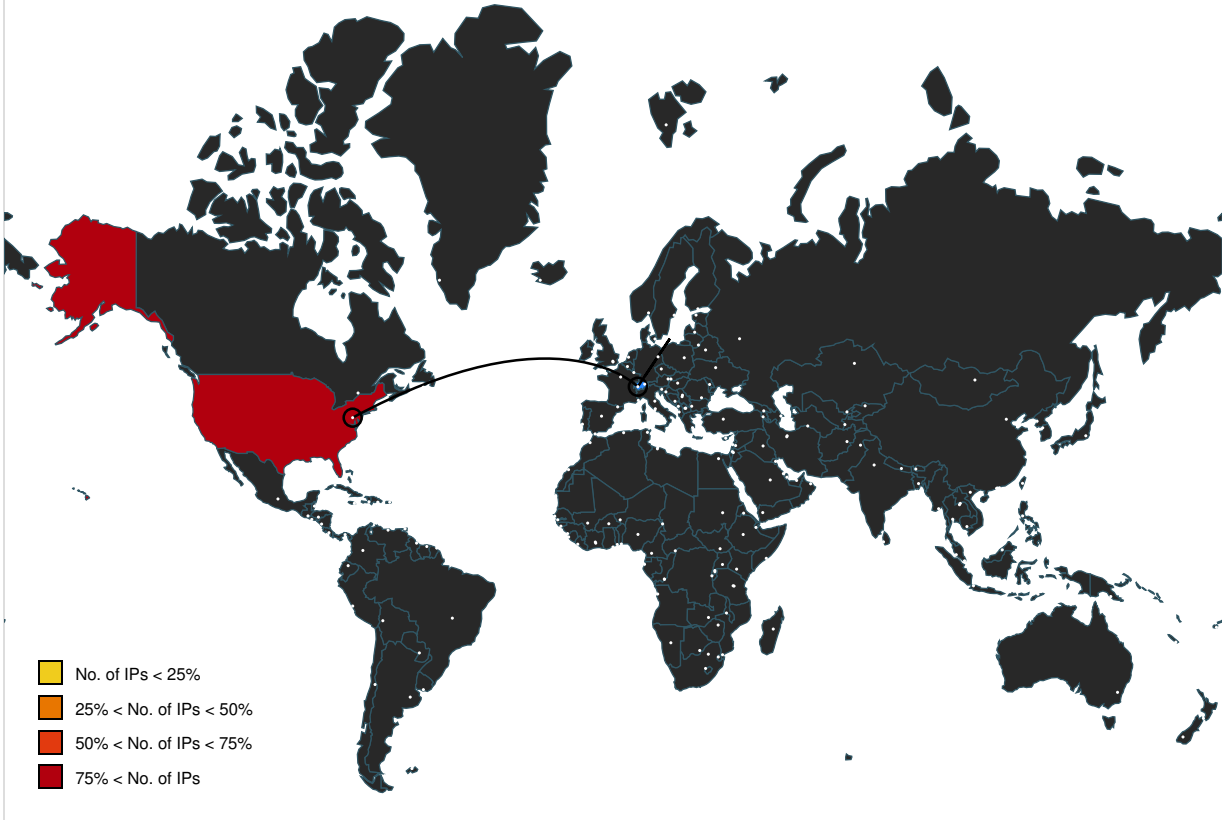
Name	Malicious	Antivirus Detection	Reputation
http://https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file	false		unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file	false		unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://traffmen.ru/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report/v3?s=gMx5mUmwuq9TlZ9qKTp9%2F2xmk7yZ0efWtwpnhfwBZoaG8au4PoBBTHLZ%2FcCZtNwexk2p%2FndcEsHZuVXcqa45OLsm%2BSaJvf4C3J0D%2FZtJclcfBsADf5ZEGlU9o6IrXA%3D%3D	false		high
http://https://a.nel.cloudflare.com/report/v3?s=sOH7aKZQs7HUmJ%2B%2BIpDazDd8U6kSBoRWr90OOINUwzQ6PDO6tOTlpT7hsiU%2F%2FIm7Mmoc82w9xaFVb7ORgr2CRA3wz2daEIcWiZsz1tp8VaBD76du9kWQg%2FV6l5uNug%3D%3D	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static.s123-cdn-static.com/uploads/4489441/normal_5fc8b59e7613e.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://zawasofolebu.weebly.com/uploads/1/3/4/9/134902788/6a0ec8.pdf)	osGcfBvGVu.pdf	false		high
http://https://xuzufudoroxibu.weebly.com/uploads/1/3/4/7/134755415/fewonuviwinulewipa.pdf)	osGcfBvGVu.pdf	false		high
http://https://voxonevixes.weebly.com/uploads/1/3/4/3/134383310/3212069.pdf)	osGcfBvGVu.pdf	false		high
http://https://denasigetul.weebly.com/uploads/1/3/4/3/134332190/3aadf349f71.pdf)	osGcfBvGVu.pdf	false		high
http://https://jatorogerujew.weebly.com/uploads/1/3/2/7/132710569/5650151.pdf)	osGcfBvGVu.pdf	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://static1.squarespace.com/static/5fc2d06c1452f90b7ff1a516/t/5fc81fa34b97230d050097b8/160695082	osGcfBvGVu.pdf	false		high
http://https://static1.squarespace.com/static/5fc59785d49dd12447543100/t/5fc892132dd5737571b7b636/160698011	osGcfBvGVu.pdf	false		high
http://https://static.s123-cdn-static.com/uploads/4451565/normal_5fc4be3b76a1c.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://vesumuzuvof.weebly.com/uploads/1/3/4/6/134685641/gewof.pdf)	osGcfBvGVu.pdf	false		high
http://https://cdn-cms.f-static.net/uploads/4498392/normal_5faf04625de48.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://cdn-cms.f-static.net/uploads/4381737/normal_5f9c867fda2cc.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://cdn-cms.f-static.net/uploads/4376874/normal_5fa0c5cb1b909.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://static.s123-cdn-static.com/uploads/4479223/normal_5fc8ecf96736d.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://cdn-cms.f-static.net/uploads/4365599/normal_5f9abc7d2f1a4.pdf)	osGcfBvGVu.pdf	false	• Avira URL Cloud: safe	unknown
http://https://daviwoza.weebly.com/uploads/1/3/4/6/134670821/rudaruzarafaw-nobokujiduv-nalegeji-regoresusa.	osGcfBvGVu.pdf	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.19.149	unknown	United States		13335	CLOUDFLARENETUS	false
142.250.184.78	clients.l.google.com	United States		15169	GOOGLEUS	false
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
35.190.80.1	a.nel.cloudflare.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:	778227
Start date and time:	2023-01-05 08:45:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	osGcfBvGVu.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:	20
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:	mal64.winPDF@31/50@10/8
EGA Information:	Failed
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): 23.211.4.250, 2.21.22.179, 2.21.22.155, 142.250.184.35, 34.104.35.123, 142.250.184.67
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, armmf.adobe.com, edgedl.me.gvt1.com, e4578.dscb.akamaiedge.net, acroipm2.adobe.com.edgesuite.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
08:46:01	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):	5.651264269000953
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QGA1cFFPtTxi7Z+P41:vDRM9ZPN8Zi
MD5:	5A146E81C1283D99CEBE393330065EDB
SHA1:	81D9087C4929126311BF2DB688A73ADBA038B140
SHA-256:	B42EF6028D554A61DAB9C108F76AB48313A8DD39E93139C08FDE1731068A4C50
SHA-512:	CCF94BBA1EF56584475D71229F417F016BF5C9680CE1B8BFC99FF9BB135F0A5A420B5E4FB063289FDA4ED081D7F04CE4919F9889201EC71EFC96F6C9044393AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ...z..P/....."#.D.[7....A.A..Eo.....<;.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.537510080355085
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVdRhvl//KtFZ9k9hyRktB8tl/le98fZe/O+/rkwGhj:mi9NqEYOFLvEk3BXK3ZG9jtBcQ8Be7YV
MD5:	FFF4BF122F668487E96379B42697CB11
SHA1:	54B981DE152D91189409DBF3C6A8820A0EEE18EF
SHA-256:	7C901F3DD63F94F40C715DECB607665D57B850124465B1DBC4A165BA5A2E399B
SHA-512:	398BF4D757545804A53ACFA4B2F5A3396D9A6D11C6185A7B4B1CCCB7C2A8420696CBF6FC8383876624D42C3A345487096A0D20A45640DB6FAC6C12F19FCD2BA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...g..P/....."#.D.....A.A..Eo.....E.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.590487812871175
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhu7h5atgCStPBet/RlUoSjGY1:DyeRVFAFjVFAFn+VSNBetZlUo6
MD5:	084040282D49E396F84728EAFFC71032
SHA1:	41305D731BB115869F108FD22E7A2CC6077D3E7E
SHA-256:	17C984321CB3A4A93B8A734ECBDFE05A36B842D3D47D3AD71C6625FCE361EB2D
SHA-512:	5CB6F2996AB3006448130D2699819D9EAFABB0188C2575FAA2846359F6FF0C7C12F783BF247BDA980B24D6A837A2F1F138A5550675879AB3B2809C22DEE6D4C0
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 ...x..P/....."#.D~.0....A.A..Eo..... .....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.662435631091272
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsMPtxFzuiWulHyA1:lbRkiDLHFzjWus
MD5:	35B82D319C5E038C75EF213244B46022
SHA1:	6F52F7207AA421A9374BA8CF4936C57357102CDF
SHA-256:	4967273216E89903C6E0776838F8F1663253A5CFDCAB284A923554349441C8BE
SHA-512:	2C8B39568F9323237C5357CC32F6A1CBFDBFE388FAADE18E44DFD346174D653CDECD6C6CABF7848AB55F430E9F7D0C4542E1D7B81CE31B37B28969EFDB1E9 154
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ...L..P/....."#.D..n....A.A..Eo.....WG.....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):	5.549099436111422
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu1Mtlr9tk/OVyh9PT41:pyixRu6yOV41T
MD5:	984EB0BE2BFBF345EFBF73964AA4EDAE
SHA1:	02A10BA62015C897940A6BAD2700890200EEEFD8
SHA-256:	1BB565CF93B744883D626339C95CF40844D47458654C92429CA1E140172182C0
SHA-512:	5C0ED8FDED7F820B91D876D9AD33E0F5EA2D372FD65BDF8CAC91C1E76C42C5755BD41DD5077BA16DC3FA759B706FD0A326D0E33D40BFEABDE316517B1125 9EB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .:.y..P/....."#.D..2....A.A..Eo.....o.....k.Q.....-_..y.....O...>..1....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.625605094369213

Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuV//RAyRktD9HlYo2sZl8xeGvP5m1:mvYOFLvEWdhwjQIRSthF3Zll6P41
MD5:	AC00BCEA5C23F5E5BCB29ED09FF84D73
SHA1:	7ADE26F5385A5F877F3F66EB5A159E113E246D11
SHA-256:	D875DCE9B2FF28106F499B2A1712F055352898F753B4C6907F8E8CF628447054
SHA-512:	10A1F637C6E28689B2EE58D0BE0823D35D6EFD49EE881BC842A62933A0E31A83986BEE0D52ABBA25F019F0EB971301FCD0201C119E6C1171BB48A7901250049
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...u..P/....."#.D.&.....A.A..Eo.....].>....uUf..N...k.....c..l.A ..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.539297172577375
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVJTA/tr/yRkt+HlcyxMtv9EWy:mJYOFLvEWdGQRQOdQwAtr9tCD6g1
MD5:	174CBFA2BEC041F61B82439D5779C755
SHA1:	547C61A8437B191A39E41CA539D199213BCAB830
SHA-256:	9B372E5A21433D36F2B8D42DC4DCEFB811D5B9F44BB12EE192FCE694EA899394
SHA-512:	372F825DB98D75B56934E6F717548C916AF65D737D657179DA8EA91098A28F519C4C56827B29E4538CD9E5851681E207958DCB504F7E6B4EA3B13C0A78DC2C07
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..;z..P/....."#.D..2....A.A..Eo.....E.w\.....c..y/L....|y.n..C/l.....X7-ne.A..Eo .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.523534256237215
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVWNiwA//ORk9hyRktbcHlrQMWqg4nRb7om5m1:mOYOFLvECMLWN8z9jt4FcuR/41
MD5:	85F5FF6EB806E206D0466D629F837026
SHA1:	1EE8B6B9550568E485A41BB60BA8D0F8E473E215
SHA-256:	7190C6DC75B4217838827A9E4AF70B98DEC8700019A4CF6EEE474CD353F35123
SHA-512:	C49BF31052FC5AD64194E70977EBD3A34D83A3965E97B7F0FEE487B0D5F71E6B68DF09ACC3FBFCF7A0D2E8F90B77B1285F1E39FA35D4EB2C3903BEDE5811FD 4D
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .."h..P/....."#.DJB.....A.A..Eo.....T.@y.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.532441048627083
Encrypted:	false
SSDEEP:	3:m+lS8FlC8RzYOCGLvHkWBGKuKjXKSO7p/KPWFvyefc/9mfqyRktUbXljYuuUy0tm:m4fPYOFLvEWdtuYJtOhby0zBUKSAA1
MD5:	2A14C6CCDA509E5A958A6D7731A60B28
SHA1:	7754B9D9B6DAC0B9F41EABEEC22254521D999052
SHA-256:	C63A65BFDDB48F914B517783DFBCB840C8CCC5AA6CC0D105DC94B66D6BEBEE8B
SHA-512:	14763447357D9C4848186B34A6F742C805DC2B947812E064F6F17DB2B19F9CC342E57653FCBB2A9DF7F4386466EC48D916593DF37B93D17EB1F4FC050146F8AD
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...z..P/....."#.D..3....A.A..Eo.....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):	5.495753128469255
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvFAu/FFA0hyRktUp9tlWd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvPFFLjtUTGjUdyA
MD5:	E0FFEE8E20F3FEB2C4E01560F1F593AD
SHA1:	0681C3996EE49224937FF5C95A8DBBA9016B851A
SHA-256:	A14B1D5331F13CF99B577315E8C4DB6A1B4699F2603ABF635849E0AC8FF77DCF
SHA-512:	158842D10C187466641C4EEF36B22C9CF5B5C87E9A4413951E1A52B4C5B0CF3B26FA51A5F3F40D2BB632C8E121F14E92CD4BA29E0BEA44A448DA54D03F678DD
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ...h..P/....."#.DT:.....A.A..Eo.....`/.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\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):	5.5042480757231225
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLvSTA/2ZhyRktpg9lBUPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLeAltpoiPqVyM+VY1
MD5:	122F21E415F022A4176F14595F2CCC36
SHA1:	F6CE0711195B080E7F201C192C3F1A17FB900783
SHA-256:	1E279689245A3576492C4A233BA9DF783087140A23710086CC427582CF27A30B
SHA-512:	1B9B0756AC1687F94A006EC215980F93E655D02A19ED66788641B27662B17772F886AE092A2D8C166780037ED44F2FDF217E9B6387F79D4199D4D194097B18DA
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .3.r..P/....."#.D_.....A.A..Eo.....S.....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):	5.601944536160576
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyClt1ptIHltwSeKaT9pr1:URVFAFjVFAFNmltwSeKaTL
MD5:	5AD817137B1CA4F2C469CF1EE37A46BF
SHA1:	E5BDC3CD0ABB3EC270BE36EFDB4FEFF3896DFECB
SHA-256:	4E2AB5DC3E0864593A5662E80960D146C89CEC68B8DDD9EBFF0AEC0EF7821DE1
SHA-512:	FE295FDE9372C26DB7EAC240EE40E1396C9FF12B994F115A7D0E7686C88034A27DDF74C4CA4EC7B96D5FBCECFD19FAAB6AC040C58DEEFF17C50A6F265200EB98
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/....."#.D..:....A.A..Eo.....t .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.470899420663224
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFviTHl/l19yRktDzyrpYFm1:ms2VYOFLvEWdvBIEGdeXuA7t/tDG11
MD5:	343DA849300BCBBF2905F4D90115A4FE
SHA1:	DFFC7AEF06502E6F4EBAEB49D51354FB311DD322
SHA-256:	586665AEB9236ACE24985CC1E2AE8EFE565777576D7C94D73D143622753CAC5F

