



ID: 753412
Sample Name: Get BTC 5763.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 19:23:56
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Get BTC 5763.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
Process Tree 4
Malware Configuration 4
Yara Signatures 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 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 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 12
World Map of Contacted IPs 12
Public IPs 12
Private 13
General Information 13
Warnings 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0 14
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0 15
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0 16
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0 17
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0 18
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0 18
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0 18
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0 19
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0 20
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0 21
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 22

Copyright Joe Security LLC 2022

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 22
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0 23
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy) 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF47a455.TMP (copy) 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy) 27
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF4716e9.TMP (copy) 27
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links 27
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-221125032456Z-209.bmp 28
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages 28
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal 28
C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store 28
C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei 29
Static File Info 29
General 29
File Icon 29
Static PDF Info 30
General 30
Keywords Statistics 30
Image Streams 30
Network Behavior 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: AcroRd32.exePID: 5312, Parent PID: 3452 31
General 31
File Activities 31
Registry Activities 31
Analysis Process: RdrCEF.exePID: 5328, Parent PID: 5312 31
General 31
File Activities 32
File Read 32
Analysis Process: chrome.exePID: 6844, Parent PID: 5312 37
General 37
File Activities 37
Registry Activities 37
Key Value Modified 37
Analysis Process: chrome.exePID: 7020, Parent PID: 6844 37
General 37
File Activities 38
Analysis Process: chrome.exePID: 2244, Parent PID: 6844 38
General 38
Analysis Process: chrome.exePID: 3600, Parent PID: 6844 38
General 38
File Activities 38
Registry Activities 39
Disassembly 39

Copyright Joe Security LLC 2022

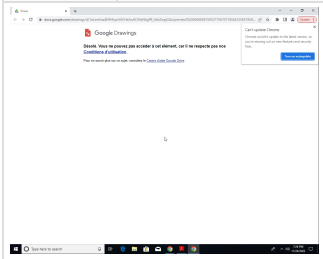
Windows Analysis Report

Get BTC 5763.pdf

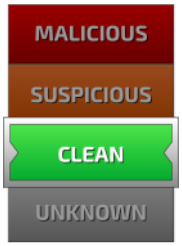
Overview

General Information

Sample Name:	Get BTC 5763.pdf
Analysis ID:	753412
MD5:	5cdfdba4f3219d8..
SHA1:	f2e1cbcd97d59a…
SHA256:	ff6af650ee8ef58…
Infos:	



Detection

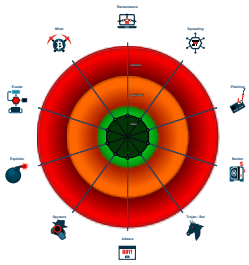


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Some HTTP requests failed (404). It is likely that the sample will exhibit less behavior.

Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 5312 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Get BTC 5763.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 5328 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 6844 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://docs.google.com/drawings/d/1wLersYca4EHHhywY6CHe2wACV0xN6gPB_XsbZwpjGQc/preview?0434006604750527756707105652256518581873 31 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 7020 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1976 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 2244 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5104 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
    - chrome.exe (PID: 3600 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6380 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

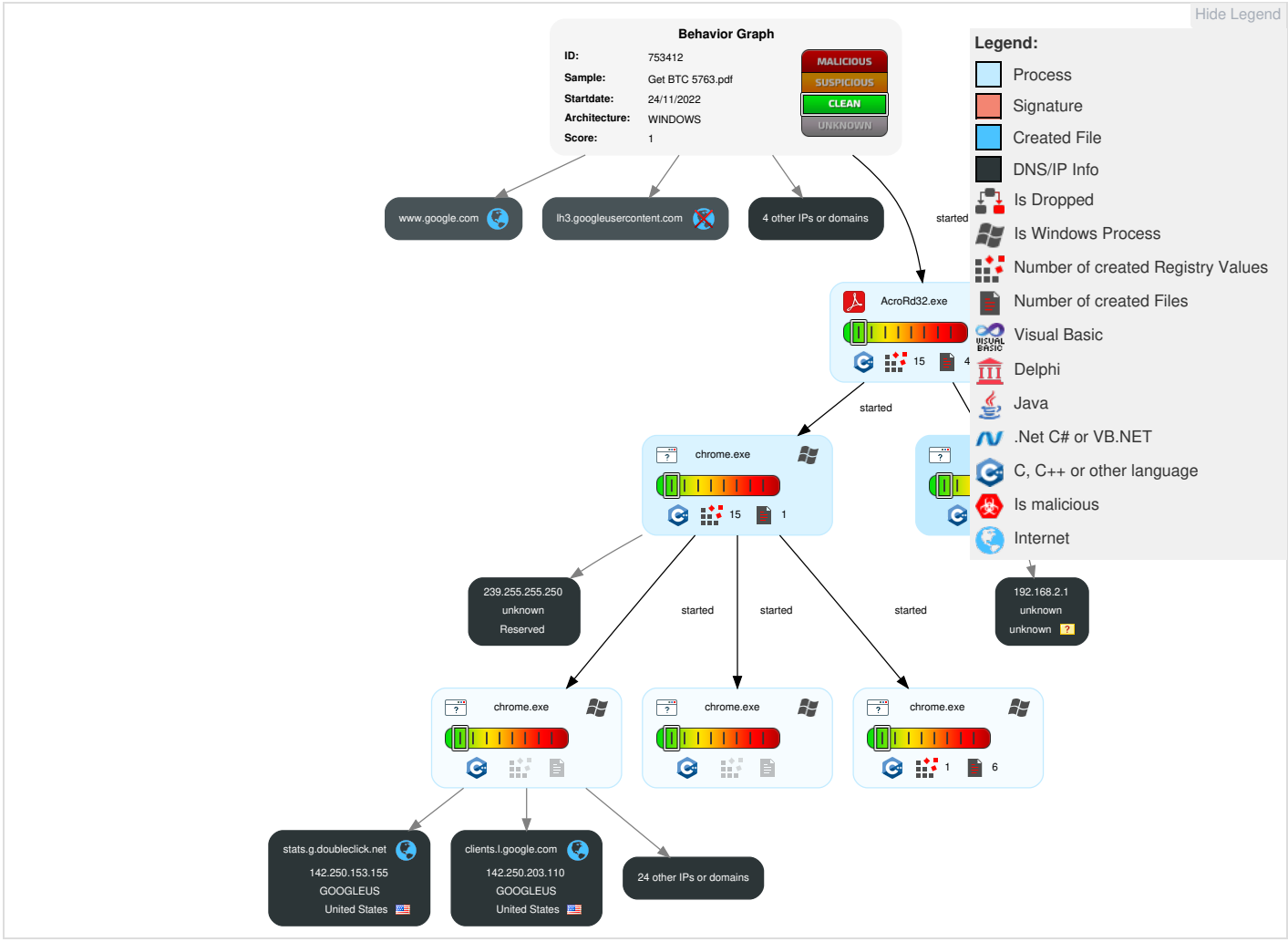
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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