SHA-512:	7423FD40304B94426C66FA7FC117C2E64359EC7E98F70DADD03A6B32F50BD84E9B06ED63312B1B8463B9B155025AC6BA3502C1B0F730CEEE46A32E13E7369A9 4
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ...y..P/....."#.D.V1....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):	5.643007513785333
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQ9AA1EB9t97xm7OhKlvA1:RbR16uAA+PL7xmJ
MD5:	AC891792956717CCB3DF61D5D522A533
SHA1:	CBEAAB0FECCE3BCAC844A1BBECF83218D830E2FE
SHA-256:	10814756142D888548320D026959050615B3179AEBC59098965D6FCC9ED28883
SHA-512:	B5BBFCFFC3E8C50017247041841C4122B371226D04E6618A8F6EA3C086E4C8CB058E677B12E7644D3D7C7A01A173190AC70EAAE95AC492B6A1EA4CC7F72F52 A
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...u..P/....."#.D3.....A.A..Eo.....n.....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):	5.600044661436762
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVui5lti7QtdPdFt1:B2geRHRQuMj
MD5:	71961E20BDC012096FFDE7A88003B347
SHA1:	D49CC67DE7A6B8FA84E7C5F3092BA434DF94DBE1
SHA-256:	9BDBFE1C0A8FADF92ECBC22990C3F034FA43528D80BF666B106BDD248DA2683E
SHA-512:	07BF9F7818F0DD603B1DCF77D58262ACCED96ED68D7F8892AC1ABEB78C51E7DEF90D31D939F3625071D21EB1BE819C5A81677000093D25B874A8F9BDBEA5C 27
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .E.y..P/....."#.D.L1....A.A..Eo.....R..$.....@..{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):	5.590585897549933
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuVYlA+//Jt3zyRktYi/gEnNWQ1SUy:mzyEYOFLvEWdrlOQv/Xj3htWEt1S/1
MD5:	2F5463829B4E37A1B3EB3E08EECBFADB
SHA1:	0BD6F4EB0D270067694E72E948FDE28CDA4C051C
SHA-256:	AEC0B4DFC33EBE8BE94B56C1A490A18B05B4FC1284A1DA63F181D96EAAEE5D0B
SHA-512:	CAACAE25767E7D846B39062322FF952BADF1B8F0CACD251F5078CA41DF61699F704195F394B7F4F40BE08AF650D720F7C22D36C843AF63DE65D3B5CAE453EB 0
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...s..P/....."#.D.....A.A..Eo.....Q.....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):	5.5576004126167975
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvZh5+//cxFyRkt+tglwJNqww6U+5y:mnYOFLvEWdhwyuzh8Xclt1lwrqwK+41
MD5:	EE1E00149780860FBC259B2A4404AA12
SHA1:	8E38D5D278B75510760319AB1EE2E279AED444A5
SHA-256:	BF8FF221491247FDA5460D35F4C07D05FC5379B1DDE3068DD09E11931D4D64DB
SHA-512:	B7A64CC1AED73AB4E862D6E19DF6E5AC4BCBA10EDFBCCCA87BFCB98631062000BF84FF3E2DF47C5A53F32E28E72480C1B2A161A4D4EADA607214808D2913A DD3
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .<9u..P/....."#.D.....A.A..Eo.....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):	5.539174678101686
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbur+XUAIG9tAQfO441:/RrROk/r0SzfL
MD5:	3493BB57A3C0D507A7E439A888901388
SHA1:	B0A974D831AB2A3C7387963D2BAF9A4FADD38862
SHA-256:	F99E58CF4C4DEE8CDB5710758C731DC518540B7FC53B92AEC7C23F572EF0DA02
SHA-512:	C8C39CB95347A33EEDB2D841BD2CE3D8DB06F4E5AB9E21736B86701322FF0CF8DD7856FEE601010FDAB7E7CDF06DB1D8D9F3BF08CBF00386E54BD2FBE4376 E1B
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..Ns..P/....."#.D.w.....A.A..Eo.....tFc<.....~..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):	5.563783987039112
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVtA//MFB9hyRktapzoIN1OFPL4m1:mmDEYOFLvEWXI+w9tMzV1QPLr1
MD5:	24A523A664E191C6C0212F9A9ACEF695
SHA1:	4EAB77FD95F1A8CEF5EB38F38BB8AE1EF6253A07
SHA-256:	F012788576942567756043 4A5F9734EF7D8EA36B4395C49BF0D26CD15ED9B217
SHA-512:	EA197F6200D9DC1E3EDD7C65E2191C1C0D0C4F03B919256076AC58A3642A1C47D1433D3756A25B147E6B5399C7CB70FE48B530D9456F19BBCDE6B664831DB7 B
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..vr..P/....."#.DT.....A.A..Eo.....q.F.....~]...%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):	5.606979550587912
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvmpAl/i5G/yRktiE8D6EsEJeUm1:m52YOFLvEWdMAu2AtiUtiEEvsEJ41
MD5:	A125E575CE16B293C686DB4C375EE0D7
SHA1:	3C2E841B65A3FE93A9CC745584682B67811A1BAD
SHA-256:	D3E693F747A5F753FC3405D888A2FC60F9AFC98D113125A542B95A75C3D74175
SHA-512:	A03CD2C81FBCE059D07FBE0769E7D6F454EA564861952FC3F7D19C5B4ABA2EEE29234F815278BBC870D5A818BDE59AC02BEBE2A7F6006CBA0672E0C62ACD4 18C

Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..My..P/....."#.D.1....A.A..Eo.....]}P.....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):	5.583998485910322
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuc0t/k9tnf4ong1:6lJRJN4o
MD5:	22D24EE2B0AF29BFC3FB61B5E55C9BA0
SHA1:	FFAB2BE67CB1448A0605525C5FD6BADDFC04562A
SHA-256:	4376CF8F8D5A9043A20B5912E8CC3F5B14ED23481D1F01298B148C953905A3FE
SHA-512:	364BB028CB34BC2D0A63D0839BE07F1F31D23277729D133968878AAD2062856401322A240F8813B5125E3B6DE12FBF0151B2C716EF20C8F85D0F7DD53431CFD7
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .).y..P/....."#.DnL2....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):	5.551141520865683
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/lu/7uk9tiVN16wG1:F8hRrROk/Br9sv
MD5:	2ACA4A28C0AD0579973BD257731C7EDF
SHA1:	07C1F524015D15613FD6E59A32C413D462AD07A8
SHA-256:	A66A49A7120E69DDFBAFC6C0A409CAE71E5C9302A6C4C865451E7354DDB882C0
SHA-512:	31A4299BE738D92487E6D66B6636798795A01FABED60D770500428A812C309A13965E0836152A04B233F4FA34F603EF18FC41742A2334B7F26F0C6774E6308C3
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..Js..P/....."#.Dwj.....A.A..Eo.....T.-.....%.k.SZ..~W.....:)'B..a d.....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):	5.628075666484812
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVZvt/a3yAyRktI4PmJelcz:mLrnYOFLvEWdrloJUQCv1aCSt7eJli1
MD5:	7402EAE4469897B16849BFF51A0FD98D
SHA1:	1059B385CF3448CB25A301A8A5BB535ED3479740
SHA-256:	39513D0092FACC6E54112256BECE9DF98B2C1E60035499314AC3E97DF4710EDF
SHA-512:	72A73B6445DE9A99A89AD575A6635DFE9277E34F68903C6ADD906F4FFB553D459BACC5EB4F43645733ED9509B10E49EFD0F6AF8FAAB1A64CDB63C43110A569 FD
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..s..P/....."#.DH.....A.A..Eo.....;"./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):	5.532702830810666

Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhueWTAIX+wnB9tVzgm2d/1:0RH/wnPLR
MD5:	CCC56642D98EBF9CF142D85FF8670CDA
SHA1:	B096F0B0CA50FB56929F91A04849CBF394F91E85
SHA-256:	488B92291DD8779C8174C88C0D0F2F931E6D0DBE8FE08021C52AE45891D7BA27
SHA-512:	0A21C5ED9E41293AA0B7FE3AEAB0C5F12BDAD3508188D5FBC9776AE681CC178FA5202DB2614FBA8FEBB0ED413C4C24C79CAE2636B69841ED423D3D826D2E2CEB
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .|.s..P/....."#.D.....A.A..Eo.....F.....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):	5.5764818797439695
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cv3TAl/JOG/yRktzlWBiaQ562HvpMm1:mAElVYOFLvEW1Ku0tkStNx56uvp1
MD5:	A7BF027076276AED32765F0435F8FC87
SHA1:	A96A5BD8C8C51F89E6BB8EB2C8356E7AD210F583
SHA-256:	F03C340BC39B7BAC1F9422272F6ADF327D342BBA55320A8E7AEAD8E1B16AA95A
SHA-512:	7A29122CC671BEB9839F296E1A369DDB9AFB7F891B92037911B755164E9A0B9BD1392C5E9379F6D01468F3942582DA9F3CDF75D28F288486B651527128B1D267
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .&vj..P/....."#.D.....A.A..Eo.....cm.....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):	5.631542926305818
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu/38ltAstjjUDLYtmOZn1:xRBJ8sfNoDcFZ
MD5:	A474C2C25A9BCD395B4376FBB913E925
SHA1:	28F35777BDE4A29CF995C67FD121F2E980C02C93
SHA-256:	8CC1D963A9F9A41F0CA05A5BEE1FD5BA54D9045151D5525CE726F5AFAF89E1DA
SHA-512:	9A66100D8FCF1F5868B4015D4F8FA97D8827A4A5CDBDFCCC202DE2F98C04C5DE6DB7041A0D5D28A24ED9D6EA748B8F97FA96072F8EB24D24BB1C64BFBD54B0B3
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ...y..P/....."#.D.I1....A.A..Eo.....8.Q$.....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):	5.549439071578889
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvywA+//K0phyRkt4/npSKGi:msRPYOFLvEWIa7zp7tWxjtG8VPu1
MD5:	B928D4B8D7F835E560A61643A7CF14EC
SHA1:	812961730DDCEC1E16088AC4CE2C9A4AEEF0956C
SHA-256:	CA39E9BAC6312FAC4C709C4B9F071B004562B9AB58E8EA9C0A5A03EA13065DB9
SHA-512:	CA80EBAC718021E5436A31C19F99F75841491AF471026A05F7212922CCFD5BE63AC232813429BBE94365DBEE289017B0E964C40623E80A974E14F17EC55DC0EA
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..$h..P/....."#.D.o.....A.A..Eo.....*.....L...Im.@.....E.nW...IP..A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.562799433969287
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVGAl//EAyRktY9Hlll6F4XVAZ+Y:mKPYOFLvEWdENU9QIXrtaCwiM3Y1
MD5:	12FA28AFC62752E3BBD4847932A37301
SHA1:	6D7283835C62DDF60B37D19EC7BB11A8C61333A0
SHA-256:	7402DD35C7503A79A9F03E870735DC40A16D28A991163A38165089459146C9DA
SHA-512:	C8FAD6F9B9CC063266B4564D55C0ADFB580F74DC43954FDE9A5BC5A6B55728E0D49F6019959A33F4CD376D7CF935E9037DAC382EBA57DC869B39714070A27F6
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ...u..P/....."#.D.....A.A..Eo.....rm.....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):	5.612037774931721
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQIA1WiStsjBRCh/41:XRc91iSaDi/
MD5:	730374216ACA940FA2021F40771FF05E
SHA1:	8FA20AFFFA897D12431F0A69ECE1FCCADC5BFF75
SHA-256:	504B0BEA90ED77852FD11B4B92C031729579D980CB478D91FDB58AF2BB2C0894
SHA-512:	5D89F1F74F6DE7915FC5748C4598B3C9F27F1B890973EDED4688A24FA8BEBD3C67D0D38282154D8789DA83821DEBBFFEF1ACABA90BFCF5C23765C27BB6CE9CA
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .i9z..P/....."#.D..>....A.A..Eo.....R.....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):	5.569221985379349
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuH1s0tkIN/kUlF4r1:bs6xRkilO0Z/7LlF4
MD5:	708A8467795059D1BF9929B8AA7384A2
SHA1:	7AE1722EB0B949AB4BBA5F7E4D1F928F217EA4DB
SHA-256:	B30807EB656CFC6D9995BE2ED7F6BA3E1BF2F452A42A8C68FAD18507C275FB59
SHA-512:	6FEE0722B726793A573CC14A7CA2111ED3D46EE2D4B89379232D03A50CE756839A3ED1576C44F9A50330BE9092A728C5E8D1E6516544F7FC674366429D5FEDE
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...J..P/....."#.DZ.e....A.A..Eo.....P...#4..I....5. ..5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\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):	5.504281726105637
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvq9wA/6+qyRktNx//XECcu1isLKo:mhYOFLvEWd/aFu09N7QtNZPEN941
MD5:	657D1E649CE96E78E544439A71721F27