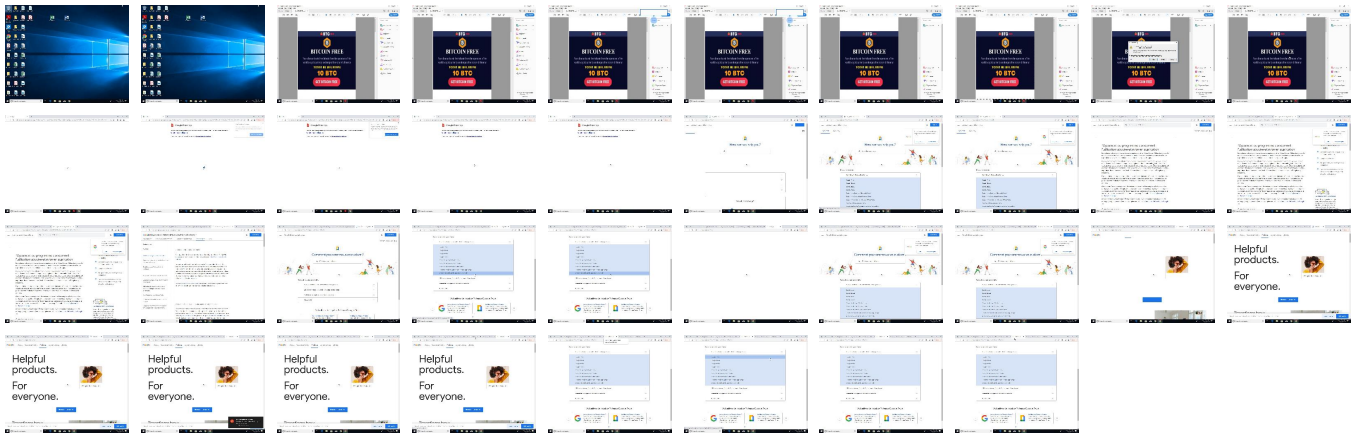
Behavior Graph

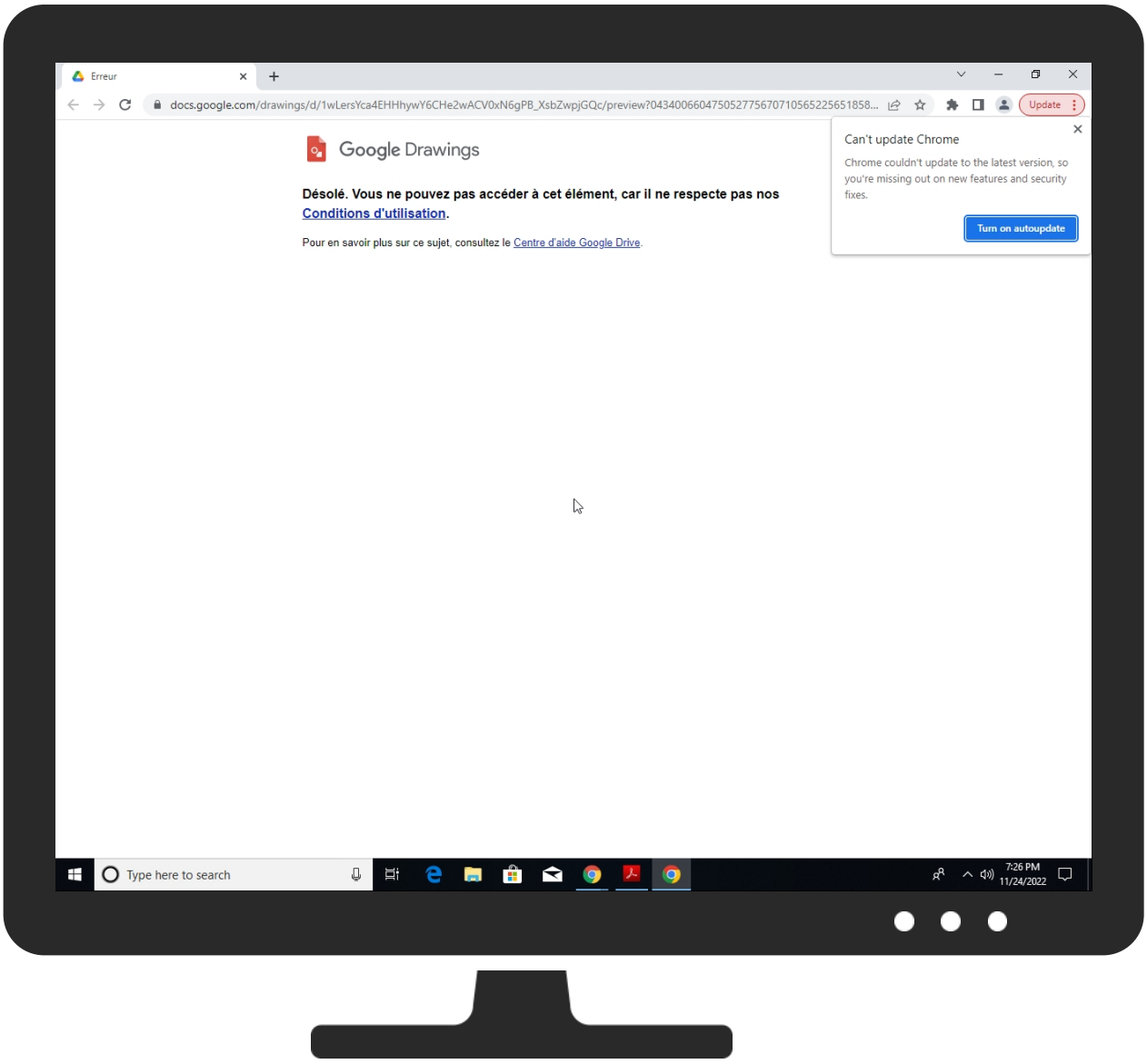


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
about.google	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://about.google/assets-products/img/glue-icons.svg	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/assets-products/img/glue-google-color-logo.svg	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://about.google/assets-products/img/glue-google-solid-logo.svg	0%	URL Reputation	safe	
http://https://about.google/products/?tab=uh	0%	Virustotal		Browse
http://https://about.google/intl/en/products?tab=uh	0%	Virustotal		Browse
http://https://about.google/assets-products/js/index.min.js?cache=15c2cfb	0%	Avira URL Cloud	safe	
http://https://about.google/intl/en/products?tab=uh	0%	Avira URL Cloud	safe	
http://https://about.google/assets-products/js/index.min.js?cache=15c2cfb	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scone-pa.clients6.google.com	142.250.203.106	true	false		high
docs.google.com	142.250.203.110	true	false		high
google.com	142.250.203.110	true	false		high
accounts.google.com	172.217.168.45	true	false		high
plus.l.google.com	172.217.168.14	true	false		high
i.ytimg.com	172.217.168.22	true	false		high
support.google.com	172.217.168.14	true	false		high
policies.google.com	216.58.215.238	true	false		high
static.doubleclick.net	216.58.215.230	true	false		high
stats.g.doubleclick.net	142.250.153.155	true	false		high
about.google	216.239.32.29	true	false	• 0%, Virustotal, Browse	unknown
youtube-ui.l.google.com	172.217.168.78	true	false		high
play.google.com	172.217.168.78	true	false		high
www3.l.google.com	172.217.168.14	true	false		high
googleads.g.doubleclick.net	142.250.203.98	true	false		high
www.google.fr	172.217.168.3	true	false		high
photos-ugc.l.googleusercontent.com	142.250.203.97	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.1	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
ogs.google.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://apis.google.com/js/googleapis.proxy.js?onload=startup	false		high
http://https://apis.google.com/js/client.js	false		high
http://https://about.google/products/?tab=uh	false	• 0%, Virustotal, Browse	unknown
http://https://lh3.googleusercontent.com/dMQ1Q4xlLrl3-KsZvX_9v56emij4OkRxzapLM7RSuZVd7PgqfjPxKR4KY8hVHYXqP2ZkS-_ZueXb9ywW66H2oCyTgIApr1ELCy3woOAviTgFP6uyAd0=h120	false		high
http://https://lh3.googleusercontent.com/vnSr97Bu2sI2_h334BHmEn1zTPrtv0hM9MLn3YxkN6JVzmir_VH62GiPIKfwtPBTOQ8xH0XNI40xfPAYbwbJEU-1jG09ovlU0f4S1Q=h120	false		high
http://https://lh3.googleusercontent.com/NksFVpnLFiAE4YKEh9n84ebvfznogwh0AyAUDpmpLqpBP7h791LS9RcIzWpE8XfsiR0NJiHomxV8FyVO2ccMF2VzB_L3omeUWuHu9d3LGJ4Ww6JKviev	false		high
http://https://lh3.googleusercontent.com/tUfd9tmqYw7QFa0Nnpde9SawF7tIAhwDw_ZM5YwuG0FmBTzjStOVQu1In41aEdg0FoXcXYEVk4L_FQDbPrXsJy-sg1BMEkU14M89=h120	false		high
http://https://lh3.googleusercontent.com/VdXRrd_xoiTD2oe-7FBLg5HOxC0evZYSk9glkZ9etAT5LNvCfL4tPySadjV9l32Y73wAauBLo6HCv4yTX7G9SYE8NG5-LFwNVBpfZw=h120	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/yfNHOlqQb-_BbTsGZle4fmncMyM2kTjYQzub_Hucf27LCQPNwJiqiOMr39an6X_yB3gCKVExXGgtYm1morm8jkXY53W8h75Z0nUepg=h120	false		high
http://https://policies.google.com/technologies/cookies	false		high
http://https://lh3.googleusercontent.com/z3dgQsXgGqfadzIUmpGI_ppolUy7H6fgqIbtW_qzLXcBww0nOby8TEE3e_fW84Qa7zeAwe339f5VLkqRD6jk7Z9sEaVh5Y_yaPG9nw=h120	false		high
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://www.google.com/gen_204?use_corp=on&atyp=i&zx=1669346820763&ogsr=1&ei=c7d_Y5iLGIbcavL3ssAB&ct=7&cad=i&id=19022645&loc=undefined&prid=117&ogd=fr&ogprm=up&ap=1&vis=1	false		high
http://https://about.google/assets-products/js/index.min.js?cache=15c2cfb	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/kQDv-46ToDkqXJ2DIlr7hKXKalQvL0NJy4oGIhNlUkxX95btXayCKNoZuaY_KT-6U8-Iz35FlDZXRd1U3bNFo99a3k0-vwIIbtElStTKYwD_UxNkjA	false		high
http://https://lh3.googleusercontent.com/Pk8YenR3VOTvN9iNHAGWp3pWYZiaYMXXWUkfAjt_LMrf222t9zn815V-GfMRJ1Hjgq7l2k1KiQmxCw5d687WTfIPgwjVfGvoHaSwRDI=h120	false		high
http://https://lh3.googleusercontent.com/C_Ty0aIlJNrRQz5pNFmgA1rsRnhZDj67eVCCHXoJFFot0FQEZydARPRKbBADyHQoA0_Dj6gLITCshiJq6C-H-QM_U2mJwJZVLOQPnwvCL2RerGMEhw0	false		high
http://https://www.google.com/images/branding/googlelogo/1x/googlelogo_color_74x24dp.png	false		high
http://https://support.google.com/docs/	false		high
http://https://lh3.googleusercontent.com/Q4UDu0hKQgAyUzO0RpJTpTKc2DyaZbU-K96JCJjqKd9_ABetMMpS6LxO6Y7Ypm2CVhCro4n4n9PTF97SlwrSjmJFaHdV-_yDr8MpX1M=h120	false		high
http://https://support.google.com/docs/#topic=1382883	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.lb.en.geaHZXF2-fw.O/m=client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo9yYF5eCIYPx4UH9gpJptM2Q_GGxQ/cb=gapi.loaded_0?le=scs	false		high
http://https://lh3.googleusercontent.com/WdC-o7ZcZL5WALPSmfUC8H4oYhlhqm1DV45CtHqV06DTRR0rE_P9JXi-J2KXLd9CTyHt_t3ehUm1o_AMltgfAGbvQDku8jsZt0kBSA=h120	false		high
http://https://lh3.googleusercontent.com/gi7EU_u6IiuIRSxunfy5LLqsEJrC08L12aufZc3rP_w8hD8ouiVW89vfe7pTQrSsLXQYyQvnlhBfarK9Ul33ccQOSqKgK3i6iyArwg=h120	false		high
http://https://www.youtube.com/embed/by-kTJ0DOLc?rel=0&vq=hd720&start=0&cc_load_policy=1&playsinline=1&origin=https%3A%2F%2Fabout.google&enablejsapi=1&widgetid=1	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=58f7292c86cc73e0&cce=1&dc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=fr	false		high
http://https://lh3.googleusercontent.com/RwVe2Cm1EjeDmYhdTzr179G0ovq_PCxgPzQ92PO-YxTBEFTHWh0L6Ev8FFDWRgRGrE81vwn95tyg9Ey189OO4kllhhpLAMIsGFZ-UKA=h120	false		high
http://https://about.google/assets-products/img/glue-icons.svg	false	• URL Reputation: safe	unknown
http://https://lh3.googleusercontent.com/9NuRdiRepVl3n1txfg7Ky2wWzB3DvXkWABXeFMSn2tzDYYkv8T_RMA9R17fWi0ziUDIDTVJx0JruCzOev37c4dkK9Wrgkeyam3pM8ll=h120	false		high
http://https://about.google/products/?tab=uh	false	• 0%, Virustotal, Browse	unknown
http://https://lh3.googleusercontent.com/oJtxC9wrYYcStJ4Ds2ylblE6GyJtbi_HWy01cp88xJGkrELh-SZ6N-kdrMmRglHFy7gsFWUNbG0Jth92P8HOVJkYyMMo76yMJ2vS=h120	false		high
http://https://lh3.googleusercontent.com/6nGdwtbmSCuuGF5fSCqvv0f-GOsp927ZXRFxC1NNEqlH-EwAGEqlHXN2rcarUTB7C8Tj8shbcg-9z-CO4XJGTVSaLbT5FPsq0rKET0ZlfWNsj9_f424=h120	false		high
http://https://lh3.googleusercontent.com/XfxlbB7lmi28_w277XeVC0u8Yngn8e1bQxhd6YK2snOdqt_uiwripgSEl5VNxgS2cJP2kf0dHv6LfSq8AG6YeJf9cpu1BE1kP36R=h120	false		high
http://https://lh3.googleusercontent.com/moWtYpo1G3n-1QfF5rNSy7n2IIQs785-H9DStefngR0kWMsmnPkzMu-SKH3eUxHVddekMttIA5olrn_wo3p50z04NyRZYPHYBc2cxvE=h120	false		high
http://https://www.google.com/js/th/lHuB0_VOqqz_4d-9x0HERCa3wAKE3cD9YwMEv3f_Pb4.js	false		high
http://https://lh3.googleusercontent.com/2qz9gwasYkOhPEumfqd3_x8HiiRu6fIQR1d-1DRAV8qfkqmQx7Rygzohal7DXbB-urTun2B0thBnpY3BRfqXnJOm4b9QQFk3L4VK=h120	false		high
http://https://about.google/favicon.ico	false	• URL Reputation: safe	unknown
http://https://lh3.googleusercontent.com/Jqo0sXz5HJpnbEwCf5qwcWSbwXbKiivjx2e1WpRjAg3pAPaj2DiOHs42I1zwyhvtXdHwTuGYXQWkNMIYGGUnXT5fiSbnwIVB1WYhdg=h120	false		high
http://https://lh3.googleusercontent.com/Amr8tRBfd1Uk8zYm779hnSCwMzArp3LGD1LUhcgPdCOIk0UJczmdKLa42Apx-wzQdrUnsATBiFsyHT5pVit9Al6PwfVewM09FnlwAA=h120	false		high
http://https://lh3.googleusercontent.com/_M14NRTYPPQYgdKReeicOfwYJfHl-USHThCxb3buQ8dKJ_XBIjR1InzdLQ3vjYrDVdOn79de6u_JkxB0D44hBrZ88olRx1fU8QIe7Cq_VzxUWalNeQ=w1440-l80-sg-rj-c0xffffff	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/6xlGJ-dkwosfUisVYzRKNE1Wcr5QDDfRfZ4bXktF-Nn0J0ucHd_JI1wjXTls7lt5mvJvvcvtrNc0MESF98dAx6ivasEsZNxoaUZU-Q=h120	false		high
http://https://lh3.googleusercontent.com/hHWA5otDm9mYUJdAqTjo7wBWj8euY-SdEhCffO7oQzG3zpzxm-YExt1VDB8X6_5gchW_Ye3bfhOJXyOWgcUr94GtgqltKP4IxiH02O-Xzw5A1IHsxiw=h120	false		high
http://https://lh3.googleusercontent.com/vNgpLTvnDUr6-QM8s4OuuESGDXs_brbGoPR-7vfwdxQI7M4MVFV0CC_Hil4qRDSp4P66ik85fdv09jKn89kDAJVknIbd6wkl0zGQJQ=h120	false		high
http://https://lh3.googleusercontent.com/ZBGpVzlWvxSjrPnKofe-W4em3dHK1zGFAcxdZ2cY4oOBeQcQZTgJYLvlE_sfqx22VqwOgiW00kMdwwsfIkIgKUWO721GvyTjmtK3kg=h120	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j98&tid=UA-69658807-1&cid=1315723257.1669346836&jid=2003982216&gjid=1946312965&_gid=1010309938.1669346836&_u=YEBAAAAAAAAAACgBY~&z=810466406	false		high
http://https://lh3.googleusercontent.com/p2EiNuo4FQe3s8dhYgEiejBxjryT3B46OTWNItLqiwF58V0T62GKHa7VrbOhI7BbnQOBvdkPFu-4YGG0Dg3b0moXWWSc_aB1hw67Kts=h120	false		high
http://https://lh3.googleusercontent.com/8v_oGMOj9bgohn50RgLhJ8XGZ2kIUdr0RG4zCkIYnfjK24ORS0WFaTWmnzxXzagUg2fwAmDy1W_Y4oTtlacT2dhQzAqOy5H9Vg23Rq1oVnhUGtOynjY	false		high
http://https://lh3.googleusercontent.com/R7Wr9OkT5zk4gY2F3-tLiMwhFaMfO_hCU5LpTxztUaTOi8kU7_0QUIvOTlhHLyMol8kvHhVvdWUtjmAZ6cqiwGhwZzdg0fvc-UXtojU=h120	false		high
http://https://lh3.googleusercontent.com/EUHFjMpMj-UPEu6jfEEP8TPV7QxQerc-n_qulHi3MFPnK_63i5ldHApJsutq7wXqNmN9V2rmk9swsQ9l0eddAv77HlO4uv6gKt8haNAMqjiM9pqNu9w	false		high
http://https://lh3.googleusercontent.com/5CsRqfMEP1Rv-PPv9G4962lyEuvb4roSLJHJQWPbmCa51AmvynfoGfoKsKiS87QhX07xQMZAeLp8qoSy7CjVZkXJ1WapQiJkroCeJw=h120	false		high
http://https://www.google.fr/intl/en/about/products?tab=uh	false		high
http://https://about.google/assets-products/img/glue-google-color-logo.svg	false	• URL Reputation: safe	unknown
http://https://lh3.googleusercontent.com/nDCFKerWuvJvG26AZOPsWYFPiw3MRFDYqVJcHzQzK6AgY96TXH50bpQ1IE__BdBxxcXm8ZTaQ6OuJ4pbYF1c-ugOTfOmjhffJXEvJQ=h120	false		high
http://https://lh3.googleusercontent.com/KSsffSSbOYj7xYrs-olsAHgyy2qkvndHeVvWUO2vv08mJxHUZAofPfenvHMAxHI5a1XCXLDqR-hT6gGx2uze2sbvDnKCPOL0APKiOA=h120	false		high
http://https://lh3.googleusercontent.com/j0mZxqPUZ28oopliF6vSV0okYdXUPZH__5C5_4zuI1eNoLd-JFgAFWu4oPFvxTguMH_Iihh76znHXocGuTuDGVtlaryO0cLZSNPVMA=h120	false		high
http://https://support.google.com/docs/answer/148505?visit_id=638049111896766255-3444834951&hl=fr&rd=1	false		high
http://https://www.youtube.com/s/player/4eb6b35d/player_ias.vflset/en_US/base.js	false		high
http://https://lh3.googleusercontent.com/aD5GNhlaU2d70gmSy5ioL1dMSUZN9cHDWPLkIBLhCsJ-BgcGUm-PD6o8XExZcx1i2iZV6PH0P8v3ceg0x7Tzd_OZ5FV0nXs5mX15sgA=h120	false		high
http://https://lh3.googleusercontent.com/tC78k3bL_DjdIByD4HSnnblCZF0nlR599IWYDDghEJDn7dwg-tuOIXGVR1TwxePI063JTgu9NvrsvRutrqHOfR5AAWduD51R8zuswV8=h120	false		high
http://https://lh3.googleusercontent.com/mjVS_Izc6fGAvuaT0v--gb2so5mZvAbI5EUMUB41cWB7tpy81trBCR8rIlj8NoKgPzDWGN-Hs97NlW0T9W57YJ5z9A8QQWwXUYa_Zg=h120	false		high
http://https://about.google/intl/en/products?tab=uh	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/9KKBHHVmyet6xnci7yplPWQPpv2H7EvPQFmvy_mTShsOMPqbiMpLQHdHAsImNBL39fTnONH302_YC8LDgE2Am8Q81uXccg302NZpsgTjwtdBbNMDNsg=w1440-l80-sg-rp	false		high
http://https://lh3.googleusercontent.com/cS5nvr3r6Q16NoV6IuJLaauz7HNNRPnuHtsHleZ8du594H4EeiOjeNxV-Nq_w-qRA87TUedLQjTmqCG5s6jNZRp29n571FDWyditF-WJhfhQTY_73OM	false		high
http://https://www.youtube.com/generate_204?cpIoTA	false		high
http://https://lh3.googleusercontent.com/g9bgL-O8I-FpF6EaoeL2a5wK8NmB3oHkfl3IVzdYQQRnv69ar4rh_f3z1Taewvmlmtbl5Z-FBQfwNJ101pTON_-qnnoB8xlfONWV_XI=h120	false		high
http://https://lh3.googleusercontent.com/_M14NRTYPPQYgdKReeicOfwYJfHI-USHThCxb3buQ8dKJ_XBIjR1InzdLQ3vjYrDVdOn79de6u_JkxB0D44hBrZ88olRx1fU8QIe7Cq_VzxUWalNeQ=w600-l80-sg-rj-c0xffffff	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=723e1a40d4cc6173&cce=1&dc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=en	false		high
http://https://lh3.googleusercontent.com/VIEuHzynryKZDPWc0-4WTv2du70T2qwaWyMVLXS2ORs-oZ535SkKE1zNRPRikEjdLw=w64	false		high
http://https://lh3.googleusercontent.com/aMTzdOYbB8kBrLq-k5PesENOhnr-7qtytONnM1GOl-drEs9jvyhYJDNaN9-n_Am7rZLxE-uQnNKC0tW6w7Ea9QX5ZsgMy5mn1ll33QY=h120	false		high

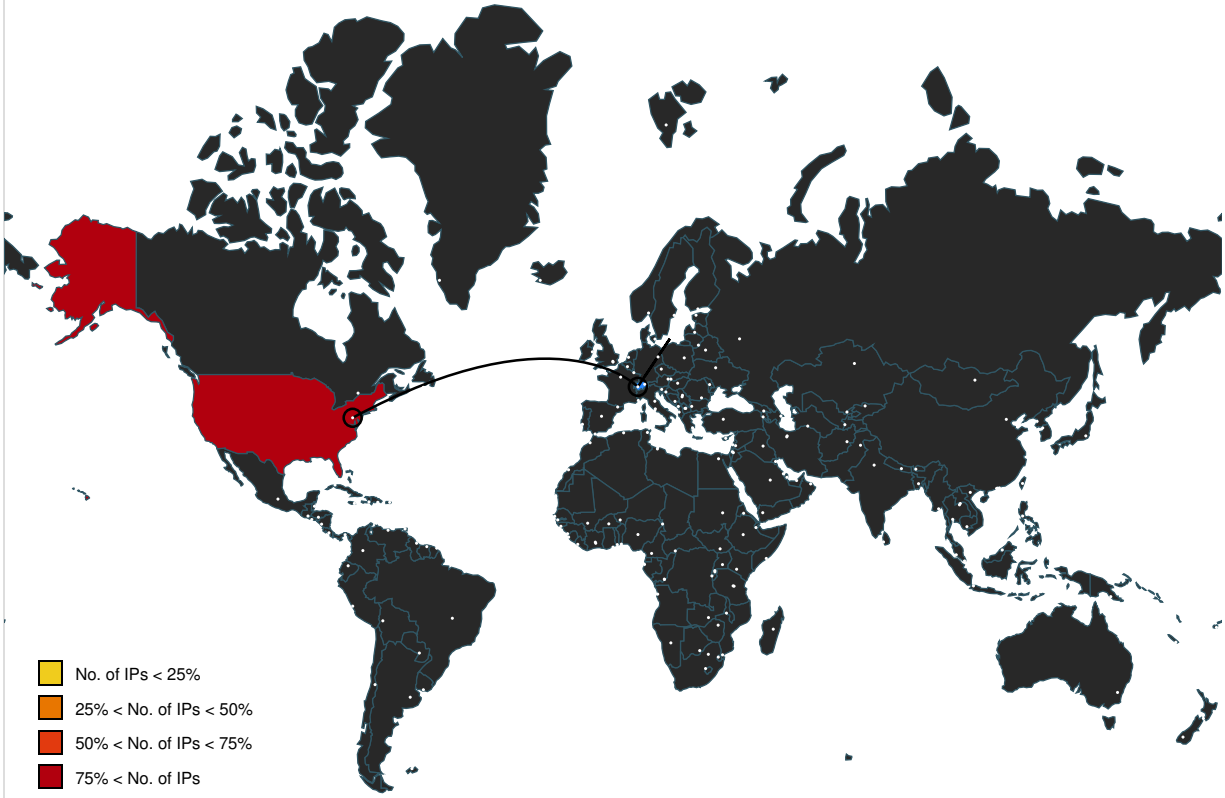
Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/UqqZocZvjGksiGtIRkKb5NsuhpQkMLt3A85IMQ81Pms9tSZ3lLpymbAeinPIe5qUJRdmOKqL9InBBVsh6_gK-1QcNGppeUa7owoKgqo=h120	false		high
http://https://lh3.googleusercontent.com/Ucxl6g9AKLX3XmK7an_99LzivIJsXn5cvQdIMM_g4nNFZdULnGa4TH45WVIFu3vKd_c41R28NdjDzCEWgAwb5wjONbIPR4agLFUO1w=h120	false		high
http://https://about.google/assets-products/img/glue-google-solid-logo.svg	false	• URL Reputation: safe	unknown
http://https://support.google.com/docs	false		high
http://https://support.google.com/apis/caseslist?hl=en&key=support-content&request_source=1&mendel_ids=10800112%2C10800561%2C10800672%2C10800686%2C10800695%2C10800700%2C10800707%2C10800738%2C10800761%2C10800763%2C10800848%2C10800880%2C10800922%2C10800950%2C10800957%2C10800968%2C10801032%2C10801150%2C10801288%2C10801345%2C10801376%2C10801510%2C10801539%2C10801599%2C10801601%2C10801704%2C10801736%2C10801757%2C10802254&authuser=0&v=1&helpcenter=docs	false		high
http://https://lh3.googleusercontent.com/xDakliA_6hjirY-kSiTQFdrVRcRxYDMDdVWFOQtp97xidbk-At7EwGfV7YQqzSgbpfmpBw6etaT20SIzenYIyyretLrgN1PbR7_OTos=h120	false		high
http://https://lh3.googleusercontent.com/_RS8nTX8HLPW-dDr374dEdQTaYn-7LI8HVVk0INaAmk7t8MYZKDssvGnep-GwPR94LJPxqq6UDnbm4tonioTpkl4Kqr6-k-670teZA=h120	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://play.google.com/log?format=json&hasfast=true&authuser=0	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=58f7292c86cc73e0&cce=1&dc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=fr	false		high
http://https://lh3.googleusercontent.com/Y1i12gHz-cP0Ir3LztFSUMijuVGSe9qetVu98aQNchjhxw9byxecnFAFfhxGFyd79tgcGpJrHjJ8S_AQmFnBqtxxDAjh81bxUMe1=h120	false		high
http://https://lh3.googleusercontent.com/PP8KjNgc-EqOm5a6yZ1w6mqbFzoyzLfCZcjhmRvWn6imgVjCiPj9j_MKz6jJuggsroU3293OtM1dIFgqushuz-Wrq-0-_z4AnqLkgw=h120	false		high
http://https://lh3.googleusercontent.com/3Vr1H8EL1F2w2g35zmQkqnbbqfM8e28GxuaTXxkovnYV7ldiiKJVqlnFRlIOfurcfZ7XDVJlJ5ET51yXw8_fJkXIzakq30XzVzI6Og=h120	false		high
http://https://www.youtube.com/s/player/4eb6b35d/www-embed-player.vflset/www-embed-player.js	false		high
http://https://lh3.googleusercontent.com/hDmpjNjn66Z7hyYvAee18jZfIss2NCbUss41HLkWh3s08AxT6prRWd6iv9CnofK6cXXS42OzQ_0J6UcM44xV1ouv2Tq53nCjI28DDorFDHS4RQrlCw=h120	false		high
http://https://play.google.com/log?hasfast=true&authuser=0&format=json	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j98&tid=UA-28138501-1&cid=498852938.1669346809&jid=1963438392&gjid=16504524&_gid=2027744316.1669346809&_u=YEBAAEAAAAAAACgDI~&z=431188696	false		high
http://https://lh3.googleusercontent.com/kM_wE3H68SPU_s7ClGAbOFWwY6UN82x0QF1LFEDlKvWVK82KEzX9b-UQfPorWw9iML0LkzZy3KEJRyj-BPL9MhMfq9kU4qHtPbADuS0=h120	false		high
http://https://lh3.googleusercontent.com/SLlieQVJNLw2RKmgpg3mMQKeaM5lTZWbOoF_dV_syPle9U7KBs-1PB--OdorbPJYFVRy5178CRGUeITtRpSRyoMyPFGjxlerox1nm5k=h120	false		high
http://https://lh3.googleusercontent.com/jtplKgVk_Y2rVLKvBy4ARGhnhOqy0R1FOoBalaDDmWZ1ZmfM3KzMSLJYgWGYkKgozsBX0c_1G54MKuLeH5izmOKTfaFrJDIsIOqvlOt1p3unGhj9g0Q	false		high
http://https://lh3.googleusercontent.com/XuX--BV0zkkLgxF4L5fJ0A1zg1yqjZ5TRyjEyaKMg873pOoy04PFwpUeUNw9kDpeocu5Dq7LRpOU3tkXF-yg9bgjyBvHjRJ2Dl91=h120	false		high
http://https://lh3.googleusercontent.com/uPpZapQO32gCKWztePKdTRzpg7rCr4_40vlgIAslU9JyF135ZdGvC33DbzA2mdmOTNK6qgbu7xWfKkR9rfJUwaK20saGLsFW9yw014GdOKBVEN9zow=h120	false		high
http://https://lh3.googleusercontent.com/oLcLMz42MUjK9Iv4M4YSOfBIHcxUh9dck3PN8kT8FR_z9_mUlWzyf4JHqPavPsKHJ7FR2rlGZf51vgEv1k5i0QQai4_J0ffYkIFbaJA=h120	false		high
http://https://lh3.googleusercontent.com/OSQqNbZm7pYKt3P0rSr0WN51Qh3NCo8BSJ37es08pTyoHjH9IMIEdw31GxuCp_qXFpqvJwXqeLRbZdrOvv-kFB-rTaHHfQj0_fDE=h120	false		high
http://https://www.google.com/gen_204?use_corp=on&atyp=i&zx=1669346797757&ogsr=1&ei=XLd_Y8elGOWIzgPdw4CABQ&ct=7&cad=i&id=19022645&loc=undefined&prid=117&ogd=fr&ogprm=up&ap=1&vis=1	false		high
http://https://lh3.googleusercontent.com/vWJNEFxN3WY5PYAYjwZ9ycEXMCCiB8EbcFXZxfSv5xkKLw67C2J5qXJTBL9KSPldWmLpVMnucrsDBmPlrf9tMiEJpYNZNcTw_ymlxgc=h120	false		high
http://https://lh3.googleusercontent.com/TlJWqgqxCA0it6tZ-n8OCkn-Om5nIEy19gQd-5UXCSpECGKSBNksOSSRa-fU6-DTcvHwnqzlnKc4A5k882qcSW15NTY2PHyNJz7b=h120	false		high
http://https://lh3.googleusercontent.com/p5IVJAicHuI6Ra6jtpYimNt53JZQNCcN06a-Q4fUaNVFo3cjVisZMY_UwBTg5fv2MUkrbwbfTw70N9-bbTfejp9S8rUNadIhWiqh=h120	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/apis/prefinsert?v=0&helpcenter=docs&hl=fr&key=support-content&request_source=1&service_configuration=&mendel_ids=10800112,10800561,10800621,10800672,10800686,10800695,10800700,10800707,10800738,10800761,10800763,10800848,10800922,10800950,10800957,10800968,10801032,10801150,10801288,10801345,10801376,10801510,10801539,10801599,10801601,10801704,10801736,10801757	false		high
http://https://lh3.googleusercontent.com/8bC8ZC9RQ_cJj5lSa8LjCfRClGeSyp4SkN72C0tMSUIqGPVjEpHeUDfAScLNKy82MiXWLBlkpMl4FhJGrGRDhzHxOoXq5v-QSt-rvg=h120	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://docs.google.com/drawings/d/1wLersYca4EHHhywY6CHe2wACV0xN6gPB_XsbZwpjGQc/preview?043400660475	Get BTC 5763.pdf	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	policies.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	docs.google.com	United States		15169	GOOGLEUS	false
216.58.215.230	static.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.3	www.google.fr	United States		15169	GOOGLEUS	false
172.217.168.22	i.ytimg.com	United States		15169	GOOGLEUS	false
142.250.203.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
172.217.168.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.78	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.250.153.155	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.14	plus.l.google.com	United States		15169	GOOGLEUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	?	unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753412
Start date and time:	2022-11-24 19:23:56 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Get BTC 5763.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winPDF@45/53@27/17
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 • Browse: https://support.google.com/docs/ • Browse: https://support.google.com/drive/bin/answer.py?hl=fr&answer=148505 • Browse: https://policies.google.com/technologies/cookies • Browse: https://support.google.com/docs/#hcfe-content • Browse: https://support.google.com/docs • Browse: https://www.google.fr/intl/en/about/products?tab=uh