SHA1:	CC6E500692D81FA38B51453CAF2539437A306110
SHA-256:	BAAA26E72A9017F67A10E98D7AFC54C3F83E9263D996FC27DFD1D90609D8E04C
SHA-512:	31C5A4FC83C2F356F27082B43D8930BE645C493D4D68125B3B6D958CB7C1FA653DD7F52FA3D49DE6C2C35A8FD9368C00A65D15FD8AC8F7612ACB8BC0BF112 F1
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .o.{..P/....."#.Dcd3....A.A..Eo.....X).....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):	5.5209317682351555
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQtc1u6FPt2tVBMqVd3G4K41:2DRuR+cYm4tVB9Vd2
MD5:	898D655F8BF13C17E8AA39F07DF307D5
SHA1:	3D6331F53ED25192F323A34CE119A60DFA7BD37A
SHA-256:	7C994FA5019A358E4AAFABC0E627BFB2ACB4507274F8A99F0D21B233B8DA9495
SHA-512:	22402ECAD5BD7758929C3867CC72D524C6FB3F2B871C955C6A53C74E5EB51389A11BBE0C8239FC04351C56A1A19D2F2955ED0F14BD15E88C476119BE3F10BC E
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...z..P/....."#.D..2....A.A..Eo.....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):	5.540976625647461
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Q5KAK12tTuA424r1:+RQGKkor
MD5:	7770C533C0AEB9E516FD09059AB6E227
SHA1:	3443A2AEE37AB844545CF0DFCC1574E3FBCA1930
SHA-256:	A52294F4CEB182F580A50FC694A1F2B9723B2F7FAB27D9CCB7C308A2234EB02A
SHA-512:	6DF269B84B2B507B2AD985E88B4E1E3DE8E96FAF0F61D82C6C27DFDE9424061386A7BB4E81C2D68314834C2E27B5E890DA933E17EBA282112AB7D015726A921 C
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .n.z..P/....."#.D5@?....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):	5.538244791476342
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFvmS3AKl//j9yRktLl9Ag2iHiE:moXXYOFLvEWdENUAuTAKlXbtHyC8n1
MD5:	1FF9F15E370DCF06CC555035EAE44DD2
SHA1:	86C5BB46082D974E31B2A76DAE34CBE70FE9F7DE
SHA-256:	6737BB29ED58753FD2DD7491711CEC460A22B64DF306044D21EABA1038044727
SHA-512:	93532B49C86A6306B902735D52BE2E0734E45966EA3D44FA9434A31ED4AE63F79F8384E8E271D7FC0C813DA89A15FEB81D7135490DBD090120AE0C4BBB6AF1A 2
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..7u..P/....."#.Do.....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):	5.589174597634885
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQ7TAXF1IStEnsLmB41:nRrROk/VrIS0N
MD5:	916C62960F479AD206030347D42B50A0
SHA1:	F9F9309361634FCF9B99BDD54BD5D4B6D7FB75EE
SHA-256:	2FD5A792BC2A8173ED05D5B8CA05B5A99EF960D7958A5467CD52350F359E3386
SHA-512:	FED4E54C518FE834495BB1C9D3AA5F4C5D0521C0F267D87AA9DCFE051B1DDDFE09DFF9EF7B1DC122053963D01D4221E177EB5F4848D808E2D4584DD1F86C50A
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ...s..P/....."#.D.....A.A..Eo.....c..... ./.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):	5.5722295878055075
Encrypted:	false
SSDEEP:	6:mZ/IXYOFLvEWdccAWuSTA+It59Qt2Ldm9741:qxRc4AQS0du7
MD5:	562035C1E3ED036B736BB76BB1DC613F
SHA1:	97AD6972E3DDFC976DAB1D34BC587328117F637A
SHA-256:	4BD822C42E1770CCA9D0389A0E61B4A34DD754EFE18865338D5EA938007A1DD1
SHA-512:	1E5BBADD24F0269C5A578263D2848663559E81257D6F82134A3AE68E7ECA1DD5A1F406A6333AAAD44C72E0FF5EF1AEBB35FD928BBB37CF79F361DA801BA045DF
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ...y..P/....."#.D.*1....A.A..Eo.....n.....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):	5.521016110491071
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvSwAl//11CAyRkt0/2B6shoq+Nem1:mMOYOFLvEWdwAPVuo9X3xt0OB6Jn1
MD5:	C4F6704C5E6EE4F894B7E69D2DDE078E
SHA1:	0D369D20A8EEA10106EDC75B22ECE6F9F0796E76
SHA-256:	99AA4FF6029C767F391946A6B8899A6037A3BB8C6731326873CA86713442E92D
SHA-512:	276109667151DF692725925CF35EBE205798E3C05B825C4B666D0A6CC642DCA0B7ECC5666C20A631FBD28BD2816647BA9258C682C06B817BCAC11E46992CB68
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .I2u..P/....."#.D.Z.....A.A..Eo.....Or.....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):	5.633428001301942
Encrypted:	false
SSDEEP:	3:m+lUDfllla8RzYOCGLvHkWBGKuKjXKBRSJvBCvlKLuV9u/a1IAyRktByN/hcfsy:m3PXYOFLvEWdBJvYQLa1PtehcsBXlh1
MD5:	789856E00911E40E6220F44B0257FF72
SHA1:	DD293AC6511E5A1591FE1105FD60B9939081BF5C
SHA-256:	80EB8ACF37AF6577B09A0E218D438506360780A27784ACED553A8EB4DFD3BD97

SHA-512:	8ECDA07898688FFF7146B9DA19DB7360A7265959EAC8BD263082D4748A30F6672F4A0A37A7AB5F839F0FAE2B9509216275C0D325351FCB190D71B95768AE1125
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .9.z..P/....."#.D".3....A.A..Eo.....un?~.....k..`..N3.... ..d..$[.....{.A..E o.....