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 2.21.22.179, 2.21.22.155, 23.54.113.182, 172.217.168.67, 34.104.35.123, 142.250.203.106, 172.217.168.35, 172.217.168.46, 142.250.203.104, 172.217.168.10, 172.217.168.42, 172.217.168.74, 216.58.215.234, 216.239.34.36, 216.239.32.36, 172.217.168.80, 142.250.203.112, 216.58.215.240, 172.217.168.16, 172.217.168.48
- Excluded domains from analysis (whitelisted): www.bing.com, fonts.googleapis.com, ssl.gstatic.com, fs.microsoft.com, content-autofill.googleapis.com, storage.googleapis.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, fonts.gstatic.com, ajax.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, jnn-pa.googleapis.com, acroipm2.adobe.com, region1.google-analytics.com, ssl.adobe.com.edgekey.net, ocsp.digicert.com, armmf.adobe.com, edgedl.me.gvt1.com, www.googletagmanager.com, a122.dscd.akamai.net, update.googleapis.com, www.gstatic.com, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Copyright Joe Security LLC 2022

Simulations

Behavior and APIs

Time	Type	Description
19:24:55	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):	5.6280696958196685
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVa8sTqkvRktQ1/iTFJrqzOJkvP5m1:men9YOFLvEWdM9QGtwi7Z+P41
MD5:	CDD5EDA9DDA5E21D5FEA9CCAEAA8A27E
SHA1:	D7A4EB1D314408252BC0FBB9BA5D42818AC81F51
SHA-256:	D301E9283F5339B657ABC7C72289C58F69D23DE84A30B752550590E25F84600E
SHA-512:	A43ACF3124702D0FC2F089C9FE9EF5BC7B1F45D99B41851C7B5119CBC166F6A6B437F0E131D05D8D66E0EFDFA010E8203A76AA8214B7DAA3DE45546E4A0CBC 9D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .(9.Z.L/....."#.D$..g...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):	5.500209936701792

Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVlXcmYqkvRkt5O9/M98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEk6qjt5A/Q8Be7Ywcr1
MD5:	34544BB7E29F484912B249DEACAA8D74
SHA1:	1B4572D3F43C53CCA4BB29513781B14F19F79FDA
SHA-256:	7A7903F9F03F80ECED9C77E1BFC07D4A12252777AC0EE1140074A778B8AB27FE
SHA-512:	B9A22FF243179D4DA16086B06EEA6545F5D99F0A74BA783C0118202762CC063E3801BE5B6415509B88880BEE19061FBD906B9BB5AD46FC832A3CE4459EB13384
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..[sZ.L/....."#.D.y.f...A.A..Eo.....KSk.....1.x.'.vl..*|Z..o...+.4....0..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.568090353503992
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhusuXtC4t/RlUoSjGY1:DyeRVFAFjVFAF4Wk4tZlUo6
MD5:	FD2B972B7C58D7E3C9EF28433002D5B6
SHA1:	F7A4717A0315E64B67EAED6E77B6A6F7269CEF35
SHA-256:	03F5F137F6656C31044E135163C3D89F1A7EDF1ABA68D92EF046CF6D1BD0A82C
SHA-512:	2E563308C4B313708AFD1826C2FB5ABCBABE890AAA3C35B3629A9386BFD1F12E6578EBEFBAB014F31A9E580BFD338E0F08E206BC9736503E00742BD91DBBFA8E
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 .?<.Z.L/....."#.D...g...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):	5.6406882967911995
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsY85t7uiWulHyA1:IbRkiDIljWus
MD5:	335327B85344B3A9B4572A6AAF3BB531
SHA1:	E43E6392F25469A44DBC7892687029C6EB2BA4C3
SHA-256:	518AF439AAEB1C1CEB5C2D1E504554CB486389CACFC62E175FAC1F115589831C
SHA-512:	025B513F8329B95D723E4901372E77727C65524CCEE171CC2F43D62D6AFF1968ED8A74960B660C81F386AA9A5F66C06521A920FB65F0EA0175109D2CD24CD43E
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 ..fEZ.L/....."#.D...e...A.A..Eo.....8 P..a...R..Y. ...7.@..2Dm{..A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.530726623968927
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuK0th/UVyh9PT41:pyixRu7fUV41T
MD5:	DDF9F7B0B601B6BD33C001F66EFD76BB
SHA1:	8928BFB62F22EAB7217765A63BF8E19238EDC39A
SHA-256:	04F9DE270AECD31422B32ACF1473ECFF80A830916D6554C0C2CFB9111DDD2B09
SHA-512:	B431D770777595531E3EA9057FFB7755B07FFE9EF628961B89F8677853A7F6D8EE6EAA9722766189C3686E47A0DCECD1A7F9B4D0EF5A3E25413BE563B9FA0B64
Malicious:	false
Reputation:	low

Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..1.Z.L/....."#.D.>.g...A.A..Eo.....j9.....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):	5.627412314394968
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuVIa+u+S8qkvRktsHl/lxlYo2sZlj:mvYOFLvEWdhwjQ/K+SHjt8d3Zll6P41
MD5:	D52FEB6D47C57840BD452BA4E2596083
SHA1:	5856D03FF2A2EC00361F73EF955B2865D9C97127
SHA-256:	768E0D297ECF0BB8149E0F98C253BAF6B820960751530D4595B4D5360F002A7F
SHA-512:	74FA5AAB72F44C6F32A00B648A5A3FBA938DF6EAB3C98D576C6B6DC0FA6B5E29B2F2E100AC0704401CBDA7E9A819AC2AEA00B0E053CCD891259EA0A64FBD 3547
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..f.Z.L/....."#.D..f...A.A..Eo.....W|.....].>....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):	5.506977136681856
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVnFibdvRkt9djcyxMtv9EWm1:mJYOFLvEWdGQRQOdQSWQt9djD6g1
MD5:	BF0B013AEECCDF6EF4FEA51387ADB221
SHA1:	611756E5B966393DF8D6493210366BEC2DD108E1
SHA-256:	303E6344722B680D557D6C740F7DF768E2DA4EAAB542990E74B393DD156E001C
SHA-512:	CB412D5DBE9D0283919772396F7D7B42CA8641EF386DF5F3552E7F480000A552EFD8750212DCCC373F9DC51D3BC0ED4CD13C9377D524149A411346874875960
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..2.Z.L/....."#.D...g...A.A..Eo.....M..:.....c..y/L....|y.n..C/I.....X7-ne.A..Eo .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.494789859434273
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVGl2x9kvRktjE/llDQMWqg4nRb7om5m1:mOYOFLvECMLy2x9jtAlEuR/41
MD5:	DA6CD03C1A50AA15382F8DA9191DE068
SHA1:	EFBB2208C5183F243F38F8C28A6105EBA7AA5E78
SHA-256:	E97920437215A25365E5244CA252E6A16C899F358B648FD28F4B63F7CC835ADE
SHA-512:	A20C288DE2BAFC7EC921F6B34325BE1E873611274B7D6E3953A89638446223278DFC2094B2B3619F2F6889DE887B7F08CCA9550F45A2145ED2FF2D5C2D48FE7
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .!_sZ.L/....."#.D..f...A.A..Eo.....|.MQ.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.610164505950876
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAujaKxQtx/llSGm0bbsIDMGH41:XfRMhaEQn/llSVKsIZ

MD5:	1046358311D98536F6246B1F396B3D62
SHA1:	7CE2A85FE0C52A9297690C4BF6DF212A02782617
SHA-256:	FC939901482D318468EA19B131595BF3EBE3BBBB5F487B83399C05C86E42730F
SHA-512:	95089E28A65264AFA559D18630C8573EDBB93B974B8CD6EA59F351FF1F8CC4F66397EA14D99A3BC5E26845D84CCE385E13ED72BBC84F76F10E95828E70FA94D8
Malicious:	false
Preview:	0\r..m.....T.....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .,..Z.L/....."#.D[..e...A.A..Eo.....@|.....`.....^....L>..Xa./.....C.y.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.510221948149685
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuY/81txpby0zBUKSAA1:pRS1Ppb
MD5:	79DE457C6E678F45147159B1C8A70692
SHA1:	0500623E01A711C22CBE3B1F296F7A133FDD00F9
SHA-256:	5C478A0218B206687600DF55EEB71B3EE3C764516C7087CA82ADD2FDD4916065
SHA-512:	82E058EA30DAC41FC2CE59F95362A068B97101DB5A345DB14C16A0F9F29F233B5EAB3C42A17BEC577A899AC0077662E61A25D0917A285FC23C74459D6F4F9B01
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .{..Z.L/....."#.D.n.g...A.A..Eo.....{K.....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):	5.502787662355337
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvlKl8EAF9kvRkt2CZlcd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvQl8EAF9jtl4jUH
MD5:	1ACE9FAB9D78362B4B8E860F3294062C
SHA1:	84F354901C0462B92ECCD28A613835F0990BB671
SHA-256:	068C72BB5DF93EB27BF46971B4D7129B1F800A047C3329BDC5C9DBC6A5BA3450
SHA-512:	4CFB02CE069278BDD908982BB3DC2441A6024E1BAD83553082EEB5BF25F0ABE91986B10913959708878728A4510CE006CFD034CB635E3E791D11E30FFB34E305
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..\sZ.L/....."#.D..f...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):	5.534593380753642
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVLx0XuEGvRktdl5UPqf9tsDMaPV44m1:mkl9YOFLvEWsfOLx0ewtdQPqVyM+VY1
MD5:	1CEBB842A39C07A60DD552578D142EDA
SHA1:	25D93281E4A3BC81277334CEC90D54EF95F250F8
SHA-256:	333C36C645F649C1701B5791632E1807662A6DD488C6EDAED5A62172DDB17C8B
SHA-512:	CEDF8779BEAF4685E10215A381BED79FB5E5843FFE34B0214A7B3C6C44C04980BE227EBA34EA3A2F86B5CF0745E0E586BE8D5118AFBA80A5A6F91A289B57BD97
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .@..Z.L/....."#.D.2.f...A.A..Eo.....AJ.....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):	5.612310622279351
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFly2TaStVitwSeKaT9pr1:URVFAFjVFAFVuSetwSeKaTL
MD5:	05BDD545C69FC19A1A71678F914E5B40
SHA1:	C7153D77E285B59EE38ED99DE09326C18E935757
SHA-256:	C1886DAB62F35FB06CC38721880F787F98441C9DAE4C4EE38965A966CADDB993
SHA-512:	CAA0E929C83C6FBED4705212CF2CC40BB25D47C40E9B334100962D35D9D96A19252F995651E3A00E73B1BCA462142785D62EDE9F5AEC13C7E350600FC432962
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 .)3.Z.L/....."#.D.w.g...A.A..Eo.....^.. .....H...{...2../.k`..r4.C. .A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.521659103730579
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQ2OVt4Ut5GFCaa+41:NRMHdNo+Ut5Gda+
MD5:	057E58F08D9FC4A5B74B7FB0907B10FE
SHA1:	CA2B7DCDEC4CA3AD5D1D31211C4765DFD18ABFA2
SHA-256:	CB9AEFE9409FAFB9D72AE98407F468630180F0F5AEF38CE7DA44869BA8B085DE
SHA-512:	1BEEF3D1AB5090ABAF7EB319605635D5FF38F73E28E86D9C6A1F41DBE6A160D5BEE24CDD5A4D6127C2BEC65C3A03A33C53C06DFAA3132A7A07E1286DAE2E 88D6
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ....Z.L/....."#.D...e...A.A..Eo.....Mj z.....G.3D.....Q.g0...._.Q.....A..E o.....

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):	5.499466344320492
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvZuEXCiCo9vRktSJyrpYFm1:ms2VYOFLvEWdvBIEGdeXuzuaCowtH11
MD5:	12913CC15C597716C52B58A0C87E3F61
SHA1:	2111B71087C23D3218AA0920B22CEB82FD9B5A4C
SHA-256:	3509A762684BD5CD88A2BB8F8024CC0EB620AEC1B1BB33987DA433D5D44AEDC6
SHA-512:	A078BDA514BCD378599AF85390C6134F710C97C4D39B637401B782A99F11AB70CB4CC4E0BA0CA65505F61156CE8309AB37CBD010CC44511F704DE529E479454
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .<B.Z.L/....."#.D.g.g...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):	5.635533380100546
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQClQtE9xm7OhKlvA1:RbR16S6xmJ
MD5:	D6092189CA01C69E902DBB52D6DDB1C7
SHA1:	D1A34A67D16577FC0829D14947985594A69E711D
SHA-256:	E74696F3D6FC2E1F79A55A54376062F9CA84DD0C34371DC4128C2B2955928566
SHA-512:	49DEE8F94730786D326942E4881A600F0C2A762A5B26A83D55F35B284AC28F73DAF6C80BDF83659495E8C3DADBF13C3E8F9EB86CDE873C9F65B6F4610B0F3B0 9

Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..K.Z.L/....."#.D.W.f...A.A..Eo.....k.....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):	5.5621299694936335
Encrypted:	false
SSDEEP:	3:m+lx2gv8RzYOCGLvHkWBGKuKjXKX7KoQRA/KWEKPWFvqk3vRoHdvRkt6dF5YufMy:ms2gEYOFLvEWdGQRQVuVQQt6dFt1
MD5:	5C48F92B39E4BC8ADDA0123DF3DAEED8
SHA1:	C243AFAA6E466F6CCA97ED42205A31418474CBCE
SHA-256:	CCF1A2905B9A725D22CF6035822D16D9F949C76E499C0E37E62E092918E6BF44
SHA-512:	0143023156853FD4BA819AD8608DCDDE9DE7AD2EE65DD6EF568BFAB5ACC04D22982DAE25BAEE1FE9B90D54D9FB7CB993B2E632C8D5FA748F88B0EF47B2BB 7DC6
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ..A.Z.L/....."#.D...g...A.A..Eo.....i.....@..{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):	5.587111201021507
Encrypted:	false
SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuV/K3xGvRkt2gEnNWQ1SUm1:mzyEYOFLvEWdrlOQsYftlEt1S/1
MD5:	38AB05CE755CC062FA4454B77F5DEA8A
SHA1:	A693F011FDF7AE64195FAD421E70DA2B21C844CA
SHA-256:	1BF10601F7D5EFCF6C7E2747EE96ABC1C02FBAEB7DEC0C377FB01EEB3F70AF97
SHA-512:	14CA8F2F1BE34B30559F678F7801B26E7C262527EC91EF4335C640613AFAEE89678C82156116A6D6BED8B5DE77AAEA10B0CA74AACD500E18B86A21FE4BF874 EA
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...Z.L/....."#.D;..f...A.A..Eo.....T.....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):	5.523151903422637
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvFmNeVNQdvRktz3glwJNqww6U+5m1:mnYOFLvEWdhwyuaNentzQlwrqwK+41
MD5:	238D99CED58DC76C21E215E5377DF29F
SHA1:	16D0D6E484FFF5084BBCE6FE6A126BC8AEB36029
SHA-256:	390F720FD469210E2E0F810047B9EF09CA17F2CF1496B1CC699101A75BE982C3
SHA-512:	7F659CF5BA29F138D6603CC6F479492D450DE0B22EB785BB866B4E25C235B4A1924BD32A77D0DB1FECA1321AA4123473D977989FDCF99BB0EA7D78EA3D2084 3
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ....Z.L/....."#.D.0.f...A.A..Eo.....m.....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):	5.554088572233659
Encrypted:	false
SSDEEP:	3:m+l26Xa8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKH/KPWFvJcfvRktCtjX8AL2OP:mYXYOFLvEWdrROk/RJbuLjtC2fO441
MD5:	716DE5DFDA7B826E67B8E5BCAD92D159
SHA1:	ADA658FAA4B8296C94B34FF10C8ED788C96F6954
SHA-256:	8CC985E9CE7BC3B250FB1C3167874DF0E0F4EE11068D583C1E23D186235BF6B7
SHA-512:	572079EE0BCE02A4237A1171B0CCD267748A29DB6E59D09EF432E1A8F8B672B2CD32C19A11145B9B7163E8A54017D3BAF55718FAA4E37C3B29930C50B59A58C5
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .D..Z.L/....."#.D.^.f...A.A..Eo.....C:<.....~..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):	5.530452100263736
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVlROhgvRktNlfzoIN1OFPL4m1:mmDEYOFLvEWXlPOpt3fzV1QPLr1
MD5:	5D1D5D4CE30C13BA7F740C7DD1A8C147
SHA1:	34718FD887E723D9DBA1D9A2CB61E1976720195D
SHA-256:	D0C2B1A9C32E53563714432E56101F66C5A74C453C23502B25F0D05E5EA31910
SHA-512:	EDEB7B2A88C8FD6AE98275C107AF1E90F2E11C34BA7B1C220197F5353420E3596F21B47F1E22F8A09BE609D6FEE6B325EE1319E1D6BD45F50CD25525C656C964
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...Z.L/....."#.D.+.f...A.A..Eo.....a.....~]...%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):	5.584009079562968
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvRsNlZm/vRktzSl/u8D6EsEJeUm1:m52YOFLvEWdMAucRt6/uEvsEJ41
MD5:	D081477E4B272539D5A5B2E30B76C007
SHA1:	DEF5FBC31EEFCE7DC8801D3B4299A9D231A5D9AA
SHA-256:	3BA74225ACA0465508BF23CF4C952AF7A24536F3786B5E5F9201F8DB82DFF08F
SHA-512:	B1CF1DFFAF91726317104DFAB210EDFA47AA066BA1C25A3399EC3F77B4EB58CD8CE746C2B18F7085ACF19EF1F49A5A61ECEC1A2F308CC8EF30AE830ED1CE98A6
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..".Z.L/....."#.D...g...A.A..Eo.....N.k.....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:	modified
Size (bytes):	210
Entropy (8bit):	5.582738188260367
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFvmeH/X/woFfvRktdIFoDb7M:mYilPYOFLvEWd8CAdAuEeXytdyong1
MD5:	91018FFC25D2CB73AFC3CC74B8CBE356
SHA1:	7211AB1695296BE74775621DFF68799C85391001
SHA-256:	614A7DC664F5AD7E94EE85FB3F5DB7906EFA1F27CB58AA02E37B690BD649CA29
SHA-512:	C8EC277558A91F201D3D419A0B4DB8BEACAB7AEE4E6B9FA0AFB1594040077286CA052EFB75F6871592745C56C1B58BF4B872D2D8503E48B8C49433A0ED59539
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .z+.Z.L/....."#.D...g...A.A..Eo.....C.P.....c}.H7M=M..-.....lx..R.I...} Rl.$q.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.57501906280205
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVlJ/2oKPWFvl02HAHsdvRktOBH/lDOe28O:mY8nYOFLvEWdrROk/luFDtmdN16wG1
MD5:	4B2B489FCEEECA4731C849C3EF8A0E28
SHA1:	5B9BB9EBD665D3707B8ABF356ACB237B6BF90F44
SHA-256:	9DFFE1AF161756D111C187EDF2546AE6F9351BF9E3EE719F26BCD27DA0530D3D
SHA-512:	4041C34467642CCAB1509AE1B3E690270653FAB07CA0D715D825E4528B193FE40D06B17BA80B7D04269D7AA6FA294EAF00B658E49A2102A4922CF2E6F11347A8
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....Z.L/....."#.D.R.f...A.A..Eo.....).....%.k.SZ..~W.....:)'B..ad .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.655939837535185
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVkbTDYGGvRktPllePmJelm:mLrnYOFLvEWdrloJUQvn8StPlQeJli1
MD5:	866E75C2D2AA8A2B6F6F8077A2493D23
SHA1:	AC80A9EEA31445BEA328B252C80751055987F2CD
SHA-256:	0E20762A0CD50A30DE47C6535B9A54ECDC6796DEF063EB353A127951E6B810C4
SHA-512:	BAC8E1966023A2F14D24E0B11B55E550790AD13901EEFECA65109B100CC3B417EABF8BF6CD879381C589BD1FDFA93D648087BA9ED9ADC828F1B54A6FE390E4 CF
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .P.Z.L/....."#.D`..f...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):	5.534747510759717
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvhf9GGvRktua/P6mgmOZLhT7Um1:mOEYOFLvEWdrlhuLFStuanzgm2d/1
MD5:	D95219FA8C7887692906A6218E103930
SHA1:	A0EF634BFC5422DDA13CEABFCF5EB835A0BB3554
SHA-256:	8F956FDE6D22D3679C46574FB80A2A4A9EF7A311EA1B300A31A700DD93F540A2
SHA-512:	6FBDAB1756D3C91B7034FCF6063728080A7CA3C037D4619AC45A63803757B462DD6E12094D21090E25F79EAD28AC6EF02FFC43CFC14C4B8806A631A78FC2DF/ 4
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..x.Z.L/....."#.D`!.f...A.A..Eo.....d.E.....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):	5.581028438107124
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cv0Q2EvRktPy9ll/lGBiaQ562HvpMm1:mAElVYOFLvEW1K5tPyHDx56uvp1