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):	5.585165841947906
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQITAXuuht7c3Me/1:3RrROk/sgTTuhB
MD5:	77EC7B5C7F4043DD49997B9668B5CC0C
SHA1:	B9BF7C4F9BC20B79DB0A9250A3150658E204D465
SHA-256:	CA231AD13B1A1CFC739FFF6FC81674488C9F55F5F06A48F3DA5C02DDE115BA32
SHA-512:	1A3968397E612F787EA1BF0BBB3B143B6925B0D2F23F0D75BED54E3B3E462F95EB035C7ED2119598213E127D5377E6C4DD8B8085E08DE1D44EF77138AFF94F8
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ...s..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:	modified
Size (bytes):	1032
Entropy (8bit):	4.9671046890677895
Encrypted:	false
SSDEEP:	12:TU4un2GIslyHMzltnjLREb1cI/ej6X5tXiI5yXAS5fzzF/6fnj:Qna3HMf2R3eQcvQSlzJ6fj
MD5:	597A0C79CB38A5815AF8C2D01461A186
SHA1:	306D18AF664F192DA5DE0BDE7320A5074F03C001
SHA-256:	2FD71109C294666BA69927531EF4BD30B621161C9D8C6DF5CD20031ABA239341
SHA-512:	5755BA845E3189DCF157C5DB1C261912CA00DD3AF23800CD335A7C8BF744D403EBC2E1279A1F30B7A348589FC400CDBB0834E288D0BB001209C920EAA60CF9 5
Malicious:	false
Preview:	...._...oy retne....).....T.....3.....p..P/.....v...q....a..P/.....C..M.....k.....#...(...k.....]...I.@.C..P/.....@.C..P/.....6<|.....a..P/.....<...W..J..a..P/.. .....oB*..a..P/.....a.....a..P/.....;.y~A...p..P/.....P....V..p..P/.....F..=z;...p..P/.....o...p..P/.....*....p..P/.....2q.....p..P/.....Gy.'.h...p..P/.....k 7A...p..P/.....:..N.A....p..P/.....;/.....p..P/.....p..P/.....P[. q..p..P/.....,+..._.#..p..P/.....J..j.....p..P/.....A?.2:....p..P/.....q...p..P/.....u\]..q..p..P/ .....!...0.o..p..P/.....*.....p..P/.....o..k....p..P/.....^.~..z...p..P/.....[.i..%...p..P/.....+.{..'..p..P/.....@..x...p..P/.....*)....J:..p..P/.....MV3....p..P/.....& .S.....p..P/.....D.4...p..P/.....+.U.!..V..p..P/.....~.,.4>...p..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):	1032
Entropy (8bit):	4.9671046890677895
Encrypted:	false
SSDEEP:	12:TU4un2GIslyHMzltnjLREb1cI/ej6X5tXiI5yXAS5fzzF/6fnj:Qna3HMf2R3eQcvQSlzJ6fj
MD5:	597A0C79CB38A5815AF8C2D01461A186
SHA1:	306D18AF664F192DA5DE0BDE7320A5074F03C001
SHA-256:	2FD71109C294666BA69927531EF4BD30B621161C9D8C6DF5CD20031ABA239341
SHA-512:	5755BA845E3189DCF157C5DB1C261912CA00DD3AF23800CD335A7C8BF744D403EBC2E1279A1F30B7A348589FC400CDBB0834E288D0BB001209C920EAA60CF9 5
Malicious:	false
Preview:	...._...oy retne....).....T.....3.....p..P/.....v...q....a..P/.....C..M.....k.....#...(...k.....]...I.@.C..P/.....@.C..P/.....6<|.....a..P/.....<...W..J..a..P/.. .....oB*..a..P/.....a.....a..P/.....;.y~A...p..P/.....P....V..p..P/.....F..=z;...p..P/.....o...p..P/.....*....p..P/.....2q.....p..P/.....Gy.'.h...p..P/.....k 7A...p..P/.....:..N.A....p..P/.....;/.....p..P/.....p..P/.....P[. q..p..P/.....,+..._.#..p..P/.....J..j.....p..P/.....A?.2:....p..P/.....q...p..P/.....u\]..q..p..P/ .....!...0.o..p..P/.....*.....p..P/.....o..k....p..P/.....^.~..z...p..P/.....[.i..%...p..P/.....+.{..'..p..P/.....@..x...p..P/.....*)....J:..p..P/.....MV3....p..P/.....& .S.....p..P/.....D.4...p..P/.....+.U.!..V..p..P/.....~.,.4>...p..P/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF52ad0a.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	4.9671046890677895
Encrypted:	false
SSDEEP:	12:TU4un2GIslyHMzltnjLREb1cI/ej6X5tXiI5yXAS5fzzF/6fnj:Qna3HMf2R3eQcvQSlzJ6fj
MD5:	597A0C79CB38A5815AF8C2D01461A186
SHA1:	306D18AF664F192DA5DE0BDE7320A5074F03C001
SHA-256:	2FD71109C294666BA69927531EF4BD30B621161C9D8C6DF5CD20031ABA239341
SHA-512:	5755BA845E3189DCF157C5DB1C261912CA00DD3AF23800CD335A7C8BF744D403EBC2E1279A1F30B7A348589FC400CDBB0834E288D0BB001209C920EAA60CF95
Malicious:	false
Preview:	...._...oy retne....).....T.....3.....p..P/.....v...q....a..P/.....C..M.....k.....#...(...k.....]...I.@.C..P/.....@.C..P/.....6<|.....a..P/.....<...W..J..a..P/.....oB*..a..P/.....a.....a..P/.....;.y~A...p..P/.....P....V..p..P/.....F..=z;...p..P/.....o...p..P/.....*....p..P/.....2q.....p..P/.....Gy.'.h...p..P/.....k 7A...p..P/.....:..N.A....p..P/.....;/.....p..P/.....p..P/.....P[. q..p..P/.....,+..._.#..p..P/.....J..j.....p..P/.....A?.2:....p..P/.....q...p..P/.....u\]..q..p..P/ .....!...0.o..p..P/.....*.....p..P/.....o..k....p..P/.....^.~..z...p..P/.....[.i..%...p..P/.....+.{..'..p..P/.....@..x...p..P/.....*)....J:..p..P/.....MV3....p..P/.....& .S.....p..P/.....D.4...p..P/.....+.U.!..V..p..P/.....~.,.4>...p..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):	292
Entropy (8bit):	5.185030844199834
Encrypted:	false
SSDEEP:	6:kOjd1FHq2Pwkn2nKuAl9OmbnIFUtjjdBZmwJjdbkwOwkn2nKuAl9OmbjLJ:kOxPvYfHAahFUtjxB/Jxb5JfHAaSJ
MD5:	9CE51067941ECE49660A2ADE4DDE9FF9
SHA1:	04EB808FB08CFC26642C88C38EC582DADCBFA0B9
SHA-256:	FD11810774DE9FC895DBB8C350C054E652F22955C2C5C8E0F929E513B516FA87
SHA-512:	985C5806CCED660B978111764D146FBE6E82AD835341549E184746437D0091EC84A1DA86F99F690823B4033A7A8C8C67B65212FC23F31D5EED2E4019014FA697
Malicious:	false
Preview:	2023/01/05-08:46:05.232 1460 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-08:46:05.233 1460 Recovering log #3.2023/01/05-08:46:05.233 1460 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):	292
Entropy (8bit):	5.185030844199834
Encrypted:	false
SSDEEP:	6:kOjd1FHq2Pwkn2nKuAl9OmbnIFUtjjdBZmwJjdbkwOwkn2nKuAl9OmbjLJ:kOxPvYfHAahFUtjxB/Jxb5JfHAaSJ
MD5:	9CE51067941ECE49660A2ADE4DDE9FF9
SHA1:	04EB808FB08CFC26642C88C38EC582DADCBFA0B9
SHA-256:	FD11810774DE9FC895DBB8C350C054E652F22955C2C5C8E0F929E513B516FA87
SHA-512:	985C5806CCED660B978111764D146FBE6E82AD835341549E184746437D0091EC84A1DA86F99F690823B4033A7A8C8C67B65212FC23F31D5EED2E4019014FA697
Malicious:	false
Preview:	2023/01/05-08:46:05.232 1460 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-08:46:05.233 1460 Recovering log #3.2023/01/05-08:46:05.233 1460 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~RF5230f4.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.185030844199834
Encrypted:	false
SSDEEP:	6:kOjd1FHq2Pwkn2nKuAl9OmbnIFUtjjdBZmwJjdbkwOwkn2nKuAl9OmbjLJ:kOxPvYfHAahFUtjxB/Jxb5JfHAaSJ
MD5:	9CE51067941ECE49660A2ADE4DDE9FF9
SHA1:	04EB808FB08CFC26642C88C38EC582DADCBFA0B9

SHA-256:	FD11810774DE9FC895DBB8C350C054E652F22955C2C5C8E0F929E513B516FA87
SHA-512:	985C5806CCED660B978111764D146FBE6E82AD835341549E184746437D0091EC84A1DA86F99F690823B4033A7A8C8C67B65212FC23F31D5EED2E4019014FA697
Malicious:	false
Preview:	2023/01/05-08:46:05.232 1460 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/05-08:46:05.233 1460 Recovering log #3.2023/01/05-08:46:05.233 1460 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):	0.008907738108328683
Encrypted:	false
SSDEEP:	3:ImtV/CuttMTLS/Jf0lt+urQTID7vt/lcvmllP62/X:IiV1kTLLlousTxvv6m
MD5:	0A339004BCB425813505AE2871E61E20
SHA1:	9BDA040B5589E1B919A259DB212F4CE8E32AAA8F
SHA-256:	46828E139BE167C9E36B556EB137571DE93A29930C366CE0666B1385BC106517
SHA-512:	DA3CE56FFA0538D022A80F7F6DAE1E89586E27FC484E82CCCAADC9EE163BEBBEDA2CAB446D507C622BAE868086E382F5436E328418BB877FBBF0A2192CB61DF8
Malicious:	false
Preview:	VLnk.....?.....).0k..... .....U....n..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230105074603Z-204.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32, cbSize 65110, bits offset 54
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	2.119756110074785
Encrypted:	false
SSDEEP:	48:HV611T10sCqbbJ9gwVzyxW9+sGbMbvq0bO1bbbbgvq0bbvqvzPvKZGL5:OmpxWoXP
MD5:	50E0B6F41EBC4EBA4269BCC68549650F
SHA1:	BCFAF794843CC99599F19D39F583FE2212B5E45C
SHA-256:	285E0322149221AE993B67B6C3C4A393E53E280A8CF708E845F2AF9D3B4AC87E
SHA-512:	99D00BF976DF9D451D97C46CF8D669520A582BA4A40C424909A7A47509A0B4468F0A4B9449B8BB0E6EE870F1640D7D50737476AE88318EF019A7FAE507252644
Malicious:	false
Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000, file counter 16, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 16
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.5681688291043296
Encrypted:	false
SSDEEP:	384:XeT9dThOtELJ8fwRRwZsLRGlKhsvXh+vSc:RkYZsLQhUSc
MD5:	1493E25F56A03B4FEA5369E5DD04B3A7
SHA1:	C6AFA44FB16877C0D67365F49D370A1FFD4A9C35
SHA-256:	F581ED070EA0F16ECFA2C0FD23558B56F3C3E49B78B58A6F63B4C245F1602213
SHA-512:	7C20A9E12175AEE2CD8AAD4391FF2FC88AC63047D5B94A5B7D61FFAFA75F5687C5D80FF18900B44E476722EDFC0EDBFDDEE5CA4973C7BC284085C4181E1C3F6B
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):	3.317225112358044
Encrypted:	false
SSDEEP:	48:7MT2iomVQYom1C4iom8Vom1Nom1Aiom1RROiom1Com1pom18iomVKiom9tqQlmFk:7BCg4OhoCK0N49IVXEBodRBkk
MD5:	A355ED99152FB1E8C5C758AE57969A86
SHA1:	4D837F790416C6A41AB2DECC32EA59365DF4BFE3
SHA-256:	F76A43BBAC2BA708498A437EA3B2B9D3DD95453F484B678AF32CC1AE4E27E224
SHA-512:	83BD2FB3B74DC3239EBE4BF09800E0264E8EAB7D1B9C852F82B81FC3C8CDB84B2488A7B4D9796B810361C9254292E0A0461EE1CD10A0FB46D6054B0695AE86AB
Malicious:	false
Preview:	.... .c.....w7.....W....<.W.L...y.....~.....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0ZJop4HOiA4PlxmzO3hGEwP/L2TYyu:J0GpiyVFihJop4uiA4N0EwPDgK
MD5:	ADFA47D162BDEE44A5AB1A381B1AC532
SHA1:	D70D719D929022B54AC149689E0E58CCAA5E4014
SHA-256:	CEC98B7B1A11DD8C64276B0B64D2E519D5D84B75C5A7818503065AA2D5E26E81
SHA-512:	5328DC062429AE2E8E0E13DF029506CAF00A29B6218941616E6181F736CEA7E0267B1B55F559D99A0BA7F7DA8366FC7CB6C454C799E6C1FB8E56B58B2B40DB4C
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

Static File Info

General

File type:	PDF document, version 1.7, 1 pages
Entropy (8bit):	7.192184687915834
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	osGcfBvGVu.pdf
File size:	88562
MD5:	63672c42600627b14529533173ea7bba
SHA1:	df1d0775e3a8bbb589cce7cf13477d03363775f2
SHA256:	8f0a22d21e75b4980311b759feedb88e338a777d9aba56ee85ef462482520272
SHA512:	081bd2a99b582bb229be375948ca0f7c13fdf33ec3d4c311c55e4af6e412d5b3834cf5571907a7ca614ea4052a9d8c1bf294786d1def07584ff057331ae59c5b
SSDEEP:	1536:HU+TufdDhNPxUHh42Pf0tjoXK/OKWeg6N7pEUpTmS9lqxNZJe42HFBHFfIlc:0CulDmHE9rWeg6zqnj2l4lc
TLSH:	1783E1F0E444DFCDF669DFF23B27B418F55AB34295DAA0C701AC835399C2C9552A3A0A
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Outlines 48 0 R /Pages 2 0 R /PieceInfo<</SPenSDK_PAGE_LIST<</LastModified(D:20230103102849)/Private<</Bin0 47 0 R /Count(1)/Length(3044)>>>>>>/Type/Catalog>>..endobj..2 0 obj..<</Count 3/Kids[4 0 R 22 0 R 42 0 R]/Type/Pag

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.192185
Total Bytes:	88562
Stream Entropy:	7.119699
Stream Bytes:	79743
Entropy outside Streams:	5.369962
Bytes outside Streams:	8819
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	49
endobj	49
stream	11
endstream	11
xref	1
trailer	1
startxref	1
/Page	3
/Encrypt	0
/ObjStm	0
/URI	34
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

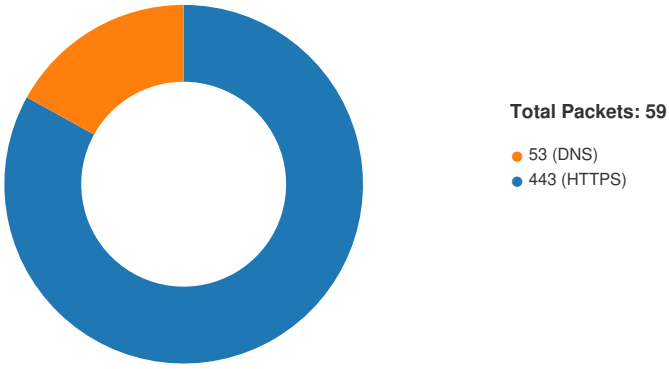
Image Streams

ID	DHASH	MD5	Preview
21	ab84748d4c708480	294211d7873f0375a1c1d5f511c202d6	
43	0000000000000000	fb97e3714e67ccb06f3945e45704fd8b	

ID	DHASH	MD5	Preview
45	0000000000000000	f5c5d01541aa7db524c0fce2b0150b2c	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:23.569751024 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.569825888 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.569933891 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.570164919 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.570195913 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.570707083 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.570755959 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.570835114 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.571063042 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.571077108 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.577047110 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.577121973 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.577212095 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.577496052 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.577522039 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.628897905 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.654439926 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.654481888 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.659209013 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.659321070 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.683748960 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.686728954 CET	443	49701	142.250.184.78	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:23.689462900 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.689531088 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.689753056 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.689807892 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.690077066 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.690165043 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.690924883 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.691034079 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.691989899 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.692128897 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.982206106 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.982270956 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.982513905 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:23.982525110 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.982609034 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:23.982729912 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.982811928 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.983243942 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.983330011 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:23.983364105 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:23.983527899 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.983561039 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.983719110 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:23.984289885 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:23.984308004 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:24.027431011 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:24.027563095 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:24.027561903 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:24.027657986 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:24.049113035 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:24.049253941 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:24.049310923 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:24.049504995 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:24.049602032 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:24.050724030 CET	49701	443	192.168.2.4	142.250.184.78
Jan 5, 2023 08:47:24.050755024 CET	443	49701	142.250.184.78	192.168.2.4
Jan 5, 2023 08:47:24.062949896 CET	49699	443	192.168.2.4	142.251.209.13
Jan 5, 2023 08:47:24.063009977 CET	443	49699	142.251.209.13	192.168.2.4
Jan 5, 2023 08:47:24.179107904 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.179157019 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:24.279122114 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.317306042 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:24.353859901 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.353908062 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.353992939 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.354515076 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.354538918 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.379089117 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.379121065 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:24.405901909 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.410754919 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.410806894 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.412288904 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.412406921 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.414802074 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.414820910 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.415008068 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.415249109 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.415281057 CET	443	49703	35.190.80.1	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:24.423013926 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.423295975 CET	443	49700	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:24.423396111 CET	49700	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.479104042 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.552027941 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.552124977 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.552208900 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.552515984 CET	49703	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.552536011 CET	443	49703	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.553459883 CET	49704	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.553518057 CET	443	49704	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.553611994 CET	49704	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.554135084 CET	49704	443	192.168.2.4	35.190.80.1
Jan 5, 2023 08:47:24.554160118 CET	443	49704	35.190.80.1	192.168.2.4
Jan 5, 2023 08:47:24.600177050 CET	49705	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.600218058 CET	443	49705	104.21.19.149	192.168.2.4
Jan 5, 2023 08:47:24.600300074 CET	49705	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.600586891 CET	49705	443	192.168.2.4	104.21.19.149
Jan 5, 2023 08:47:24.600605011 CET	443	49705	104.21.19.149	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:47:10.081274986 CET	58565	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:10.112699986 CET	53	58565	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:23.492022991 CET	61007	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:23.492961884 CET	60686	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:23.507110119 CET	61124	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:23.512403011 CET	53	60686	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:23.525136948 CET	53	61007	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:23.535167933 CET	53	61124	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:24.331460953 CET	64906	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:24.351005077 CET	53	64906	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:26.763458014 CET	61088	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:26.781332016 CET	53	61088	8.8.8.8	192.168.2.4
Jan 5, 2023 08:47:26.786401033 CET	58729	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:47:26.803812027 CET	53	58729	8.8.8.8	192.168.2.4
Jan 5, 2023 08:48:24.547538996 CET	51419	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:48:24.567121983 CET	53	51419	8.8.8.8	192.168.2.4
Jan 5, 2023 08:48:26.826318979 CET	52437	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:48:26.845930099 CET	53	52437	8.8.8.8	192.168.2.4
Jan 5, 2023 08:48:26.849025965 CET	52825	53	192.168.2.4	8.8.8.8
Jan 5, 2023 08:48:26.868598938 CET	53	52825	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 08:47:10.081274986 CET	192.168.2.4	8.8.8.8	0x847	Standard query (0)	traffmen.ru	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.492022991 CET	192.168.2.4	8.8.8.8	0xae7f	Standard query (0)	traffmen.ru	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.492961884 CET	192.168.2.4	8.8.8.8	0x177b	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.507110119 CET	192.168.2.4	8.8.8.8	0xc552	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:24.331460953 CET	192.168.2.4	8.8.8.8	0x8c7b	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:26.763458014 CET	192.168.2.4	8.8.8.8	0x1c4	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:26.786401033 CET	192.168.2.4	8.8.8.8	0xbfcc	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 08:48:24.547538996 CET	192.168.2.4	8.8.8.8	0x28d0	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:48:26.826318979 CET	192.168.2.4	8.8.8.8	0x32c1	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:48:26.849025965 CET	192.168.2.4	8.8.8.8	0x1aa8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

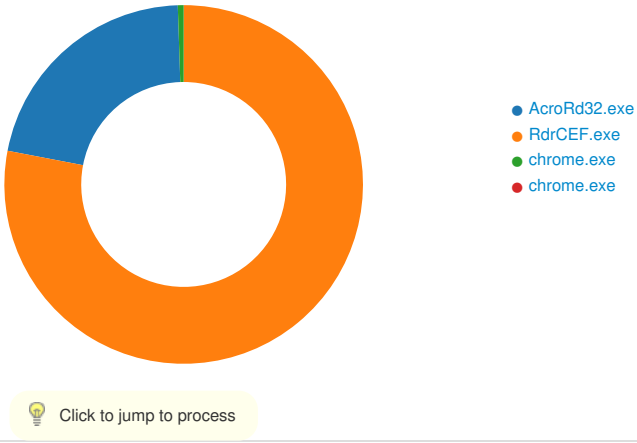
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 08:47:10.112699986 CET	8.8.8.8	192.168.2.4	0x847	No error (0)	traffmen.ru		172.67.186.133	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:10.112699986 CET	8.8.8.8	192.168.2.4	0x847	No error (0)	traffmen.ru		104.21.19.149	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.512403011 CET	8.8.8.8	192.168.2.4	0x177b	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 08:47:23.512403011 CET	8.8.8.8	192.168.2.4	0x177b	No error (0)	clients.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.525136948 CET	8.8.8.8	192.168.2.4	0xae7f	No error (0)	traffmen.ru		104.21.19.149	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.525136948 CET	8.8.8.8	192.168.2.4	0xae7f	No error (0)	traffmen.ru		172.67.186.133	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:23.535167933 CET	8.8.8.8	192.168.2.4	0xc552	No error (0)	accounts.google.com		142.251.209.13	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:24.351005077 CET	8.8.8.8	192.168.2.4	0x8c7b	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:26.781332016 CET	8.8.8.8	192.168.2.4	0x1c4	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:47:26.803812027 CET	8.8.8.8	192.168.2.4	0xbfcc	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:48:24.567121983 CET	8.8.8.8	192.168.2.4	0x28d0	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:48:26.845930099 CET	8.8.8.8	192.168.2.4	0x32c1	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:48:26.868598938 CET	8.8.8.8	192.168.2.4	0x1aa8	No error (0)	www.google.com		142.250.184.36	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- traffmen.ru
- accounts.google.com
- a.nel.cloudflare.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: **1840**, Parent PID: **3528**

General

Target ID:	3
Start time:	08:45:56
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\osGcfBvGVu.pdf
Imagebase:	0x1080000
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	10CCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	10CD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	10CD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	10CD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	10CD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	108EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	108EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	108EA55	RegCreateKeyExW
\Device\HarddiskVolume4\Users\user\Desktop\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	10CD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	10CD41D	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	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/osGcfBvGVu.pdf	success or wait	1	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	osGcfBvGVu.pdf	success or wait	1	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	10DDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 6A 6F 6E 65 73 2F 44 65 73 6B 74 6F 70 2F 6F 73 47 63 66 42 76 47 56 75 2E 70 64 66 00	success or wait	1	10DDF69	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 38 34 36 30 32 2B 30 31 27 30 30 27 00	success or wait	1	10DDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	88562	success or wait	1	10DDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	3	success or wait	1	10DDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	10DDF47	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	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	10DDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	10DDF69	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	10DDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 31 33 35 31 2D 30 37 27 30 30 27 00	success or wait	1	10DDF69	RegSetValueExW

Analysis Process: RdrCEF.exe PID: **5988**, Parent PID: **1840**

General

Target ID:	10
Start time:	08:46:01
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:	0xc80000
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
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	16	D883E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	68	D88447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	164	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	5	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	16	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	3	D759E2	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	10	D759E2	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	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1629	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	D759E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	D759E2	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	3	D759E2	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	3	D759E2	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	3	D759E2	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	3	D759E2	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	3	D759E2	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	6	D759E2	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	3	D759E2	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	3	D759E2	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	3	D759E2	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	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	2	D759E2	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	D759E2	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	3	D759E2	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	18	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	D759E2	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	D759E2	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	D759E2	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	18	D759E2	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	3	D759E2	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	41	D759E2	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	3	D759E2	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	45	D759E2	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	3	D759E2	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	85	D759E2	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	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	D759E2	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	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	35	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	D759E2	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	15	D759E2	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	3	D759E2	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	5	D759E2	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	2	D759E2	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	D759E2	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	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	D759E2	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	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	13	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	D759E2	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	15	D759E2	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	3	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	179	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	D759E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	169	D759E2	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	2	D759E2	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	8	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	215	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	D759E2	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	199	D759E2	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	3	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	16	D759E2	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	2	D759E2	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	D759E2	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	2	D759E2	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	325	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	D759E2	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	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	D759E2	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\css\main-selector.css	unknown	4096	success or wait	2	D759E2	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	2	D759E2	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	4	D759E2	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	2	D759E2	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	148	D759E2	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	2	D759E2	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	12	D759E2	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	2	D759E2	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	31	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	48	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	D759E2	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	7	D759E2	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	2	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	D759E2	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	2	D759E2	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	2	D759E2	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	2	D759E2	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	196	D759E2	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	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	D759E2	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	D759E2	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	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	6	D759E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	D759E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	D883E5	ReadFile

Analysis Process: chrome.exe PID: **6048**, Parent PID: **1840**

General

Target ID:	13
Start time:	08:47:20
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 https://traffmen.ru/wb?keyword=eicar%20pdf%20test%20file
Imagebase:	0x7ff683680000
File size:	2851656 bytes

MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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	7FF6836DA143	RegSetValueExW

Analysis Process: chrome.exe PID: **4280**, Parent PID: **6048**

General

Target ID:	14
Start time:	08:47:21
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1852 --field-trial-handle=1784,i,17276974344343449179,18398132625013484821,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	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

Disassembly

No disassembly