MD5:	B7DDF5AE1B69C977828DB2116DB13248
SHA1:	D8405C15277593925BA657FE77CEA68C18855020
SHA-256:	75A5027AC6C4940B6269C440507528FE679CAF8033B7D385368081C0E04E151B
SHA-512:	C019A30B95851117BFF274F672528D0F73F4485D46C7212069F2570E01B403B154BF742BFFB7F1701A33F898BBD70688A568A18B734288A4672E6C47F63C2F60
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...uZ.L/....."#.D..f...A.A..Eo.....B.....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):	5.621534938221349
Encrypted:	false
SSDEEP:	3:m+lSy/08RzYOCGLvHkWBGKuKjXKBRSJvBCv1KPWFvqX/HlllFdvRktsOY8UDLY3T:mWYOFLvEWdBJvvuo/HYtNUDLYtmOZn1
MD5:	8C2D3F3533EA4322B0B2E1D0C0A7C40F
SHA1:	C9AC4AE8C1DC33EB9A3B4CA4E06ABE0C8BC9B51B
SHA-256:	BD7976A92A34E0FB036C468A7F0DE0123B16AA274D4644A814861099A5A748D3
SHA-512:	2D0BB401D50A8D1B066AF022B18D25926C342EA886571824E08A1ECA9054C6ACE5AF80F12D9D7C517FD12CBC47D0A7841036E09490613770AD27D58F75EBB51
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..`.Z.L/....."#.D...g...A.A..Eo.....a&.S.....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):	5.545321920911231
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvR0UdvRktre/tnpSKGoSSlf:msRPYOFLvEWIa7zp7XUQta/F8VPu1
MD5:	95A16FC4F211DDAB664A890CA796929E
SHA1:	E0DDC89FB0BE005711EB6D1FFAFEDDB7BC7AF84F
SHA-256:	4410FC70B376478050C52E3F0D9979ED6616D408CE9547138C6A5408B3F7CB92
SHA-512:	EF6B6993D05ABDB89E5491FD0DD932DA271F6D15E5950881A6257DA49E0A37D012C80B0CCED2FAD1F4BC102FF5FC57F8694C86518BDCDD8051B0F03A316BF 28
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .;lsZ.L/....."#.D]5.f...A.A..Eo.....4r.....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):	5.596436272538276
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuV28p+m9vRktGoG36F4XVAZ+8cV4:mKPYOFLvEWdENU9Q588t/GKwiM3Y1
MD5:	B8038C26EE93BAD857DB2E85C99A4C8C
SHA1:	03510A6C91A4D2B1DF14909F06DB14A8C413AAC8
SHA-256:	B3173795FB5F78CD6E039318D96268E67D0FAE0098E4B3B6A178F36B569B5498
SHA-512:	9F21711F4524EA93B436EFA3BA36918BCA5625FE5A6233861135647BB305D9123F9C89BBB9B4A44DFDA96D696D86FD600DD12E669280E3886AE7053A81A8DBD
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .?N.Z.L/....."#.D,..f...A.A..Eo.....TM.....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):	5.599585416923149
Encrypted:	false
SSDEEP:	3:m+lQWt6v8RzYOCGLvHkWBGKuKjXKjcAW6KLuVnHl3w29kvRktBF/B4MY3jBMQ7G6:mQt6EYOFLvEWdccAHQAt0jBRCh/41
MD5:	11666A493C34BE905853085A05274C57
SHA1:	D53ED8BCB7F8E60F24CADF7C2B1FCD4882841E07
SHA-256:	188EB4F13F63CEEFEFE801B4F8851065F0CF27FEA308C5D8D626D9AB31042EB9
SHA-512:	3789036CCCCE0253A90CC435B80AB83A934D8D3EAE26A9CF0F7915A48D5BF3984A524654633E777855CAA040D18CBE35D355A19F29F00547C251E7F760B2293
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .=/.Z.L/....."#.D...g...A.A..Eo.....&.....PJm...0x.x..RD...BB!@5..<..] ....A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.560996294773765
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu1EwtRNIFkULIF4r1:bs6xRkirEwH3F7LIF4
MD5:	515D1F91BBF35977828D59B1A5B30C36
SHA1:	D1C412E96785B9B338B60904F401FA8FF2707597
SHA-256:	75770DB309D203CD134F8B7E372E0285ABC2851BB87E551EF7BB65E3312ECFD0
SHA-512:	DE4E0BFB5333E0E8514CCCA03CA38D10D936EDF6CB331871825DB08E9A018C19809F894DDCC3F2E41BD5A83890B4A01F1126089FFCC3FA21FA2104AAD28E7 9D
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .I.@Z.L/....."#.D._.e...A.A..Eo.....OOB.....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):	5.4899451583202525
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvbvbuaoE9kvRktxyXlECcu1isLKo:mhYOFLvEWd/aFuhswtxy1EN941
MD5:	994CA718697C3A621E58B4B0830026F3
SHA1:	7A605E0BCADBF4CFD3D69DE2E4E715B3E4F5B5EB
SHA-256:	08E5978DE1AE3CC11E823A04AD7FD3091CF425CC3B1E07D9FA0B2DCBC67651B1
SHA-512:	B224FA22BE63DDF5569E13CFB2572ED2506FD106A7AA328459E41A07BBB2D36DEC2E208E72EEEFC274D635ACDEEBF61DE0C60E3DB74742FE87537C609DB15 ADE
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ...Z.L/....."#.D..g...A.A..Eo.....a.f.m.i.o.p..3U5.....^...I.A.. Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.5160300855012405
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQetgDBMqVd3G4K41:2DRuRfQB9Vd2
MD5:	89031C8B6E397C5E2A827F9FA237B577
SHA1:	9BBEAC77E403FB018F946F4C7EC802719EFD44D7
SHA-256:	3FCDE63E7EBAE5EBB9C93984661B2358E80AE473A469F8C779D3814E145AD79B
SHA-512:	A8E74482B3CF344E3FACB0C1F7827CBC833E21A9057CF160F9155B92909543C3A0B423C8FF8C2AB0F8142293C955DD404D850BC69811229B472A08D2F33CB20
Malicious:	false

Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....Z.L/....."#.D37.g...A.A..Eo.....dDd.....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):	5.5581294934093375
Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVT/H9vRkt0XNpW4ThzJuA4bx:mkqYOFLvEWd8CAd9QlQtwuA424r1
MD5:	787579B243D591C531AD2F9C0555DB36
SHA1:	942DAEDE366774C6D1B65E400BE0BB6F18784695
SHA-256:	A12F60D82931B410DCC8788F279172C5F9AF0CF14A68D36AD5C8EB4E5DD70DA6
SHA-512:	D8298984331632D122D9D9E373419DFE77A5E9A73D91B3B27AF909BF95FB97035E0A29ADAEBA052F81B90818500ED65AC992EAF8424E432E492F57F1AB2AD42
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .g..Z.L/....."#.D2..g...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):	5.549428198836326
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFv6+JGGvRkte9/1Ag2iHio/Mm1:moXXYOFLvEWdENUAuvkti/+yC8n1
MD5:	AD31892C8BE68BD1F8703DA21AB3CDC8
SHA1:	A466498E2D7ED8CE143BBE68FB6674A96260800A
SHA-256:	C606A7B5BEDAABCEB8AA86903E0B8A00039D04271A691C6959D4E4268007CE37
SHA-512:	38B5EAC8193CA171C2DCDC4BF56C718967241A512EF6C2B5531A67E8359963EB212EB1BF527513276BAABDDED03311DB3220EB04B6CA81F793DBEF42CEB3A A7
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ...Z.L/....."#.Der.f...A.A..Eo.....P%.....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):	5.616671330140792
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQj2qiFSt8tsLmB41:nRrROk/VloIN
MD5:	73AE14C36565F5190880AB1552A1EB4A
SHA1:	B085199BEAAA0BDBBF06DB0184A8E4CF34D0AF0A
SHA-256:	DB95A7FC09DBE0EE63B4CF58EB0F8DC9306C00E077915DD7BD6028DEF68BD4D5
SHA-512:	F7985A01D934F73BAEC924FE5805AD046D49C2573965040638076AFC0B2765E49ACB37DF12C1E9B05C4F2C30ED84A68B35B735E4A715442645D4B0B377F68925
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .F.Z.L/....."#.D.B.f...A.A..Eo.....,..... ./.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):	5.555040823641522
Encrypted:	false

SSDEEP:	3:m+lUV/la8RzYOCGLvHkWBGKuKjXKjcAW6KPWFvt0p+loNhxGvRktcZrobk9mZa6E:mZ/lXYOFLvEWdccAWush9tAdm9741
MD5:	9DE9D7A2883A8FE2F57A45E6803EA3B2
SHA1:	72B972A56029B8707A0A97C82819BDB748484EA5
SHA-256:	D68ED7880B17B95843DF4993FB45BFBC2541621DEC505AE9858E503C140C597E
SHA-512:	696321D5722A2112F33F123E380966DEE10626E6EDFD2A4656DE3FBCCB34AB0133FDEBDFD8C4061FB81ACA1947626F5888060F9A37FB4E35F8C87CD2AC72F4(F
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .m?.Z.L/....."#.D...g...A.A..Eo.....'};.....U...I.>P...X...x..0U.~;m.x.k.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.522313475718964
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvyNl8fvRktMqllll2B6shoq+Nem1:mMOYOFLvEWdwAPVusNlDtMOEB6Jn1
MD5:	7416A53DDB0A88C44C7D877B67AB1AE0
SHA1:	F3C42FF118F81AC159EAE8424B4E04571DAE8A17
SHA-256:	C90693DF0A1C72368193AD0123850CC095FCF80F46E4E36580B0D197879C14EE
SHA-512:	F75489963AB7827B8F33F2C42C444A1CD4EE1A34DC73F927563B84334A78B4653453D64EA088340DC52A94B9B639D8C9F50342FE08EBC6EBD5919A1C41D18D3
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .e..Z.L/....."#.D...f...A.A..Eo.....k....F..D..O.n;[.1m.....=..A..Eo..... .....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.626306421092853
Encrypted:	false
SSDEEP:	3:m+lUDfllla8RzYOCGLvHkWBGKuKjXKBRSJvBCvlKLuVp9Q0kvRktGbQN/hcfsB4:m3PXYOFLvEWdBJvYQCtJhcsBXIh1
MD5:	E51975E0560A842627F367133F0D3230
SHA1:	091FA85A9DF3F7E9C0B62D1FBBC0EB6E1FB18334
SHA-256:	4C5443CC9E79DBB791D50053ADC299BF46FB60E8F822692170752239AFC1B7B8
SHA-512:	46E257E72101F0FDEF2EE3CBAA8101C9D3D32B1E4ABB545BB0ACE58719A34D94564160653AC77F26A63BD18BD4C221B177F0015EAC5FDC76C9A4A057154C1E2B
Malicious:	false
Preview:	0\r..m.....T......z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .`6.Z.L/....."#.D!=.g...A.A..Eo.....SD.z.....k..`..N3.... ..d..$[.....{.A..Eo.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.57688097015567
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQbHsNE9t1Wzc3Me/1:3RrROk/susCW
MD5:	567515CBEBC1FB7A066E54A4D09222AB
SHA1:	0A1B4D8A830C8E71F04B98CB84A42C9FF28E0D14
SHA-256:	16999D84040417FCE4A81E1F2EDE01A301B1D0A793A0CFFDDB6CAD6858397054
SHA-512:	885A69A1F6AC871A9A9BDAB45B37ECF087A85233CE6234EEF9D142E6ADDED8316CF5852DE5D92853C313BDA309D26918EDE7548FC1BE49C4C337BE6418C4F3F
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .v..Z.L/....."#.D...f...A.A..Eo.....6?.....9Q].8O.z....=..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.08787025016182
Encrypted:	false
SSDEEP:	12:El8vV+/l/C45tgPLAZc04DMzlqCUjhLi+/l/qRYGU3jwDtvD19pAAewNcbga:El+OHcvML+3ltyxOkga
MD5:	092A3DA36451AB9965B96431B3840225
SHA1:	CE1BE8D69066D2D19BA41BDB10266B8AABAD828B
SHA-256:	46E80CF22B53DF1670E856D761F92FB1C9E4B8F26455633A35A2C42B454F2196
SHA-512:	28B78B65E619B37057A50C66E59CA9D184093D5968551AD8AF25A6856FAA387D2BC314EDD111C0AC1481F817FA72FDE16C24D5734A9205BDABD4A49E79126CI 9
Malicious:	false
Preview:	0...=..7oy retne....+.....V.....*....zZ.L/.....:.y~A...zZ.L/.....oB*.ZkZ.L/.....#...(...A_./.....D.4...Z.L/.....[.i..%...Z.L/.....k7A...zZ.L/.....]...I...=Z.L/... .....,+..._.#..zZ.L/.....<...W..J.ZkZ.L/.....J..j.....zZ.L/.....6<|....ZkZ.L/.....2q.....zZ.L/.....P....V..zZ.L/.....!...0.o..Z.L/.....P[. q..zZ.L/.....3.....zZ.L/.....v ...q...ZkZ.L/.....a.....ZkZ.L/.....C..M.....A_./.....qi.K.L.9...Z.L/.....K..JM.gb...Z.L/.....=Z.L/.....F..=z;...zZ.L/.....o...zZ.L/.....Gy.'.h...zZ.L/.....:. N.A....zZ.L/.....;/....zZ.L/.....zZ.L/.....A?.2:....Z.L/.....o..k....Z.L/.....*.....Z.L/.....q...Z.L/.....u\]..q..Z.L/.....+.{..'..Z.L/.....^.~..z...Z.L/..... .@..x...Z.L/.....*)....J:..Z.L/.....&.S.....Z.L/.....MV3....Z.L/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.08787025016182
Encrypted:	false
SSDEEP:	12:El8vV+/l/C45tgPLAZc04DMzlqCUjhLi+/l/qRYGU3jwDtvD19pAAewNcbga:El+OHcvML+3ltyxOkga
MD5:	092A3DA36451AB9965B96431B3840225
SHA1:	CE1BE8D69066D2D19BA41BDB10266B8AABAD828B
SHA-256:	46E80CF22B53DF1670E856D761F92FB1C9E4B8F26455633A35A2C42B454F2196
SHA-512:	28B78B65E619B37057A50C66E59CA9D184093D5968551AD8AF25A6856FAA387D2BC314EDD111C0AC1481F817FA72FDE16C24D5734A9205BDABD4A49E79126CI 9
Malicious:	false
Preview:	0...=..7oy retne....+.....V.....*....zZ.L/.....:.y~A...zZ.L/.....oB*.ZkZ.L/.....#...(...A_./.....D.4...Z.L/.....[.i..%...Z.L/.....k7A...zZ.L/.....]...I...=Z.L/... .....,+..._.#..zZ.L/.....<...W..J.ZkZ.L/.....J..j.....zZ.L/.....6<|....ZkZ.L/.....2q.....zZ.L/.....P....V..zZ.L/.....!...0.o..Z.L/.....P[. q..zZ.L/.....3.....zZ.L/.....v ...q...ZkZ.L/.....a.....ZkZ.L/.....C..M.....A_./.....qi.K.L.9...Z.L/.....K..JM.gb...Z.L/.....=Z.L/.....F..=z;...zZ.L/.....o...zZ.L/.....Gy.'.h...zZ.L/.....:. N.A....zZ.L/.....;/....zZ.L/.....zZ.L/.....A?.2:....Z.L/.....o..k....Z.L/.....*.....Z.L/.....q...Z.L/.....u\]..q..Z.L/.....+.{..'..Z.L/.....^.~..z...Z.L/..... .@..x...Z.L/.....*)....J:..Z.L/.....&.S.....Z.L/.....MV3....Z.L/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF47a455.TMP (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.08787025016182
Encrypted:	false
SSDEEP:	12:El8vV+/l/C45tgPLAZc04DMzlqCUjhLi+/l/qRYGU3jwDtvD19pAAewNcbga:El+OHcvML+3ltyxOkga
MD5:	092A3DA36451AB9965B96431B3840225
SHA1:	CE1BE8D69066D2D19BA41BDB10266B8AABAD828B
SHA-256:	46E80CF22B53DF1670E856D761F92FB1C9E4B8F26455633A35A2C42B454F2196
SHA-512:	28B78B65E619B37057A50C66E59CA9D184093D5968551AD8AF25A6856FAA387D2BC314EDD111C0AC1481F817FA72FDE16C24D5734A9205BDABD4A49E79126CI 9
Malicious:	false
Preview:	0...=..7oy retne....+.....V.....*....zZ.L/.....:.y~A...zZ.L/.....oB*.ZkZ.L/.....#...(...A_./.....D.4...Z.L/.....[.i..%...Z.L/.....k7A...zZ.L/.....]...I...=Z.L/... .....,+..._.#..zZ.L/.....<...W..J.ZkZ.L/.....J..j.....zZ.L/.....6<|....ZkZ.L/.....2q.....zZ.L/.....P....V..zZ.L/.....!...0.o..Z.L/.....P[. q..zZ.L/.....3.....zZ.L/.....v ...q...ZkZ.L/.....a.....ZkZ.L/.....C..M.....A_./.....qi.K.L.9...Z.L/.....K..JM.gb...Z.L/.....=Z.L/.....F..=z;...zZ.L/.....o...zZ.L/.....Gy.'.h...zZ.L/.....:. N.A....zZ.L/.....;/....zZ.L/.....zZ.L/.....A?.2:....Z.L/.....o..k....Z.L/.....*.....Z.L/.....q...Z.L/.....u\]..q..Z.L/.....+.{..'..Z.L/.....^.~..z...Z.L/..... .@..x...Z.L/.....*)....J:..Z.L/.....&.S.....Z.L/.....MV3....Z.L/.....

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):	5.1927026002593415
Encrypted:	false
SSDEEP:	6:n0Vq2PWXp+N2nKuAl9OmbnIFUtqIogZmwYIoIkwOWXp+N2nKuAl9OmbjLJ:nMvaHAahFUtZR/TL5fHAaSJ
MD5:	7E5806C79D3B641EA234E41C95C0236E
SHA1:	1A4BFDEBAE0408DA6FF83BB068A65896061CD437
SHA-256:	43AB055C161ED1E7A04C8758F1062368265C5F94CBCCF74E8752198553CC5BE2
SHA-512:	42CE00A39F177642CFEE30C7DF793513668E26427521415CE65782CE9945436406432BE5EEF770D567494C4AA634876BC7EDB4AF5A1BDD891107AE5106A83755
Malicious:	false
Preview:	2022/11/24-19:25:00.199 1484 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/24-19:25:00.209 1484 Recovering log #3.2022/11/24-19:25:00.209 1484 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):	5.1927026002593415
Encrypted:	false
SSDEEP:	6:n0Vq2PWXp+N2nKuAl9OmbnIFUtqIogZmwYIoIkwOWXp+N2nKuAl9OmbjLJ:nMvaHAahFUtZR/TL5fHAaSJ
MD5:	7E5806C79D3B641EA234E41C95C0236E
SHA1:	1A4BFDEBAE0408DA6FF83BB068A65896061CD437
SHA-256:	43AB055C161ED1E7A04C8758F1062368265C5F94CBCCF74E8752198553CC5BE2
SHA-512:	42CE00A39F177642CFEE30C7DF793513668E26427521415CE65782CE9945436406432BE5EEF770D567494C4AA634876BC7EDB4AF5A1BDD891107AE5106A83755
Malicious:	false
Preview:	2022/11/24-19:25:00.199 1484 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/24-19:25:00.209 1484 Recovering log #3.2022/11/24-19:25:00.209 1484 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~RF4716e9.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):	5.1927026002593415
Encrypted:	false
SSDEEP:	6:n0Vq2PWXp+N2nKuAl9OmbnIFUtqIogZmwYIoIkwOWXp+N2nKuAl9OmbjLJ:nMvaHAahFUtZR/TL5fHAaSJ
MD5:	7E5806C79D3B641EA234E41C95C0236E
SHA1:	1A4BFDEBAE0408DA6FF83BB068A65896061CD437
SHA-256:	43AB055C161ED1E7A04C8758F1062368265C5F94CBCCF74E8752198553CC5BE2
SHA-512:	42CE00A39F177642CFEE30C7DF793513668E26427521415CE65782CE9945436406432BE5EEF770D567494C4AA634876BC7EDB4AF5A1BDD891107AE5106A83755
Malicious:	false
Preview:	2022/11/24-19:25:00.199 1484 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/11/24-19:25:00.209 1484 Recovering log #3.2022/11/24-19:25:00.209 1484 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.010978819626460943
Encrypted:	false
SSDEEP:	3:ImtVdXb+j4x9pPlXlpyPll//zVrzlltD0lGQZ7XEZhGIeIHdP4/X:liVtg4x9pdM//hFwl570ZhdelG/
MD5:	E36F8F81D3C03F6AAF7D768706B7673F
SHA1:	EECE93F9E417717892E50F6A159516DD76C255B0
SHA-256:	C6E687FF9677244574F37AD2877726DF64E5BAADDA2ABE8C4759BDE8344E44F2
SHA-512:	0582ADCFA1A09095D4482C9A61475C8B77FF444BF2655DE4F6583BBB2699A054BBB2292DE2741FEEB27AFE0835B0B48F476418EE1A666DE20CA146D1EB4390A4
Malicious:	false

Preview:	VLnk.....?.....Tq.>..j.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-2211250324562-209.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):	3.8613823329806443
Encrypted:	false
SSDEEP:	768:+vk3dGGGGGGGGGGGGGG4GGGGGGGGGGGGG0GGGGGGGGGGGGGGGGGGGGGGGGGGG+:+vk3n9A9W99/9EvD3Sc839q
MD5:	818F5EEE3C3659AD0B057B9D953BAF1E
SHA1:	01DF2AE5B664CCCD260817C5275D396E15007782
SHA-256:	BA76C1EEC6977B38BA871D2FC1133A2AD9B85B405C113E084AFD203F5FF969C4
SHA-512:	3C2AB6EF1DA53F67F38BC1FCC9349E4553B88A60C3D558DD0CB4E0C0ACD3BA4C325FF7F73ECD67EF3461DD6B4C58C9ABE56794E054A718908BC776CC6AC558F
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 12, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 12
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.564759645073216
Encrypted:	false
SSDEEP:	384:3eI9dThpNlrCtELJ8fwRRwZsLRGlKhsvXh+vSc:RNlrCkYZsLQhUSc
MD5:	DE83AC90FA4C2D0A875EAB09770D86BC
SHA1:	95C395F3FC07DCD45B6AC46130944E92ED794194
SHA-256:	F84D0019F282ED9E4AB4CC2475107349D16A320118B539F5F33751F93E5758E0
SHA-512:	989BBEB1CB51569E478D20F598931924ABDFA9C06796A5B0E98971C4872775FC0655432760BBADAB05C51646891B3224634B6D87709593459C788D36209447E8
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):	3.288385615044931
Encrypted:	false
SSDEEP:	48:7MOom1C0BiomAxiom2om1Nom1Aiom1RROiom1oom1pom169ZiomVsiomgZqQlmFq:7S0BXxOhAPCsZN49IVXEBodRBkq
MD5:	9FD02B38DFF20DE6AFE69CA845F8F3AB
SHA1:	D36689317C6B4F9058A2619A3587030D1732C55E
SHA-256:	00DD33F686C07B904ABE49186F24050285C05D645F5229DA8F04E41BCFB8811E
SHA-512:	73DD7569B83CED119B02BAE0296B0C0161128AF1DDAC17869DC34988427E3364DFD15F830694DCA11C1F256CA964BFB1289A9A293FECAEDC18AB2CB4357962CA
Malicious:	false
Preview:	.... .c..... .....s..... L.s.y.....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_store

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	0.6750050738677021
Encrypted:	false
SSDEEP:	12:BZ2vX7vz+YXnTIHLjJ9wkl4c6/oCyitQBOIP0xg5/fLM:BZeXTz++lvJ9wkl4c6QbiuBOI2gxLM
MD5:	C38DB0F968872CB3B1FBF6AE9A0EF9DC
SHA1:	F33A6E1368267704758D324C3170FFEC35A64886
SHA-256:	6B804B2E7E3F3F270A809298758697B12697A26846FF9D20E0FBFDC9F64EED8A
SHA-512:	55BC7AE2ABAF607B7B4F6804390ED8FC796EDC0D778728DDF84E62B97BE74C1BD9547CA1EEAF3646BADD30C8AB1A7E20D534249DD976E07BA83B718DF6A39AD8
Malicious:	false
Preview:	...Q.....{W.C..$;..U....b.T}..k..... .....g$#..q.....i>....[}l..... .....M^.....A.....W >.D...{.... .d...h.g.U7.Z..!.....j.&...Q,9.....M4..mN.1...CB&....$.....,1!.f_?.1..&.....a....t. ...]U.hQ.?..*#1....r|..0c...=.....]..J.....LfhI.<.....].5...P.5.9..{`b.GB.....$.....r.&"8..2..x5.n.j.{.S}..l..[..4..K._.*....Q..A..L..YY..vg..M...x..d|0...k..l..~...-Cih.KW...._".i._.!..X.r..... .&.Q`....90....L... .bz.s-Z.}..;v..>...%.|.^.....}.qm..:....Pf....`.&.L.....ny.....)I.M..Q..xZ...$.I..... ....

C:\Users\user\AppData\Roaming\Adobe\Acrobat\DC\Security\ES_session_storei	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	0.7519410049126055
Encrypted:	false
SSDEEP:	24:DM9iGGEWwXc9BeayznQAY3vFVV5jDBJej5JVzesSSUeolpgdXcdSqx2DX95:oVXG9BCWZ857zctIawz
MD5:	48B99ACAEC7BCFBDB7F0B4B96B2453B1
SHA1:	BE8AF0C8AF83D943747928B45EBBF44ACDCB374F
SHA-256:	D92FEC879C4EAF4D3B887C7FDD0FC602F9C97C0BBA66024E4F280C27DDDFD0A9
SHA-512:	429D4DB90913FA07F2402BBF3802A4DF6DFCB1E367E4B41D8629B85F463FAAF38F5A6EC51D0551C4CA845FDE856C2203875DB5F87DBA6388B0A4A648363DF32E
Malicious:	false
Preview:	...s..K.....j+...%...X...Ba.....zzd~.....#B..0_...\..=.u.!!..+@.f...Y.)mg..;...Ab.....a3..k.....MU.Jq.$*.jnG..*.WY..W.~...:.D.M....n.L.....d.."b..]n.....bj....p...d..cN.s..+P8. {z:x.P$:..n.L.X.....co[v"Y....^...59.32.tn/Ce0.*\..i.N.N.}A\.e.U..7$zf_x..j*.buOq.N...P=0'.....e..#.....I..;Aq...|.el.78..g.#.....k...#2>.....G....% ..K..=W.!..@..[..7_>Pl..(.$. .%..`'.kglw.....UC.4.....^.M...!....4y..O..~.|...vpY.8\H..z..Kb..j.....7G]D.9$.7.rRu..,t!^..0.e...|.X.]..k.KVnb.B;.n..P.....q....P....:mg.jH..R..3m..x.$...zR.b$..QR.M...`.....U{....(.a ..Z..EZ.6+.BM.Fq....Wgn...=..k|.. ..>....q...T?6zSB.....1..6.....s...l^k.Lt..f..c`..V.qz@.+..e$..... .....

Static File Info

General

File type:	PDF document, version 1.3, 6 pages
Entropy (8bit):	7.983028017034608
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	Get BTC 5763.pdf
File size:	276977
MD5:	5cdfdba4f3219d8d7c53430060b0f741
SHA1:	f2e1cbcd97d59ae214dc02aa55177991e638a67e
SHA256:	ff6af650ee8ef5849e423451bc2e359bd7f8e40a13b3c6d64692f8bda82bf04f
SHA512:	30035a21d7045e379dc0cd1f007748bbf08234a08e0c60ee841c95258cbe3016074d9bb35af55ec06240d8cd04a682d03b988a95ecf48b6a5506ed9b8a94e33a
SSDEEP:	6144:eP4luB66RYDbE7/9CI0Kv5ryxgwurCJVwgd7CLdFD4:fbwYfEvxWgwvwgd7qD4
TLSH:	5A441260EB35684EF58988396D2D360C815EF16B05C1A48209B80F977AD0EADCFF6DF5
File Content Preview:	%PDF-1.3.1 0 obj.<</Type/Catalog/PageLayout/SinglePage/Pages 3 0 R>>.endobj.2 0 obj.<</Producer(Synopse PDF engine 1.18.6228)/Author(QOWEYWD8EEEkW07Lk5Em0654zO3)/CreationDate(D:20221124105657Z)/Creator(FSBQNJQXQygytbiugj)/Keywords(Futibory Pyjogof Puxe

File Icon



Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

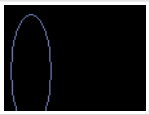
General

Header:	%PDF-1.3
Total Entropy:	7.983028
Total Bytes:	276977
Stream Entropy:	7.995345
Stream Bytes:	262229
Entropy outside Streams:	5.377557
Bytes outside Streams:	14748
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	77
endobj	77
stream	34
endstream	34
xref	1
trailer	1
startxref	1
/Page	6
/Encrypt	0
/ObjStm	0
/URI	2
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

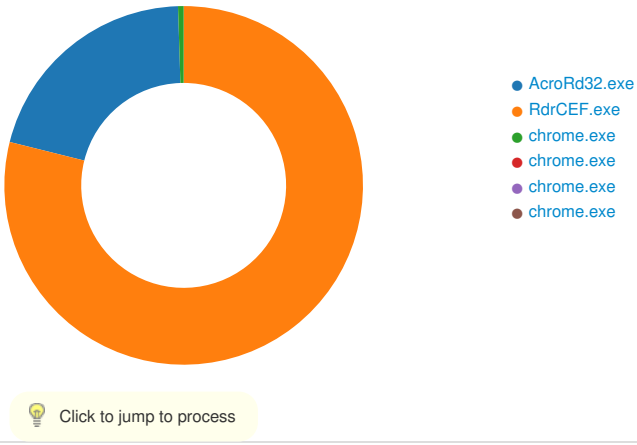
ID	DHASH	MD5	Preview
6	32f0d8cc70696916	61dacf1c4b1fbcda822e652382a11f68	
41	c4923818c2440000	19cc7c6f4982f39f0efeee494bee982d	
42	18764390a0a020a0	f46cec8808cc8b887fbcddd23fd4d887	
43	801fe080807a8110	b5883193ec93e62c92be1ed4dfdacd49	
44	8080404040404040	750c60c0d056699e3f9630e766459986	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 5312, Parent PID: 3452

General

Target ID:	0
Start time:	19:24:49
Start date:	24/11/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\Get BTC 5763.pdf
Imagebase:	0xa00000
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

Analysis Process: RdrCEF.exe PID: 5328, Parent PID: 5312

General

Target ID:	1
Start time:	19:24:54
Start date:	24/11/2022

Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0xaa0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	4	B959E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	37	BA83E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	113	BA8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	218	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	16	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2178	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	59	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	11	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	B959E2	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	4	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	4	B959E2	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	7	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	4	B959E2	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	3	B959E2	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	4	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	24	B959E2	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	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	24	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	4	B959E2	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	55	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	4	B959E2	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	59	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	4	B959E2	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	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	88	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	4	B959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	53	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	58	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	20	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	13	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	B959E2	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	20	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	237	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	286	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	266	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	3	B959E2	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	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	7	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	3	B959E2	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	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	6	B959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	10	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	248	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	12	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	23	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	3	B959E2	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	487	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	B959E2	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	B959E2	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	2	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	3	B959E2	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	2	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	6	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	224	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	3	B959E2	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	16	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	47	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	3	B959E2	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	14	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	3	B959E2	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	3	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	3	B959E2	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	5	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	3	B959E2	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	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	31	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	B959E2	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	B959E2	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	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	B959E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	4	B959E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	B959E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	BA83E5	ReadFile

Analysis Process: chrome.exe PID: **6844**, Parent PID: **5312**

General

Target ID:	11
Start time:	19:26:14
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://docs.google.com/drawings/d/1wLersYca4EHHhywY6CHe2wACV0xN6gPB_XsbZwpjGQc/preview?0434006604750527756707105652256518581873 31
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Analysis Process: chrome.exe PID: **7020**, Parent PID: **6844**

General

Target ID:	12
Start time:	19:26:15
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1976 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **2244**, Parent PID: **6844**

General

Target ID:	16
Start time:	19:27:19
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5104 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **3600**, Parent PID: **6844**

General

Target ID:	17
Start time:	19:27:19
Start date:	24/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6380 --field-trial-handle=1620,i,16339735771370879276,14243754389076047463,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly