

ID: 440305
Cookbook: browseurl.jbs
Time: 07:17:51
Date: 25/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Sigma Overview 5
Signature Overview 5
AV Detection: 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 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Private 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 41
No static file info 41
Network Behavior 41
Network Port Distribution 41
TCP Packets 41
DNS Queries 42
DNS Answers 42
Code Manipulations 43
Statistics 43
Behavior 43
System Behavior 44
Analysis Process: chrome.exe PID: 5144 Parent PID: 4944 44
General 44
File Activities 44
Registry Activities 44
Key Value Modified 44
Analysis Process: chrome.exe PID: 6152 Parent PID: 5144 44
General 44
File Activities 44
Registry Activities 44
Analysis Process: chrome.exe PID: 7576 Parent PID: 5144 44
General 44
File Activities 45
Registry Activities 45
Analysis Process: AcroRd32.exe PID: 4176 Parent PID: 5144 45
General 45
File Activities 45
File Created 45
File Moved 45
Registry Activities 45
Key Created 45
Key Value Created 45
Analysis Process: AcroRd32.exe PID: 7764 Parent PID: 4176 45
General 45
File Activities 46
Registry Activities 46

Copyright Joe Security LLC 2021

Analysis Process: RdrCEF.exe PID: 7776 Parent PID: 4176 46
General 46
File Activities 46
File Read 46
Analysis Process: RdrCEF.exe PID: 7880 Parent PID: 7776 46
General 46
Analysis Process: RdrCEF.exe PID: 6864 Parent PID: 7776 46
General 47
Analysis Process: RdrCEF.exe PID: 6528 Parent PID: 7776 47
General 47
Analysis Process: RdrCEF.exe PID: 4204 Parent PID: 7776 47
General 47
Disassembly 48

Copyright Joe Security LLC 2021

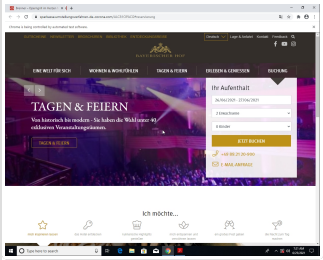
Windows Analysis Report https://sparkasse.umstellung…

Overview

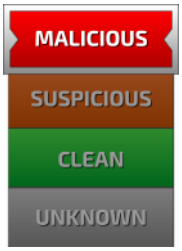
General Information

Sample URL:	http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG
Analysis ID:	440305
Infos:	

Most interesting Screenshot:



Detection

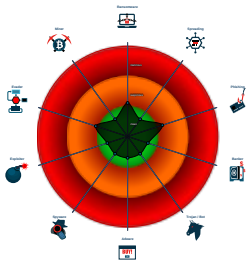


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Drops files with a non-matching file e…
- Form action URLs do not match mai…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5144 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6152 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,12754223477804659990,14032383889391973514,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7576 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1564,12754223477804659990,14032383889391973514,131072 --lang=en-GB --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3624 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - AcroRd32.exe (PID: 4176 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Downloads\PfifferlingeMittags.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - AcroRd32.exe (PID: 7764 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Downloads\PfifferlingeMittags.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - RdrCEF.exe (PID: 7776 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 7880 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,412468737400131831 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14220142155135163333 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=14220142155135163333 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6864 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1692,238294790207997486,412468737400131831 1,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9558252731115271562 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6528 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,412468737400131831 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15100887731048530030 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=15100887731048530030 --renderer-client-id=4 --mojo-platform-channel-handle=1824 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 4204 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,412468737400131831 1,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1029686541791480953 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1029686541791480953 --renderer-client-id=5 --mojo-platform-channel-handle=1984 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

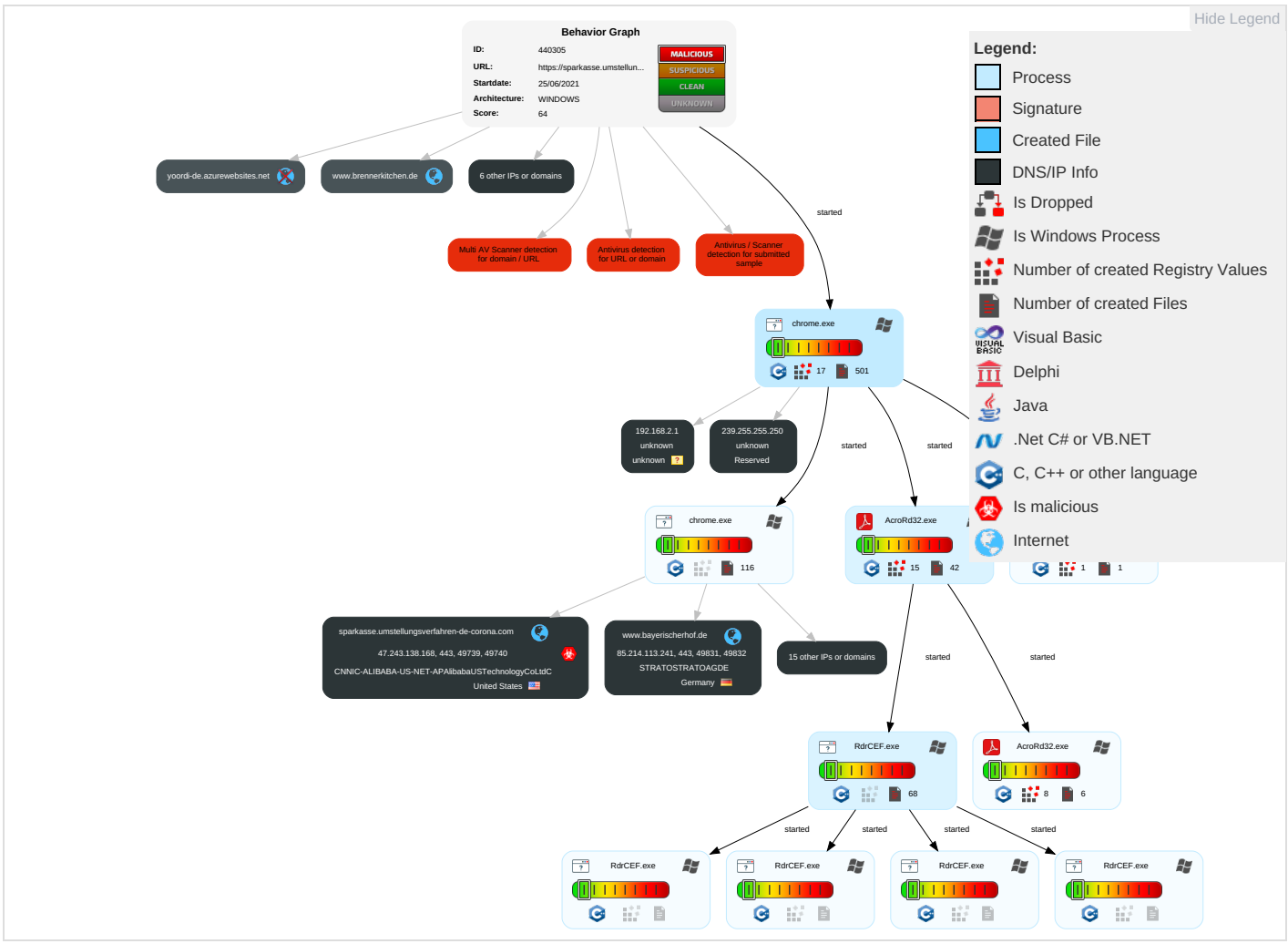
Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
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	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

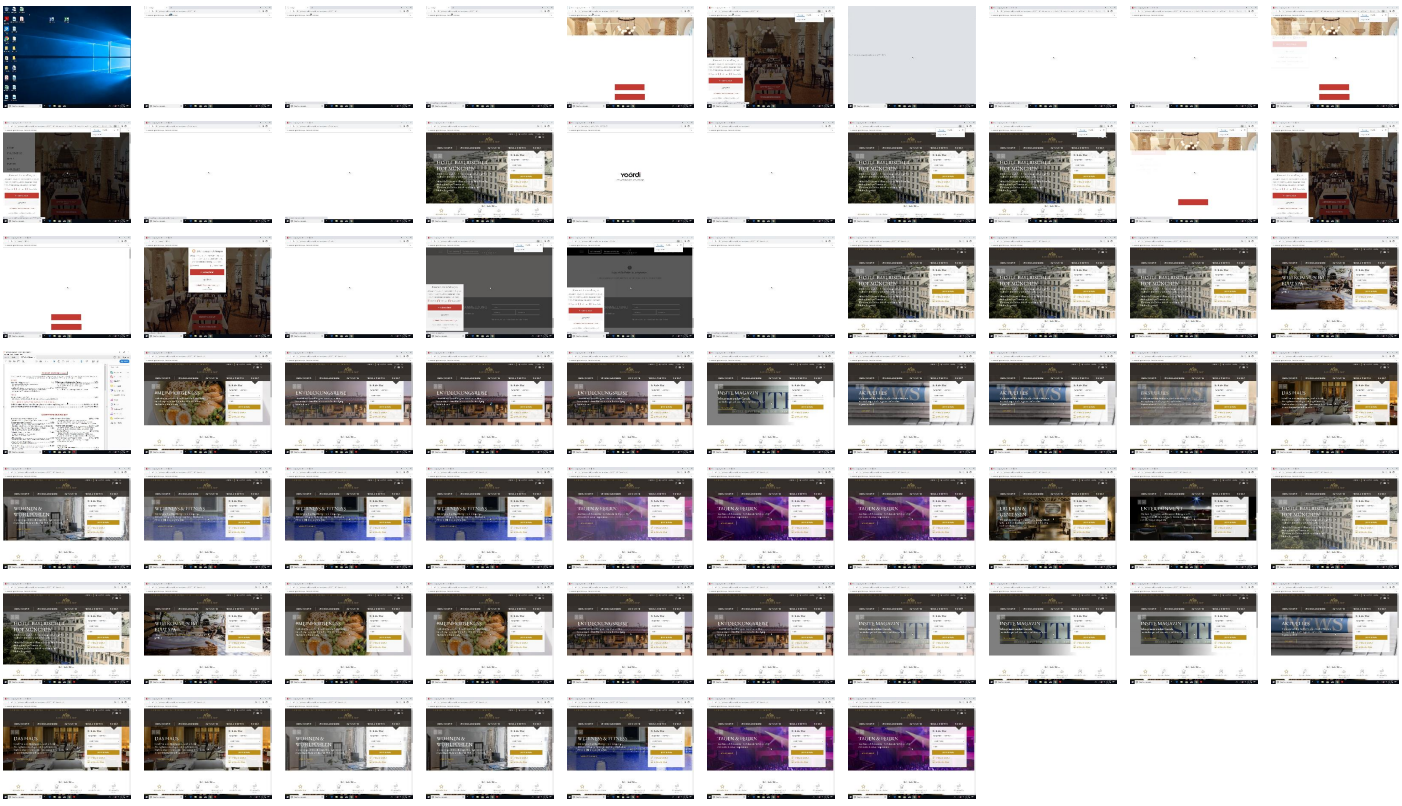
Behavior Graph

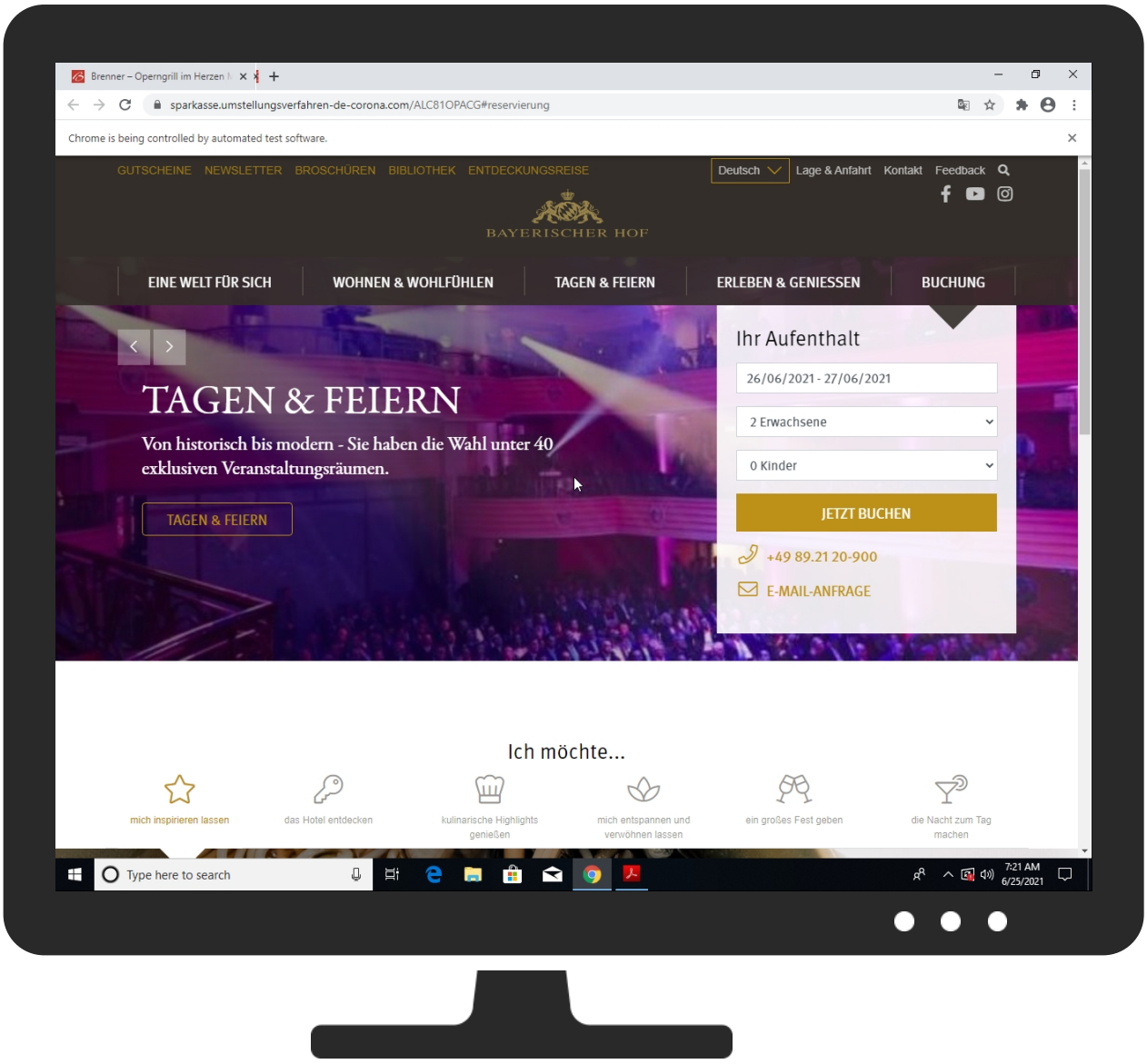


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG	2%	Virustotal		Browse
http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sparkasse.umstellungsverfahren-de-corona.com	9%	Virustotal		Browse
www.brennergrill.de	0%	Virustotal		Browse
de.yoordi.app	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://sparkasse.umstellungsverfahren-de-corona.com/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://sparkasse.umstellungsverfahren-de-corona.com/#reservierungHotel	100%	Avira URL Cloud	phishing	
http://https://umstellungsverfahren-de-corona.com/4	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/borlabs-cookie/javascript/borlabs-cookie.min.js?ver=2	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/transparent.png)	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACGBrenner	100%	Avira URL Cloud	phishing	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/B	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/themes/astra/assets/js/minified/style.min.js?ver=3.4.0aD	0%	Avira URL Cloud	safe	
http://https://www.brennerkitchen.de	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/N	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_567d14d950f17f259f65c	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com/2Hotel	100%	Avira URL Cloud	phishing	
http://https://www.brennergrill.de/wp-includes/js/wp-embed.min.js?ver=5.7.2	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/K	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/jquery/ui/core.min.js?ver=1.12.1	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.2.4	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com/#karteBrenner	100%	Avira URL Cloud	phishing	
http://https://umstellungsverfahren-de-corona.com/	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACGU	100%	Avira URL Cloud	phishing	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.2.4a	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/themes/astra/assets/js/minified/style.min.js?ver=3.4.0	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/imagesloaded.min.js?ver=4.1.4aD	0%	Avira URL Cloud	safe	
http://maps.gstatic.cn/mapfiles/api-3/images/mapcnt6_hdpi.png	0%	Avira URL Cloud	safe	
http://https://brennergrill.de/6V	0%	Avira URL Cloud	safe	
http://https://brennergrill.de/%d	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=3.2.2a	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/l	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/m	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/js/webpack-pro.runtime.min.js?ve	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com/#kartet	100%	Avira URL Cloud	phishing	
http://https://yoordi.app/S	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/MittagskarteFri	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/Brenner	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app/37/37f2bd57525d8d73dbcd66.js	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/imagesloaded.min.js?ver=4.1.4a	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2aD	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app/che/chef2bd57525d8d73dbcd66.js	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://https://brennergrill.de/l	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/Mittagskarte	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app/vendors~CARD10~CARD2~CARD3~CARD4~CARD5~CARD6~CARD_1~DEMO~DINEIN~HOME~PICKUP~PR	0%	Avira URL Cloud	safe	
http://https://brennergrill.de/m	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://brennergrill.de/r	0%	Avira URL Cloud	safe	
http://https://yoordi.app/r	0%	Avira URL Cloud	safe	
http://https://yoordi.app/	0%	Avira URL Cloud	safe	
http://https://de.yoordi.app/36/36f2bd57525d8d73dbcd66.js	0%	Avira URL Cloud	safe	
http://https://sparkasse.umstellungsverfahren-de-corona.com	100%	Avira URL Cloud	phishing	
http://https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_a7ce780949735c20349e4	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_d013db1583b49aa8be633	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.brennergrill.de/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.2.4aD	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/)	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-includes/js/wp-embed.min.js?ver=5.7.2aD	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/borlabs-cookie/javascript/borlabs-cookie-prioritize.m	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=3.2.2	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/en/Brenner	0%	Avira URL Cloud	safe	
http://https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=3.2.2aD	0%	Avira URL Cloud	safe	
http://https://umstellungsverfahren-de-corona.com/0Q	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.brennerkitchen.de	217.31.83.134	true	false		unknown
www.bayerischerhof.de	85.214.113.241	true	false		high
sparkasse.umstellungsverfahren-de-corona.com	47.243.138.168	true	true	• 9%, Virustotal, Browse	unknown
www.brennergrill.de	217.31.83.134	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.74.193	true	false		high
scontent-ham3-1.cdninstagram.com	157.240.210.63	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
consentcdn.cookiebot.com	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
de.yoordi.app	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
consent.cookiebot.com	unknown	unknown	false		high
ka-p.fontawesome.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://de.yoordi.app/tkaway/brenner3/	true		unknown
http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG#elementor-action%3Aaction%3Dpopup%3Aopen%26settings%3DeyJpZCI6NTcwLCJ0b2dnbGUiOnRydWV9	true		unknown
http://https://www.brennergrill.de/	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.74.193	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
47.243.138.168	sparkasse.umstellungsverfahren-de-corona.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
217.31.83.134	www.brennerkitchen.de	Germany		29140	HOSTSERVER-ASHostserverGmbHDE	false
157.240.210.63	scontent-ham3-1.cdninstagram.com	United States		32934	FACEBOOKUS	false
85.214.113.241	www.bayerischerhof.de	Germany		6724	STRATOSTRATOAGDE	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	440305
Start date:	25.06.2021
Start time:	07:17:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.win@63/354@19/9
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG#elementor-action%3Aaction%3Dpopup%3Aopen%26settings%3DeyJpZCI6NTcwLCJ0b2dnbGUiOnRydWV9 • Browse: https://sparkasse.umstellungsverfahren-de-corona.com/#reservierung • Browse: https://de.yoordi.app/checkin/4803721994206769 • Browse: https://sparkasse.umstellungsverfahren-de-corona.com/ • Browse: https://www.brennergrill.de/ • Browse: https://www.brennergrill.de/en/ • Browse: https://sparkasse.umstellungsverfahren-de-corona.com/#karte • Browse: https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG#reservierung • Browse: https://www.brennergrill.de/Mittagskarte • Found PDF document
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:19:05	API Interceptor	1x Sleep call for process: chrome.exe modified
07:19:56	API Interceptor	10x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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):	410
Entropy (8bit):	5.684182577625305
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Qda6xqi7Z+P41TK6ttf2en9YOFLvEWdM9Q9lJFHi7Z+P41TK6C:vDRM9SayZiEvffDRM9u5eZiEHS
MD5:	307A12B7DA7B14D696349958F16ED00B
SHA1:	86CAF9D9693C0A3D5B1332D3C0D45642C409D56F
SHA-256:	2974C1D4B3E5BCD47B89E8821B11729C18ED8407E9A9DF436D2BCF4FFD1E5AE0
SHA-512:	AE610E152B13990690175AC11379796A40A8FF0E270ABD6742B1D1172556C46A64D465A7BDBB141DF3A68260F66FE27FED1585E805F1516B6DE7B5A98F63BE67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..?..&$/....."#.D....Y5.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... .3.U.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .PY..&$/....."#.D.qk.Y5.A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .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):	348
Entropy (8bit):	5.6158006335097905
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEky5V+Ci8Be7Ywcr1TK6tY+i9NqEYOFLvEk9ER0/tIQCi8Be7Ywct:V9zGRi9PQG99zvDCi9PQ
MD5:	68EE2742411801436ABFDD71080E5FBA
SHA1:	CDC3FF522E77DE200DBE3D06F5D9206C0E76A9AF
SHA-256:	EA27C46AEA21CACC3D7239207BF15276394367FCD7321E3F6D8CF7A682AED012
SHA-512:	6230BAD5524B041F6240F6CA712C4CC2243D80107FF0069E51385ACB5D96C63AD5518591BDA71B412D93E558E6E2454C2DF95A9C8A64145D8C035186B6784EB4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..<..&$/....."#.D.b..Y5.A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....6.\.....0\r..m.....,....._keyh ttps://rna-resource.acrobat.com/init.js ....&$/....."#.D.D..Y5.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....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):	492
Entropy (8bit):	5.628360086723457
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAF+gT2plUo6jHbyeRVFAFjVFAFMIG8plUo6jD:tB4v4fESBFB4v4NSB

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
MD5:	FD9E66C7C69DB5B477F1418DC164A863
SHA1:	7F38F50C696DDC1050C2B354BDB5AFDD575C668C
SHA-256:	3D79133A995AD6C3CB3F94CE8F68997A6BA5E4AD9AACD48138CDF438C9B75BFE
SHA-512:	2264D9AC7D0A16096EB0D4C2E30FA315331A8383FDE5E551BE44AE0C8E9D6F2CC13F33A564070355B71AE2815F792842B5536C6D936A4D0F5E916F21B45B0DE
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 .....&$/....."#.D....Y5.A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo.....ap.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view /selector.js ..`..&$/....."#.D.,i.Y5.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....P.....

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):	5.654245396048644
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsVciWulHyA1TK6taE:IbRkiDQNWussf
MD5:	7EE58EB37CB03B5E6FD4D4252543E2D0
SHA1:	33B3F2974D4D416FA728AFFF3493CF725710DE70
SHA-256:	E0F74B7807238C97582F3A767F0D2549B1B6E25A658A3D49B1E9D12D4E8E9679
SHA-512:	A4A69E2D784DBA0406FF45DE42FE9183B863533A54764D238CB1D2A428800D783DEFC8B54CBB0FDE4242F84503C1482558E468457F26E06C8FD03504A2E07BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..g..&$/....."#.D....Y5.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....dKR.....

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):	420
Entropy (8bit):	5.584365801459596
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuKpyWomUVyh9PT41TK6tY7f2+yiXYOFLvEWd7VIGXVu3l:pyixRu/WKV41TEoyixRuB6V41TE0
MD5:	7CAD2351FF815B7082E9511B248484B9
SHA1:	EA9F81447DD0384CE6161F3DAA1A07AA9B80DC08
SHA-256:	9A9AEE0B40411EDF03AC2E6D561BF0872DA4CFD16B36768A0724C29DDF1667C8
SHA-512:	4104F8413C2C1E72A0FDD0F1E1C55156DE497F08A5F6ADB9F94482EE866A3071F4D2A41D94024BE7825A785410DD0426288C11C3BA4E388E252228C4D324E8DF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....&$/....."#.D....Y5.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....&$/....."#.D.ej.Y5.Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....rE.....

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):	432
Entropy (8bit):	5.68759749958015
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQaZHbNLZIl6P41TK6t/8vYOFLvEWdhwjQh+C4BkNLZIl6P41TKa:0RhkR7NLZCYRhktxWNLZCL
MD5:	7F6EA41D7CB137C32D100A24A1747C88
SHA1:	EE4EC5D75792DC829CED50C367A1D9A55EA962A4
SHA-256:	8C597D9A4E7D4379F2FCF7CA3D227C759552613531643775A4078BD4949C0ACD
SHA-512:	EAC2D5C9BD3428F8E051603217081826A21F5A1163FCD51284A0B1AD695EE9DC0C7F1D03F81A4BE1B521BCC02201A2E089AD10AC7C9C14D848478A08E343CC 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..q.&$/....."#.D....Y5.A.].>....uUf..N...k.....c..l.A..Eo.....A. .Eo.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .HP..&$/....."#.D..Q.Y5.A.].>....uUf..N...k.....c..l.A..E o.....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):	418
Entropy (8bit):	5.610728489682451
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQjB86g1TK6tltMJYOFLvEWdGQRQOdQT416g1TK6t8F:2RHRQCoB81eORHRQCj1
MD5:	490F4535CDE197B404308706AC0A19D1
SHA1:	5E10955F136A5404A1A2E621C26AB8A13B478077
SHA-256:	65D2E3C694909A3242045B7F789CC4720A64CAEB0C141C07B3C309AF31463DB2
SHA-512:	3F0731DDF57BD035483F68DB1EDE25FD572E3AA6495A500BC69B4252607ADF3E885E31F4352F02B308FF132C8B06F29DCA672CB55742695D1CC9DA7593CC848
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .....&$/....."#.D.;..Y5.A..c..y/L....\|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....`.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .....&$/....."#.D..j.Y5.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo..... .....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):	358
Entropy (8bit):	5.627570883326144
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLS2Qls5MuR/41TK6tpSEOYOFLvECMLJad5MuR/41TK6tNN:Z5Mx5MuR/Ek5MNa5MuR/E
MD5:	B875C442FDAE1ACDB4B369F0A3E1D061
SHA1:	9B2D083B8C1BBE28D16F42807B5B79ED3909824A
SHA-256:	2010BA4DE3CE90F8D5917562A7B7040A08510FD58C062C5035D9F2E7AB104C4A
SHA-512:	36FC6A3CB25C127BD876D04798CC4820018C6758A37A17B29049FA706D2144F7C466E10228187E078768A39011F910EBF7FB2EAF36F35D6E8FD7BCBB763B64F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..B..&$/....."#.D....Y5.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....L@.....0\r..m..... .3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .....&$/....."#.D.]..Y5.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....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):	428
Entropy (8bit):	5.561203840072624
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtu1c0lYsgMby0zBUKSAA1TK6tp4fPYOFLvEWdtuklR39gMby0zBU:pRslYBMbeoRLnCMbev
MD5:	C5E869FB32CEACAED41BF12690091913
SHA1:	8E82136CF7849B35B3BABD008A8F7621D2D6380C
SHA-256:	0CE4856C5F9E1FB93BFEF0FB283985288EFF8ED46EF31DBA16462910B94FEC1D
SHA-512:	395E8693CF47FC027D7CDE62A1C335A53D9CC56A3477278419E33BD619CD4802938B1051187EFA83ED9A7B8E6694AA71C8E5B3C781E78CF6CB5AD6AEC33D88 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .....&$/....."#.Da...Y5.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....&$/....."#.D..i.Y5.AQ..E.=....=h`t..t..3%A.F$. .w..A..Eo.....A..Eo.....A.....

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):	354
Entropy (8bit):	5.599862600142339
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFvc35xcvtUdyP41TK6tbHed4HXXYOFLvEjMSWFvgxItkvtUH:KkXxKMSCvUxotUl1ikXxKMSCvgx3tUlR
MD5:	C8A7A4BBD9266A73F63CA18C4DD940DE
SHA1:	C9732BEB536F8EA8938E3A319529648B624A8A94
SHA-256:	6E63AC6232C40ECD7E1D1C4CED0A462237934276548A8C600781C87EA4E6EA4C

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
SHA-512:	84FBAEE1DD5CFD6464D21523F8A6C2C1F428A4A4FA40C48F4A4C86BDBDDC99EC704ECEE9D51F671D8144B140B01E514BC04A791F92A77CB331B86B91C1F18D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..?..&$/....."#.D....Y5.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....3.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .'...&$/....."#.D.V..Y5.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....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):	374
Entropy (8bit):	5.617764896824281
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL1EYhyM+VY1TK6tFTkl9YOFLvEWsfOLNBKQ9qyM+VY1TK6tft:5h6OL13MkQh6OLiQdk7
MD5:	D22F2299DFF4AAD8D7369B7FDE5AC48D
SHA1:	A8622AF083CA674A5CECE4739FA2454599BFA6B0
SHA-256:	A7417ED13E9FE9F3A37EED1FBD5E246C3183F17CBBF799B3DCF6A43FC24D64D3
SHA-512:	373950B6036C5B6E6C06066545F65FDC86CC45669EFFCE163C3DA5F82768BD1CEB300FD3668B6D0AC3B738E5B970A516120AE4101E517A3787C72F16561BBDB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....&$/....."#.D.@.Y5.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....Jx.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....&$/....."#.D..B.Y5.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....N2.....

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):	488
Entropy (8bit):	5.631212433896695
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFo+wSeKaTLniRVFAFjVFAFAKwSeKaTLng:UB4v4RwzXLniB4v4RwzXLng
MD5:	BF4BFD63DD9AB5B800D1129F7F506834
SHA1:	F383E2D6E8523BBDF270B3E60C9BCDB2916AC3EC
SHA-256:	9261855D1EBAF428D6441F356BB4B2114AEC2134888A3130D0C87CE545B93E71
SHA-512:	A73DAB44A73940C3ECD9C5D7B34F8B106FABD935E77F7A6A3E30328F07AB72AE7C49FC39773EFCC542FAA6691EB0399FC4A980359681B6B65E2A3B0087E83F36
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ....&$/....."#.D....Y5.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....m.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .....&$/....."#.D..o.Y5.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....B).....

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):	422
Entropy (8bit):	5.561039345945517
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuV4q9WY11TK6tf2s2VYOFLvEWdvBIEGdeXucaMY11TKn:BsR2EseersR2EsejW
MD5:	B3F46E0F341CE14D22ECAD7691AB0288
SHA1:	DA81CB10198052388A2A78062D2A217FEF04AAAB
SHA-256:	1204122EEEF060689819B005863F0ABE5165955E29650BC8DC5392AC3015EB35
SHA-512:	92A554686D504967D88560F9A984D207F91976EC907448A113D5273F58B0C2D49DCCAD3A3E92D133D4EA7766EEC71883F896B914F08027A3FB0A695A5DF3927B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .....&$/....."#.D...Y5.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .S...&$/....."#.D.sh.Y5.A.A.o]@r..Q.....<w.....].n\....A..Eo.....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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.690310535308977
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQRi98o44B7OhKlvA1TK6tz+aVYOFLvEWdwAPCQrrY4B7OhKlc:RbR16YK8o1BJkRpbR16cBJkV
MD5:	848541A8E5F3911FBD281089F8BF1CA3
SHA1:	61AE1CE1BB80BBC1AD9BE260FCD5BF7841B491C2
SHA-256:	48891ACE963B7F6E15FCBE299C6A5FDA84BDFC06426DA30612F84B253CBF39EB
SHA-512:	A6B3076CBF9FBC6A57DF48B85DD267E38EB2E6CFF003D926402A037A7BAA8CC8EA9B6BBCF947F4D02030684587C5A0E3EB3E5B54F52967A5414D8AC7C001A688
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .uk.&$/....."#.D.U..Y5.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....t.....0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .=...&$/....."#.D;SQ.Y5.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....7.....

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):	422
Entropy (8bit):	5.628620682054164
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVumVUQdFt1TK6tkks2gEYOFLvEWdGQRQVuA5ZgQdFt1TK6t:B2geRHRQPU0g2geRHRQng0
MD5:	BF12852199A023278CCAFD38F419F792
SHA1:	307671423CC0B381D4592B6B37BC2A7DA1C927DD
SHA-256:	28D71EFA5515F8CF23FBF7F18191D7D45D452A8AC68CB760E22A14E3A0C3B4DF
SHA-512:	71E13B58E370F3A0E288323DA08476876D9293AD6EE7F7AB1C39C6533706660B786D2489FF4A924A465CBD83C0BB5E2C0702ED40FD2D4DB9E31ECE75B3F2F36
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .....&$/....."#.D...Y5.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .....&$/....."#.De.i.Y5.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....F..w.....

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):	412
Entropy (8bit):	5.5939302778222855
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQmtt1S/1TK6tp+zyEYOFLvEWdrIOQdtKtzt1S/1TK6tUl:WyeRlnt1wayeRlO4Rt1w
MD5:	888FE32DA65B65FED4F02BA5FED4C410
SHA1:	04E740E8DE21BAF1F8EEC6BD0DCAA2F1C2DAC115
SHA-256:	F915147F6306FD489D18E1ED61B2C36D0BEB37FA726AFF640010F4754012EE0B
SHA-512:	AA442C0126D5E266689330BB8D8C33AF3271D485C0883768F5407CC3977BC4AE11E58FE62225B186CAA1CCB727DAA4C0D6A11FB04A45E7133B5525907F39445
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .u%.&$/....."#.Di.x.Y5.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....j.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..n..&$/....."#.D_.H.Y5.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.....u.....

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):	436
Entropy (8bit):	5.615183318603996
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyuo6rqwK+41TK6t/2nYOFLvEWdhwyuwrurqwK+41TK6t9l:wRhDwK+EVgRhlNwK+Er
MD5:	540BB6002FB83E4A74992BDF7F26B328
SHA1:	110EB03FD8D50BB8509E17769F7F5AF6D3E25AE6
SHA-256:	D9F04A2979699DD7101FEC85AECA31A8927E86E0797E73619B1D6D0BD04728A7
SHA-512:	7D647677EF3A549432FD60DBAABF68B511CD98743F030869E9F5139AD4C3BFB38DDC725941D94DCD18505EB5BA95B73E1F0B333BEA818238518180419F0CC0F

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ..y.&$/....."#.DM...Y5.A.....7...o..a=.98I.....(3.$G.A..Eo..... ..A..Eo.....G.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .h...&$/....."#.D..Q.Y5.A.....7...o..a=.98I.....(3 .$G.A..Eo.....A..Eo.....C.....

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):	460
Entropy (8bit):	5.667132050494533
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbu8IZfO441TK6tQeYXYOFLvEWdrROk/RJbuUocrfO441TD:/RrROk/1mfLE6RrROk/N3fLE
MD5:	3CDFD214CC01FC736813C8B7765FACA9
SHA1:	589F589117D6DD7C2BADF75340B71AD051049844
SHA-256:	58673604E2E3623E8FBA190CF68215B47B627A730DF7B3B1AC29812E0448D33E
SHA-512:	9F1B5569F13218E7937CFCCF033C92613812D74670DF1C4D2BA66411325D71627261FFEA370D5E894C8E792AABF3E5709054565A4DFE3C92934D9A1EDA1D47A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....&$/....."#.D..x.Y5.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....,".....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..'..&$/....."#.D{.H.Y5.A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....N7.....

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):	372
Entropy (8bit):	5.6187051801370895
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIn/4s1QPLr1TK6tGd/EmDEYOFLvEWXIka/q2K1QPLr1TK6t6f:xqTCQsCPLnIdTqTGcCPLn0
MD5:	9B968A459AD6165CAEC5CDD997631D29
SHA1:	029F1DC55B8EDE8B9715C6133669AAC1605B35FF
SHA-256:	B01D5B865E86102C1EB9E167B57C4A192B3DBFA4BE38945356A72DD620A3989C
SHA-512:	B1A0C8F533767E4342EB13FE0DC4F38C03342C7B9BB82D52D36098E8B50AB7EEC60E38394F4D6957D755D250953D4AFCE4048A4FE523891575531E5A642873BF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ..{.&$/....."#.D..?.Y5.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....>.....0\r..m.....:.. ..f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....&$/....."#.DQ.A.Y5.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....sN.....

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):	414
Entropy (8bit):	5.6354505665092605
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuk6PpsEJ41TK6txu/E52YOFLvEWdMAuMNtmsEJ41TK6tML:zRMO6RsDzupRMyN8sD
MD5:	71926840BE3943656DC98617C91BFC27
SHA1:	D567E68F2098F047255383409DBD854FC8D974D5
SHA-256:	77B1E2BBD4147DA78F5BB099B8DCAAF4C24E4CEC9ED37665AC38C6C5B39350FB
SHA-512:	A9CEB0909F0E50FC1FAF77D926A32A0B2A946FDBA748C648166710C12F8B9BB955FAED0AD082BF798DC4B393C8F4A918A60B1BA6A026EB831FE1580A587DDD AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....&$/....."#.D....Y5.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo..... {.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .i...&$/....."#.Dr1j.Y5.A..z._a...'.v.....4p3..1.']...A..Eo.....A.. Eo.....87.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Size (bytes):	420
Entropy (8bit):	5.607807633251473
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuGzBgFong1TK6tp5YilPYOFLvEWd8CAdAuFDWOogBgFony:6lJR5gFoMfrlJRTOogBgFoM
MD5:	845B7E7214AD8E0296DD67BF673D7334
SHA1:	70CFEB0B1A1EC55A78E0EA560BF11EE58640C007
SHA-256:	92A1500A4F6308DDEF94A6EB6F3294487CFA2D41D0DA0174968F8CFEE344DA9B
SHA-512:	1587069C11007E5640D9E6F2EF7DFF64A16F66F2C01D4B6BB50015570329A4808459A99249DF90B59A5CC9FE4CBA75DD8F7CB576690BF399E925E87013A72ACB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .u...&$/....."#.D/...Y5.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....s.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .....&$/....."#.D.Fj.Y5.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....X.....

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):	446
Entropy (8bit):	5.627268612279976
Encrypted:	false
SSDEEP:	12:F8hRrROk/1QfOe2g8hRrROk/ZQPOe2vdl:UPJ/WF2pPJ/Zq2
MD5:	148FF89A7DB4CFC954C751D589544C51
SHA1:	7CB790A4E66138B6569C6F63EB2110240DBE6ECC
SHA-256:	F3DD6C99FBBF58664D0A6E4F3DF54CA53BE3B2DED1A586D68738619DCEBB73ED
SHA-512:	003EDA8E9CAE1697EBBC3DA9B51E721B5420C2DEA69E31BC706B5602AE1DEBF0FEE0E144E0B60B798907E68421B23BF9890E139A8A068F220CD1E7D7C2822C31
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....&$/....."#.D..x.Y5.A..%.k.SZ..~W.....}'B..ad.....A..Eo.....A..Eo.....s.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .<...&$/....."#.D.xH.Y5.A..%.k.SZ..~W.....}'B..ad.....A..Eo.....A..Eo.....k.~H.....

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):	426
Entropy (8bit):	5.686807257048936
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQIQlRrNJIi1TK6trh2LrnYOFLvEWdrIoJUQGu6LirNJIi13:ehRcvQlRrNJIC/uhRc9hLirNJIC
MD5:	657E9834E03953DFBFE7BACEC2A64F1F
SHA1:	7A16E80AE4CA198C1589CB0A537EF1DFDDA1444A
SHA-256:	DFC9F1B53FD3B96961CF6EEDBF12CB7F8EE84F7D2E66F11D3FB98CC0300D052D
SHA-512:	516AFD81A0CF79D1B9C61BF3BC575B3FCFD08203B03331C671094AFC3C8640F05D136E3C79D4CCEE2455378684203B78C098D63386770E1007EFBC19D59D71E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..(.&$/....."#.DC.y.Y5.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..q..&$/....."#.D..H.Y5.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....o.....

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):	416
Entropy (8bit):	5.631404686190018
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuZXBaI+KiZLzgm2d/1TK6t+8OEYOFLvEWdrIhu2VZLzgm2d/1g:0Rz/iRReoSR2RRe2
MD5:	339C084BFC1222657F4B654656AEFA1F
SHA1:	FD1D53348E5CD6ADD9E7428EBCA66003F47FEF5A
SHA-256:	B952ACB822A7FABAA2CE2017CE77696EE30C929748D03815EB085FC0B49EE0CE
SHA-512:	DED6B27E201CA15DD0610A64F83F9201BEFBB01E85231B6FD9C62C35238F105597E7AB16C9F346226E01AFC65E9A54C489429EDDA270CE7B7DCAD89B31C7CD73

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ....&$/....."#.D..v.Y5.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....oL.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....&$/....."#.D.GH.Y5.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....w[.....

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):	376
Entropy (8bit):	5.6345542280514636
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kp0ljW2kx56uvp1TK6tSAElVYOFLvEW1K+lOkx56uvp1TK6tu:6JJKiy9cJJKow
MD5:	1C3223050E55DECA8916F664F64BFDE9
SHA1:	C8732A0538E3933954E8FBCDA9C0C2C17EF7408E
SHA-256:	EA7EA054C8A1CBC707D88BE9B37DF64D423D6CFC833991511BDA05B7EA66541A
SHA-512:	8C8DF7E9D9B719A84CA0F28F2CB7F07860DF8E07233404C35E25E0AD58A93CE464478AD4251A439831E8E4CEC8D9F5253F1EA7F74CA4D8EDC6885CE1BDAE4583
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .\...&$/....."#.D...Y5.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....y.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .U)..&$/....."#.D.|'.Y5.Az?...SwC...^..y.....V..7R-O.....A..Eo.....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):	428
Entropy (8bit):	5.698169226643751
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuJkCxhUDLYtmOZn1TK6tV2WYOFLvEWdBJvvufLjEhUDLYtmOZ5:xRBJekCUDcFZLDBRBJcBDcFZL
MD5:	F6DE39F073D7405BDB8DFE5460711214
SHA1:	281FF57280D8BDC07BB9C3FC4BB26A571F3AB763
SHA-256:	EA60F2FBE91191201A11E33571D43F5C66CE9F02ED8B34F4F1BAC1D0C6C1281C
SHA-512:	25DCA6683958850B40F504AB699771609547A716B69242DDBB7E8B220AAB92D31AF138A6CF0FE92496EFA04A73619E729356630E54F89DF67B4142D1C635CE51
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .R...&$/....."#.D@...Y5.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....9K.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .....&$/....."#.DD.i.Y5.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....OR.....

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):	422
Entropy (8bit):	5.6246806267718235
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7dQHVPu1TK6tzAMsRPYOFLvEWIa7zp7SDUSVPu1TK6tl:BPHLackPHsDLcX
MD5:	1B33804B509904C2A25ADFDE72908CC5
SHA1:	D890356F08C708AD92F3862756F75C6E02DB224D
SHA-256:	E5993787C47ECCBE46180738C0AB29F2FACE26BAC8EF494EE9078B2306112D9C
SHA-512:	1DFE89EC682320AC8975D17443FFD9F0FFAA4B6AF663829B9C522942C5AB137DB87BFC9F4C9BB02F6905DE0148D202C48C93BF487AF812BD52A4201992C2E43
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .7...&$/....."#.Dm...Y5.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....C.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ....&$/....."#.D...Y5.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....oMe.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Size (bytes):	416
Entropy (8bit):	5.629790905400065
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QTMkwiM3Y1TK6tcKPYOFLvEWdENU9Q3Y1PwiM3Y1TK6t:bJRT9owr0rJRT9Zwr0
MD5:	6A3DD8A9A2E449409329FBC1FDCB0C72
SHA1:	F9E648F3DD99D60955673629AF8ED3FECE0E06B5
SHA-256:	2AA186C747900CD09C2C4E0F5BDF35CA79AA9DD2C9707DA5D66C1ECA915C3364
SHA-512:	50573CD87F93C15EB3136369AB4D1A9E4B4B3BF43AEAC763D404F932D3EFD810E11447E94289A1D5045AA34FDA6767F3E2592A6EED36095625D39B6EADFF692
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..n.&$/....."#.D...Y5.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo..... ..A..Eo.....@.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js ..B..&$/....."#.Di.V.Y5.A...M....m+lS..e.....<7.U.P8 *.0K.A..Eo.....A..Eo.....t<.....

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):	416
Entropy (8bit):	5.6401008731163795
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQW2RgQRjBRCh/41TK6tkNMQt6EYOFLvEWdccAHQmY/rqSRZ:XRc9o+QDi/ECRc9ZYvDi/EXL
MD5:	B23B8715225DE98347BDBFCF131DDEF2
SHA1:	359AE68F55D2CE650227A949F727050CDD15D5CC
SHA-256:	95FD4698A989995237E36DFDCAE6CDA63C7050EF56375BD573B3340EB05091A9
SHA-512:	9B554BB612CA364E7DD31D122CD09FEB85E2689AE79809A3DEC3FBAF57B094E1CE91D647E3E1E928E00852BEEFA1D4B05D59895C3B4211A222B12ABA56DDD E9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....&$/....."#.D.H..Y5.APJm...0x.x..RD...BB!@5..<..]....A..Eo..... ....A..Eo.....l.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....&$/....."#.D.{u.Y5.APJm...0x.x..RD...BB!@5..<..]....A.. Eo.....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):	5.57292221469655
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuPLu1y9VULlF4r1TK6tdX:bs6xRkixiLlF4nT
MD5:	C4E8CB855A11478F1E529BC50BF3B8C7
SHA1:	E9C02CF702F600FF5C32D19625DD647BC31139C4
SHA-256:	9CA1CBF779E274664F8E457B8C2D1A01D66189B7A9CB60310BDF70B9CD628640
SHA-512:	D5567D620F9ECAA2509A5FF1C238889C4CB0D1D5183692D1F65CBFA014DC40EC3E1196B878D8ADB7F0CDEC552DC26BB0626D37A62D61A32EF9005833EA95A 36
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..y.&$/....."#.D....Y5.A.P...#4..l....5...5..).w.. .h. ~..A..Eo.....A..Eo.....p.....

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):	430
Entropy (8bit):	5.503873249970856
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFus/rE5N941TK6tmHehYOFLvEWd/aFuR4u4n9N941TK6tvW/:WRy/rE/9EZRAbr9EQ
MD5:	52A892B6E64028B3345C22CD310F5127
SHA1:	74A254D5F5BCC16D3750D157CFD5CF481DE79B70
SHA-256:	CAE5DAB7EBD990E548D31B58A312AC8F4CFC72258F91E9C26E641AF73B57DF5A
SHA-512:	41AA0651995E03652E9B80E47CB8A566B8B3897AB5441A4217B95B5530E1F3E3DBF490E7B4B56075B822880A2671CC60DA01ABBA7B978454CE64F5D6E55C5220
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .b...&$/....."#.D....Y5.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....e.*.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .....&$/....."#.D._i.Y5.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....e./.....

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):	416
Entropy (8bit):	5.565045372822308
Encrypted:	false
SSDEEP:	12:2DRuRnPAUk5pB9Vd2k34DRuRb0B9Vd2kjl:8WPU5vbdTOi4bdT
MD5:	8BF4E896BC3B8353930793E88FE4134B
SHA1:	DB6E17552855EC7DD6E1509712D8D2A3D1D867D7
SHA-256:	ED23F6BF090A8E9D6027F0D4AC78A0143D7B70E3E399ECE6517EFA705A2FCE0A
SHA-512:	911B1E4A7242484383FBED7129192CA02742C4AB8AEDC4ED34651517F62B7D9828928BA58515E303ECA1988FE5DE2F4FCD6F0C453753E1B16E4A3A7AE7BD40C7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .&...&$/....."#.D....Y5.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....]........0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .....&$/....."#.DG.h.Y5.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....X.....

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):	416
Entropy (8bit):	5.61794846727279
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QgaRuA424r1TK6t72kqYOFLvEWd8CAd9QBacuuA424r1TK6/:+RQvaIrnwRQM9rn
MD5:	BDB3AD7CACE66FB11345CAABDA897432
SHA1:	554A9D53E96199CEDC1B224776F11EF86C108F03
SHA-256:	C57DDD20D55ABB1BB85BB8037D74043374FD6E33339FABD3B6D66181662EEC50
SHA-512:	2C4C64E4C5F29550B565879798CA95C03C1F28E28A7B4B4185FEED6BFB2DB0408721E7BA310D53BEC5A2AF2C8096CE8FDCF76B8D28D73410B1744005226019C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....&$/....."#.D....Y5.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....=Q.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..a..&$/....."#.Dq.m.Y5.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....T.0.....

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):	420
Entropy (8bit):	5.620426271533032
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAut+Kro/yC8n1TK6thPHlEoXXYOFLvEWdENUAuxKRyC8n1TKV:xhRT2l/7QnfZhRTg7QS
MD5:	32D07AD0FBBC2D75C0E173E7556AFEB0
SHA1:	BDE3BF523F5F3F826F5704883E6F27A864CF3D5F
SHA-256:	CC07330EEBDE2282F9D1655E4CAF20223A3CA578603CA777B4BED584FE1EFCF7
SHA-512:	69BB601C893AD030993E4A7EC588A5CDA628120EA4362DFBBA61D7108FEE1A82BB1E947F1DE34CA5B987A4B4016837AF0557BDE689D4EC0A8BC3380CAC700509
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..w.&$/....."#.DL...Y5.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....:.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .....&$/....."#.D..P.Y5.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....j.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.668941472782785
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQRIZLM6LmB41TK6thQZYOFLvEWdrROk/VQK/dBBDLmB41TD:nRrROk/VYISmCRrROk/VRB+m
MD5:	B7E707A093FAD1819663E7817060782F
SHA1:	332EF89DDB679D602A0A2F75B3B8B802ADEE4323
SHA-256:	40A58A79A319639E7C65365B4C99ED3408D2EDB3181E1AE6F7046ADD20704281
SHA-512:	8019A21F6433C252550DD9F2066E25903039034E334069F73027D9C7A0FE5C32B679D8D3B567BD6883AAA0E3B181E9477FF66B1F84965FF81B2ED7F84958AD07
Malicious:	false
Reputation:	low
Preview:	0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .;..&$/....."#.D`.z.Y5.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..u..&$/....."#.D=.H.Y5.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....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):	420
Entropy (8bit):	5.6197723857531106
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu7YoAdm9741TK6t/XNMZ/lXYOFLvEWdccAWuqai+Adm9745:qxRc5/Adu7EVyxRctAdu7E
MD5:	07FEE8DF7DF5C630B6BFB5AD3BB5498B
SHA1:	B5BBF04D56E5A89F99D16F06E2F2C70B6AD75A8B
SHA-256:	CEE89F5652AC5581CB1D21A4DBE8A87E38D97475D090A08D17E7CCBB64D440D5
SHA-512:	7EC3C6DD67909245BE8331D1346DE30C519D0D7D99E8BBABD0FBDF18921E7564DDEED24E1946A594F99C41454632B049D6A27673FC1E60FDC32FD052BB80944
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..u..&$/....."#.Dn...Y5.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....YG.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ....&$/....."#.D..i.Y5.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....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):	408
Entropy (8bit):	5.646109998732046
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuHGDmcrQGQcJn1TK6t8HeMOYOFLvEWdwAPVu+aqioxcJn1TKO:2R1i4Lq+R1FKL
MD5:	FF431F2BB3392F85E1B07FC2269F9894
SHA1:	537868543CEACBFF460BB03FEAFEEBA7FB5D806D
SHA-256:	626B517321A153E80060AAF0A1B68A1D5047CA00B88E147252B0874C57081668
SHA-512:	82EAAFDD146B5B6A83086500D14B45B56DC80742CAA9825B525ED3EF116C0DD6EB9B30262B162F00B9C1D401F77C328C82EACCD37AB7E986D7048670101E9CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..X.&$/....."#.D...Y5.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .....&$/....."#.D..P.Y5.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....{HW.....

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):	424
Entropy (8bit):	5.665900139722382
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQEluUGSzhcsBXIh1TK6tEf23PXYOFLvEWdBJvYQA2F5Szhcd:mxRBJQ1vGSDB0fxRBJQ2zSDB03
MD5:	9FB2224F1FC1505B73E28E593A63CB23
SHA1:	5B1AFCB215E8344098EAA199DE98E60DDD8BD397
SHA-256:	B4C3AC294C6CCA07B33FD1F456727D382BD2712E871078480D4F2929A4146AF5

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
SHA-512:	33197A7AD098E28E81B0947623907376A6B8444CCD12E79255AEB9FA414BD3F15EFB2C5AD9B5765F868DB268D9956BCA621838E2D7F25644150D1CB75FD15EB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..7..&$/....."#.D.e..Y5.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..E o.....|..4.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .....&$/....."#.D..i.Y5.A...k..`..N3.... ..d..$[.....{.A..Eo..... .....A..Eo.....k=.....

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):	456
Entropy (8bit):	5.623508532294229
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQ9BLQGDc3Me/1TK6tc9XMsPYOFLvEWdrROk/RJUQUY/3Z:3RrROk/sjGDcm9XVRrROk/sVc
MD5:	483BBEA7204556E8AECCB18CB7DAA727
SHA1:	E6D5EA5D44716F6BAF4D7F0B8BA68A13056F8EC6
SHA-256:	A42EB52726BE9CA0240878530ED2A581789B42069FA268F75A3D75962EB15AAB
SHA-512:	16E504899EAA254036093377623AC4D266703DD8D1417D932265E52827938FBBAE4966418E048B40488D4363E25AD337E6FC81BDCCEB4EEEE84A06292506206A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....&$/....."#.D..{.Y5.A.....9Q].8O.z....=..:.N.{....N{.A ..Eo.....A..Eo.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ..w..&$/....."#.D..I.Y 5.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....erWJ.....

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:	Maple help database
Category:	modified
Size (bytes):	1032
Entropy (8bit):	5.076592387130009
Encrypted:	false
SSDEEP:	24:TYzbPaI+23MQgMto+6rDUUj1JVYlEMc0IwCyh90JnTzEyEvYkIGofiS:T0y/EYrAowG
MD5:	D5B18A5FDDCF4EA26761BA36907668C4
SHA1:	69B97A4753FE04580CF6DC299EEA164287DC6AA5
SHA-256:	E6074184A05F87F8C23D2B8DAF9A1DFC368479F32615A61282ABD0136E7E51F4
SHA-512:	BAFB29F998201723E466BC9DB488D743E9C00B712EAF00D5A2848FB158EE2080A9EC04CDCDD2B36F0A6BBF6A3D840810BFBA502ADFE9CA5C1B13E237D3951573
Malicious:	false
Reputation:	low
Preview:	..... .]oy retne....).....T.....3...@...&$/.....v...q...D..&$/.....C..M.....k.....#...(...k.....]...I.....&$/.....&$/.....6<|....D..&$/.....<...W..J.D..&$/.. .....oB*.D..&$/.....a.....D..&$/.....;.y~A.@...&$/.....P....V@...&$/.....F..=z;.@...&$/.....o.@...&$/.....*..@...&$/.....2q....@...&$/.....Gy.'.h.@ ...&$/.....k7A.@...&$/.....:..N.A..@...&$/.....;/...@...&$/.....@...&$/.....P[. q@...&$/.....,+..._.#@...&$/.....J..j...@...&$/.....!...0.o@...&$/..... ....@..x.@...&$/.....*)....J:@...&$/.....A?.2:..@...&$/.....&.S....@...&$/.....MV3..@...&$/.....q.@...&$/.....u\]..q@...&$/.....*....@...&$/.....o..k..@... &$/.....^.~..z.@...&$/.....[.i..%.@...&$/.....+.{..'@...&$/.....D.4.@...&$/.....=....m..@...&$/.....+.U.!..V@...&$/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.142358518338951
Encrypted:	false
SSDEEP:	6:mGcQyq2Pwkn2nKuAl9OmbnIFUtpVMNAG1ZmwPVMNAQRkwOwkn2nKuAl9OmbjLJ:lkvYfHAahFUtpVu1/PVA5JfHAaSJ
MD5:	FA65BD3625A1488251BA2FAAE614F980
SHA1:	350FEB34E0EC2E73090A6C41BADC34F60A98AE7D
SHA-256:	03F3F4A363BA566790A399C4373BC11B709AC88A621EF533BAF2F4BD755A62B3
SHA-512:	9187596258B051EA9488E5590B9FB85F91721F42F23FAC14B736B0D6111E0DDB209FB689FB0CD1E0EFBE398174A0DEA912B2E0742187B9445172902A537A0F55
Malicious:	false
Reputation:	low
Preview:	2021/06/25-07:20:12.163 630 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/06/25-07:20:12.166 630 Recovering log #3.2021/06/25-07:20:12.166 630 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

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):	786432
Entropy (8bit):	0.008050090959268128
Encrypted:	false
SSDEEP:	12:I+mmTsx+mmTsxlNTpyxHHyTpyxHHyTpyxHHyTpy:TmbsmbPXytHwytHwytHwy
MD5:	03B3B4BB0F979E273B32ECC52C9B0E01
SHA1:	D307CEFF6AC7E7D3E424C1A855C56168596AEF69
SHA-256:	299FDCED8539A4D45595DBB33856A5A4045215BFECDD3EB7206996390C48C643
SHA-512:	4927E9663FD9AB3DB4449C765F0A55D33DFB51029B3F129E8FD1625C0C5F5593F52E59F180A5A0D1FE49D13C16D84EF3875FAB580375CADB6C5A4CF7439EDA1
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....).0k..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210625065248Z-540.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	1.702884022858162
Encrypted:	false
SSDEEP:	96:5vCYdTA0Biv41ySaWmfDBoNjwFOZ97v4zeej95oPhSUut9Xhd1ZYjQp:ttuSiQ1yiqBCjbsXy0bYu
MD5:	237A8005F865CBFB63F01412A8682305
SHA1:	F804195EB8D6D885A91B05C9489FD8DDAADEEAEB
SHA-256:	FF7682BF1AE5A223CB7018BD21EE739F527488D3C89A287C61438687471DE607
SHA-512:	21A283E4D0224A02DF7FE4AA5226C237FCECBCEB038566F498685E1AEF4FCF4182CB4AE78F0D0AF402ED4960082A86ED190F7758E2E70129F4E3B8E2D91CA06 1
Malicious:	false
Reputation:	low
Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.4493908404723923
Encrypted:	false
SSDEEP:	96:k49IVXEBodRBkWCgOOh1CK349IVXEBodRBkWCgsOh1CKn49IVXEBodRBkWCgsOhG:HedRBaedRBAedRBmedRB2
MD5:	A3AAC98EE84501E7195C398C83BF81F1
SHA1:	24278B4A2D3B626575D5A01DFCDC397CCA4CCFFA
SHA-256:	AB50BA22132DFDC157269395062FF07487936E0A1FD67A0237917E275EA08063
SHA-512:	EC3554930A58B0948CF1593478CB1A475EF24F1B90C09E5BA4796E9E6E27860756198D54C21E10D47A1E0BF0BABAE8F6E96C247604A68B7BD0BE5B261492575E
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	modified
Size (bytes):	34928
Entropy (8bit):	3.3146140869676253
Encrypted:	false
SSDEEP:	96:zCgOOhZCPR949IVXEBodRBkQCgOOh1CK1t49IVXEBodRBkeCgsOh1CKNd49IVXE3:QiedRBBSedRBJCedRBKyedRBX

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
MD5:	EB21277400DE75B0C33B14E09F49A160
SHA1:	9CA7AFE5682D77F51CE08309D941364CC41C64FE
SHA-256:	FCE08854234F13D5DD71272E1348C7E8DB7434969466D38D3D0CF960830C23A0
SHA-512:	CA7E98EF8AB8BBCD69175268E29E64AE072EE367A84C4A2A236E0BE1B1D449713D42DD75BF350387A90C030E36E629575B0B15A36DD4ADDC33F114A52108A7F7
Malicious:	false
Reputation:	low
Preview:	.....j7S*.....W....X.W .L...y.....~.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_33E8F98A524575FDD27708D6D61F97ED	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.083953418932811
Encrypted:	false
SSDEEP:	12:JY0Xc5FZp38Y4WizbK0lwuYC0qf1VDwC5XnN1m:JY0Xc3ZmY4Wi6u0A/wyN4
MD5:	C6D3C39A9AA48FE953BE20E002C729FB
SHA1:	78B4090791EFD57474AA39BEC3A0B137F40AFC33
SHA-256:	5C79873F2274270D0F01B1603922FC410D27BF13F747F2AD84E8566727740ED4
SHA-512:	8A0E3746B455601EC2348A56BFE91B0BC5B6D6F7CB670FBBD28091A01C71AA8218905BC1617C424A8BFA1B51CE5EBB2B4B456D69BD5CD68F37D719769400A22
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210623222013Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+.....V....r.....20210623222013Z....20210630222013Z0...*.H.....C!....I....q....=~l.X"..R....ot.....-GM..\.A.j...+.~9..Vc...;...WR.L...=..'..".cW.50....[....O3q..mw.....9..~..V..6...$O.b..b.P.].y>Z.'..b.3U.....97.bw.Ds.....`.I.:.OB..SB...u.....0.t!.....H.Z=.\s.....Yo.3s2@..K.X.sN.[.;...Y.9..X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_33E8F98A524575FDD27708D6D61F97ED	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8346429816435212
Encrypted:	false
SSDEEP:	12:2wNomxMiv8sF1JbqDkwJrBfnELwNUinC/YmxMiv8sF1JbqDkwJrBfnES:qmxxvnFqYwJNETAmxxvnFqYwJNES
MD5:	859FEFF7829F0BFEADC7CC88405A4A8E
SHA1:	3B224F1287A578CB4EF4040F824E97B7B761E00E
SHA-256:	8D0BCCA6575A9914920C3C91CF3A6BFF65DAA02A5639A793E9587F96DA055EE7
SHA-512:	95E4274B19F58E72B2F3CD72E0A1C1893B61E7BCCC1A1388B6034229DC169E19F1E3D41F73C9C4175F7D56AE80CA589ACEFB4D603675661925B073D2E88AB8C
Malicious:	false
Reputation:	low
Preview:	p..... .....>yU..i..(..... .....}.D.h..@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.K.X.B.1.Y.M.1.K.n.r.v.%.2.B.J.y.8.e.C.W.2.I.I.%.3.D...".6.0.d.4.4.2.c.7.-.1.d.7."...p..... .....>yU..i..(.....L..}h....r..m.....r..m.. .....}.D.h..@.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.K.X.B.1.Y.M.1.K.n.r.v.%.2.B.J.y.8.e.C.W.2.I.I.%.3.D...".6.0.d.4.4.2.c.7.-.1.d.7."...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7764	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157979
Entropy (8bit):	5.174259815365338
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3++:RNj3aRlQShhp2VpMKRhWa11quVJX+
MD5:	159ACCAFBA209FBC642499809CE2B513
SHA1:	6D94F57B63CE3BE71EDFB081ECB848B7D06EB2BE
SHA-256:	ACE286E29DFDB19080E514F3447F46E0E4ED658263AC209A9B4BBCECC36139D3
SHA-512:	E02BD1B88C1188CBBD4D6C1F5B31A44A278B213D991C6E9B9B06C620D66B1290DFBDF6D7BF92082D51A146C8AF772DAA659F9C2DC0A416C6BA9BE14B89C6EB8

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.7764	
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt16.lst.7764	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	9566
Entropy (8bit):	5.226610011802065
Encrypted:	false
SSDEEP:	192:eTA2j6Q6T766x626Oz6r606+6bfs6JtRZ65tsu6rtG16lMXY5B5Cfk:es4p0vTLcdfIfsmtRZEtsuatG1gMIzV
MD5:	63B24EA3A13EAC476D6309BB202EF459
SHA1:	89502C393549C20C933E4553F51F74F3DBE085EF
SHA-256:	2B4BE0BED267BBD4E4FFFC912A6C7ED6A8D4735DCF9B69FF90F37CDDEF4110EA
SHA-512:	2CB315DD00867DEE3A2CBC4017B59C53B41E817216FE0111A60947E1F0D81FF6767D8F7B5C406AAF9E6516BE716A086642AFFABBEFBE4C5B260437C89E3535EC
Malicious:	false
Reputation:	low
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\CMap\Identity-V.FileLength:2761.FileModTime:1426577652.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:Type1.FontName:AdobePiStd.FamilyName:Adobe Pi Std.StyleName:Regular.FullName:Adobe Pi Std.MenuName:Adobe Pi Std.StyleBits:0.WritingScript:Roman.OutlineFileName:C:\Program Files (x86)\Adobe\Acrobat Reader DC\Resource\Font\AdobePiStd.otf.DataFormat:sfntData.UsesStandardEncoding:yes.isCFF:yes.FileLength:92588.FileModTime:1426577650.WeightClass:400.WidthClass:5.AngleClass:0.DesignSize:240.NameArray:0,Mac,4,Adobe Pi Std.

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.4331110334817385
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiC0Zegbwra5Z7vnUJrq4WE7QwsEdufYyu:J0GpiyVFiheg8rAZ7vn5wsWufK
MD5:	4C135AF6CC162CCF0B839B3FB4FAE707
SHA1:	3E21D55E3E940002BFA66FE46158B7098E700284
SHA-256:	AD73BFBB2211731E87A7FB1AD46D2312BA4FC82CA0558AFAF48D7FE54A79B75E
SHA-512:	6D1EB1609226DAEA8166D3B781CDB2641F8083B522662B1361388FC54F257F7E40B13D3175659525BCB6D570396C8D159D8E27338067643AFA54EB13B68DD6FE
Malicious:	false
Reputation:	low
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....."F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$....."F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Google\Chrome\User Data\01b5067a-1604-4c34-8e4a-c498f1244979.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	108920
Entropy (8bit):	3.7513834423120733
Encrypted:	false
SSDEEP:	384:IHQBFNTIqyX6wTLV0aJIN5riv933GJPSHDOGJCdr489CgtOxHWG/L+flH/Derc18:yxK2hlK9AiIeTU4DQgkir+LK+bJRv
MD5:	AD75A5EF91FAC756497DEE8742F035A2
SHA1:	5F9E8A426DC9C909DD3BAED310883CF7DDF97891
SHA-256:	72DB3FFA9508F3AFA96A4FA802E7B6605EF07808C9667A311E63932CF29F54A2
SHA-512:	A10F19549E36CE9981317EF9EFF8EAF35CA50ACC43E803A48BC3E4765B28EC67037E67671A2A1C2E0F7BB1C0DCCA3D3870AF27706D97E749AD009F32B8D627D4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\01b5067a-1604-4c34-8e4a-c498f1244979.tmp

Reputation:	low
Preview:	t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....=8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\0e99390c-42fe-4fb2-9518-b86775aeb8dd.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	165617
Entropy (8bit):	6.049995757275568
Encrypted:	false
SSDEEP:	3072:zmS6aIIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:JzpXa/W10dGaqfIlUOoSiuRx
MD5:	32F12A67144EB61E0A9AB234A6C2F150
SHA1:	845EF765A7D3252B14B1E798DC3A50D8C5304B6A
SHA-256:	A76AB7162E0E7C12C96FAE87208C7D57B0E94ED85AE127C50D31BDA00A685E70
SHA-512:	DF0C5498EABD065F29C2350F51D7E62C52A990C96E12EC4DE6CD7CA90B6D6CDD2C7BF601575C19F7487483EF8AD2A0365DCA43A91A2763FB2BDA725EC6E706A
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715692134"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\1c3e1be7-67b6-4d96-ab5a-a9dddd4744d9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	166058
Entropy (8bit):	6.051229838415099
Encrypted:	false
SSDEEP:	3072:KmS6aIIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:izpXa/W10dGaqfIlUOoSiuRx
MD5:	3AE1C2FA69D40BA84DA96D91B641E27E
SHA1:	31D3E57A725A3978AFF4871C2B18B6D92C2741AC
SHA-256:	81A67BDB4D1C3FF6A628DF7785D6882D7A596A12E241FCEC5A6A461BDDBAB366
SHA-512:	AFF904BF14A84E3965C0CF8B7F7B9E4F738F7979F76D62983B75D78B3F5425D7473830542E5FC2CCCCC6C55F4F17821411CDA06B321949AF1F7696C11F664351
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed"

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ffe6ef6-6cb0-4890-a1b8-dc67c9695779.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7516490144133288
Encrypted:	false
SSDEEP:	384:bHuFNTIq/TMJIN5riv933GJPSHDOG6dr4rRNxGH/Derc1mc/In5pR2OTzJN41hIw:q2hlKbaiIeTZfD43r+LKFbJRY
MD5:	509629D2C893690C1AA3EB8449069B50
SHA1:	36F428B0F7E0C17B07090503E7CF7A1029C4C117
SHA-256:	3F071246F3D4E8B554CFFD1880D9392D81E890EEB396B4E5BFFF92C2FFCBFF80
SHA-512:	0CE5D01EFC1CD4B48E5006E8522328CA2F13C61C9030C96643031CE401CC83937F6B6088E3CD332BCCDF5581AD9D4B09A057DCE8476AA77257CEF8906A2E61D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\1ffe6ef6-6cb0-4890-a1b8-dc67c9695779.tmp	
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....=8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\28fb55de-9f74-4c2c-b4f3-b96f4bb0efe9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174341
Entropy (8bit):	6.080246326712281
Encrypted:	false
SSDEEP:	3072:7amS6alIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:GzpXa/W10dGaqfIlUOoSiuRx
MD5:	DD169C752A3ECB014EBC250C60FEC02E
SHA1:	46C8B25ACE8702C5581E1D977EEA13B3AAE2500B
SHA-256:	FC8C28E96CEFC4D3DAD4AF7AC622333A421CBEC40DC7698AC0858E4F9D4C53DE
SHA-512:	165B09C37F95B076940FA9799A3A03A93A1889D2E467B039B0F24F3E094DB181303C1C52CC8F0B7A70123972814E69D5137D6EA53B6632CAD6D95CA46B06749E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715692134"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\2fc34a77-9609-473b-843f-232ac4f00742.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174083
Entropy (8bit):	6.079750245486145
Encrypted:	false
SSDEEP:	3072:qZEmS6alIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:sYzpXa/W10dGaqfIlUOoSiuRx
MD5:	F648A67AD5F15DB28F251E585CB0A1DE
SHA1:	8F57DBBC8A4B893129E5779E40D73DEA2FCFA9B2
SHA-256:	C8E376E422DE83FE2C5E0F729DBE322AF99574C53C742820C45FC19E0A34866A
SHA-512:	A04B40B3110CF0FDB9BCB3C8A241CB364327FDC74E9DF25A1A09E119B0E2D29E5517FBC3E72BC9CACD9D94F36576A235680F56AEB0A2B06E0FDD007FA94B2 2D
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f85e696-bd85-48a8-8349-5324db062c12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174083
Entropy (8bit):	6.079748176992909
Encrypted:	false
SSDEEP:	3072:qaUmS6alIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:3ozpXa/W10dGaqfIlUOoSiuRx
MD5:	440A441F8E20E6BA2CBDEC68FDDCF696
SHA1:	7979DC7005D9A3ABF6F3FCD74DAE966C02E4BC9B
SHA-256:	C116EDB81DA42A2768BAA9745A74308F761707C78EA2AF30093A172825222E0D
SHA-512:	19A9F30530F381F349A1ED632850B5665D0A57D4996A7583EF41A985855D13975A001C7880B5F887A79A9716895459FA51204C86C381C60549F1AF61E87497BD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\8f85e696-bd85-48a8-8349-5324db062c12.tmp	
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\94670336-33a4-481c-b9d4-6ae8ab5cfa12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	174083
Entropy (8bit):	6.079750424707954
Encrypted:	false
SSDEEP:	3072:7FVmS6alIPDqVyYa/t0f13KdnddYFcbXafIB0u1GOJmA3iuRx:RHzpXa/W10dGaqfIlUOoSiuRx
MD5:	294BB86D9E422A42172239C84484BBBA
SHA1:	8A0F9FB166CD2B0C3ABA37C0B26708FF76E373D5
SHA-256:	ECBEFE10D90B1D89188E832D9A2BA0ED3679848550EAEB95FE1B0F7A60168770
SHA-512:	3191D8574668F83A5C7AE2B5AC0B6F700D00D282843805E180963CA47A1C3C6F8305F863394427B1AA7A86F2B6CF1CBA6CC3E4D148E384F59364FFE1CBE4E1F
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.624598323746358e+12,"network":1.624598325e+12,"ticks":5872287547.0,"uncertainty":4493236.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715692134"},"plugins":{"metadata":{"adobe-flash-player":{"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000002.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Xv:1qIF/
MD5:	206702161F94C5CD39FADD03F4014D98
SHA1:	BD8BFC144FB5326D21BD1531523D9FB50E1B600A
SHA-256:	1005A525006F148C86EFCBFB36C6EAC091B311532448010F70F7DE9A68007167
SHA-512:	0AF09F26941B11991C750D1A2B525C39A8970900E98CBA96FD1B55DBF93FEE79E18B8AAB258F48B4F7BDA40D059629BC7770D84371235CDB1352A4F17F80E145
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000002.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3117
Entropy (8bit):	5.522527040460245
Encrypted:	false
SSDEEP:	48:/lwLIJlwBe8eQYxlwBe8eQYWlwhe8eQYzfaRwje9eQYKRsU:/lwLOlwVYxlwVYWlw1YzfYwGYKRsU
MD5:	DD65CE5678AA78F60D5FD84933A52341
SHA1:	5D9C3F017541F39AD97BA14529D8C8F8FA052CBD
SHA-256:	91FD8767AF68A996F8D827DB963D771D8B1476175627CA4DB3097FDD7FC5CCE8
SHA-512:	7DD100E2A8E6404CDBC764976BA9B4FEE148629CACD25A3A2F4CB85A64DA9D9057DD7E4DF933FACE85BC71B2576E66685857DA42D3CA2F98850623774053BC F
Malicious:	false
Reputation:	low
Preview:	t`.i.....-download,186f8791-b13b-4f1d-9240-f20c999bd0a5.....$186f8791-b13b-4f1d-9240-f20c999bd0a5.....9"...(https://www.brennergrill.de/Mittagskarte .Nhttps://www.brennergrill.de/wp-content/uploads/2021/06/PfifferlingeMittags.pdf...."(https://www.brennergrill.de/Mittagskarte*.0.B.J.Fri, 18 Jun 2021 12:36:23 GMTP...Z.a pplication/pdfb.application/pdfj.....r.....x.....O.....-download,186f8791-b13b-4f1d-9240-f20c999bd0a5.....$186f8791-b13b-4f1d-9240-f20c999bd0a5.....9"...(https://www.brennergrill.de/Mittagskarte.Nhttps://www.brennergrill.de/wp-content/uploads/2021/06/PfifferlingeMittags.pdf...."(https://www.bre nnergrill.de/Mittagskarte*.0.B.J.Fri, 18 Jun 2021 12:36:23 GMTP...Z.application/pdfb.application/pdfj..|...;...C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.D.o.w.n.l.o.a.d.s.\.P.f.i.f.f.e.r.l.i.n .g.e.M.i.t.t.a.g.s...p.d.f...c.r.d.o.w.n.l.o.a.d...rhd...0...C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.D.o.w.n.l.o.a.d.s

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\028a4bba-3ea4-42f6-916e-d4990c4786e4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.5358975875072085
Encrypted:	false
SSDEEP:	384:3TEt3ELlVyX91kXqKf/pUZNCgVLH2HfDdrUlHGunZ5l6rX41:qELlG91kXqKf/pUZNCgVLH2HfZrU5Guz
MD5:	CDFC975FB9B2C09B35DDD62CB9E40F6F
SHA1:	14B71503F965FFD806ECEC563DE22DCDA3964A54
SHA-256:	F61C9FDC66F996627D1010871F4B25688AF4EAE1E3977C30E8E93A66619D07A6
SHA-512:	5805DB9E586BAB8F2129FF8A9ABF94334E00BA1308AAEA40334296BFD3CD7EE639376E3D72103BC9DA2F282872C4E204D8EA9500201F0B7C7E0051FBD6FE6D5 6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13269071920676980","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\03d2d795-f416-40b0-a9f1-107b9ba2d960.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5890
Entropy (8bit):	5.166317802707135

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\03d2d795-f416-40b0-a9f1-107b9ba2d960.tmp	
Encrypted:	false
SSDEEP:	96:nOLNHAsMRfYTIVGk5k0JCKL8tUlkb1kbOTzV1VuHn:nOLysMRATIYkh4K6skbdVU
MD5:	6002F378E2736F4FC068F0F03F4CE8B7
SHA1:	91E9786D328A99005AE395AA738B82A8ADC0C464
SHA-256:	75DB54BE5B39CE814A36218C544198DE324AB2773E22A79298308FDE9FC3ABF8
SHA-512:	62CED52182822685154B72E3945EE0B81BD066FC32C57BA181C3F58D0B270F057A05B2E425330D71142A6F26968A038A4007A4370A76151940659DF120F8CE52
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13269071920956822","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\41a675e4-eece-4fbb-97f4-db53685f3036.tmp	
MD5:	FE435196F4C29F9153B80B9C16E146EF
SHA1:	2E56DA7BA393A3C1229FE8F5D4C18AEFD098142F
SHA-256:	F09BCD815F8A37CD8E89580E034A78D71B74568DAFAD14A1E827136A1CFB2D24
SHA-512:	5E499DD029E91C07F3A974AC2E1E1854F6E599B4B056334C7C9407F825193DBEAB969E03874D113D52669B1B2BAE0B86D8C1B9F0E971674992B746F2C870C400
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","suppor ts_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[], "server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com" ,"supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271663 923818215","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271663933125044","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.googleusercontent

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\579ec50d-dab0-4c84-a55a-c3c62973e601.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3696
Entropy (8bit):	4.86335912853886
Encrypted:	false
SSDEEP:	96:JnzMKDHGXOLW7DGWK/xZgxiGwGkGlrGBjOmhMJKThM:JnzMKDHGXOLKDRSxZgxiRfQmjOmhMJKK
MD5:	CB1186F3DFEB5C031CCBBF1ABDA1A676
SHA1:	2F9013D03F2DB7A269B8A0A197773264D16C3221
SHA-256:	4597811103D4EDBF485A1D272076920030994394B020F783C36E3593036ADCD8
SHA-512:	02D2E5E11955A5FF5A68CDE24F6B91B59DC3CAED44D87C5B3AF0C1317DB28D5AF9DFE32F87CA3CF60530B0A2EF025F6F9A1A032EF1B54406C94DC17171515D 7
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","suppor ts_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[], "server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com" ,"supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271663 923818215","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13271663933125044","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://clients2.googleusercontent

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6ca78cd0-d0cb-4370-a415-8708bdf33f0e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1373
Entropy (8bit):	5.588483055475819
Encrypted:	false
SSDEEP:	24:Ya9RAeUN6H0UhsSvrfwUPlG1KUBezkq/HeUe8zUeBb7wU7RUeiQ:YGieUN6UUhwUcKUxqPeUekUetwUFUeP
MD5:	F0CB0D02EAE29F68CC3E070A4CDBBEB1
SHA1:	50943ED179E1892AA0CA0979FB2A5CD199BFC88C
SHA-256:	EB93CFA24677684DD927F2D7D20BBA70549C31A26C391AFBB0B46AE5A1E0D843
SHA-512:	2455EFB40726B65604725669BD19AEDB2CCFDC84DDB643B29B1BAE8696E8791C4D4FE17A1107D8097FE45C480F396AEBD4C9F8B44A01A94AE08E1A45999FB4 3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1656134345.008514,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts _observed":1624598345.008519},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subd omains":true,"sts_observed":1601450995.029298},{"expiry":1635484727.069835,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https", "sts_include_subdomains":true,"sts_observed":1624598327.06984},{"expiry":1656134329.774278,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2Ok gA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1624598329.774282},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO 1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7 YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\885b9627-900d-42b1-a867-296b2f6b1106.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1206
Entropy (8bit):	5.5866934427531385
Encrypted:	false
SSDEEP:	24:Ym6H0UhsSvrfwUPlG1KUBezkq/HeUe8zUeBb7wU7RUeiQ:Ym6UUhwUcKUxqPeUekUetwUFUeP
MD5:	FCF47B445BCAC18624CB52865BB20EEB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\885b9627-900d-42b1-a867-296b2f6b1106.tmp	
SHA1:	F92DA8EAC6E2E59DEE86667EF4DF60F8B3CA210E
SHA-256:	F2B63AC26D4CA39E060D9D01005CE59B404F1562574A9BC5CA70E5545A835BCC
SHA-512:	F0CD9F8A4A4DE7DF9453EDF5876AD8BD598DDCAFF9795B950631DF21190C4055111D6B9EBA07F9C43CA92AB998640EEEF737A2404E86A8EF56DF1DE5165962 6
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1601450995.029298},{"expiry":1635484727.069835,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_in clude_subdomains":true,"sts_observed":1624598327.06984},{"expiry":1656134329.774278,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"forc e-https","sts_include_subdomains":false,"sts_observed":1624598329.774282},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8k DM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho 8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451013.786337},{"expiry":1656134323.81828,"host":"8/RrMmQ lCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.2843823351692025
Encrypted:	false
SSDEEP:	6:mGM4pM+q2Pwkn23iKKdK9RXXTZIFUtpVM4nZZmwPVM4VpMVkwOwkn23iKKdK9RX3:lM4M+vYf5Kk7XT2FUtpVMq/PVMEpMV5B
MD5:	E2B53B325ACF786499777867936C1899
SHA1:	98369768A1DD3712CF7BA68D7A5A835C8707DA43
SHA-256:	02A35751858EAFBDF475F0670E9FC913754EF79FEBF2B23DDFAB487E43618352
SHA-512:	44C7D1D4DF1936CBF5C7096BACE228E6E0BE7083C7BCC7C9CB0060341DEBDE624D7D3ECAB37FB5D2E2E0535C284A1FF36DAB46D2F54690DEBD91735731F8 6C
Malicious:	false
Reputation:	low
Preview:	2021/06/25-07:18:53.994 166c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/ 06/25-07:18:53.995 166c Recovering log #3.2021/06/25-07:18:53.996 166c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik eDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.266194118751354
Encrypted:	false
SSDEEP:	6:mGM4sBM+q2Pwkn23iKKdKyDZIFUtpVM4kXZmwPVM4TSMMVkwOwkn23iKKdKyJLJ:lMzM+vYf5Kk02FUtpVMT/PVMaSMMV5J+
MD5:	E4BB9CE6E16FCA5B6DF18DE7DA069050
SHA1:	C299D7CE5AD9AD8025434607422671B9BB96D83C
SHA-256:	4D9B962D017BA2B7C380216643CE3F4AC76DDC1037664CB655F4478A43049C10
SHA-512:	4474B6557EAB2CB5E53471B2A4DCB8F478FC4F439A5A5D8EC6FF8AAAF7FD2BA51CF8591F9D26A1C4ABE43E4E2CA465E1FD2B3343AC1622139BA29D5BCF010 5D
Malicious:	false
Reputation:	low
Preview:	2021/06/25-07:18:53.988 166c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/25-07 :18:53.989 166c Recovering log #3.2021/06/25-07:18:53.990 166c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02efe818acb3d568_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15823
Entropy (8bit):	6.045904021186041
Encrypted:	false
SSDEEP:	384:RNpboEvmObR7V1D0JGOPeUzi9CIypF5YU7Z5KrpvhVhG8wCU:RKOj1DuGOP1I2mG8u
MD5:	BD9345D44E8AD2E469CF843E07ED432A
SHA1:	9793DDADF59C978053E095D398C0B24126A17355
SHA-256:	70144692694DE55436F4BF66ED813C635DFC76310FAF7BB3328DFCB4F91FAA84
SHA-512:	DC215D2D41F17B7D408FF1BD5500FF48B67A09AE62BA2F70B88FA7539404AED23916352F95F786D60EEE5B004B6BEEEF78A209BAE0BD49487521A4816759151
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02efe818acb3d568_0	
Preview:	0\r..m.....o.....;....._keyhttps://www.brennergrill.de/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2 .https://brennergrill.de/N...&$/.....N.a6q.-..W.&.A... *.g.....A..Eo.....n.....A..Eo.....'..+....O....0<.....X.....8.....(S.P..`\....L`.....Q.@.....jQuery....Qd..`.....migrateMute..(S...`.....4L`.....0Rc.....Qb.%.....t...`$...I`....DaR.....Q.@."U]....define....Qb..~.....amd.....`.....M`.....Qc.2h....jquery...(S.....Ia.....I.....@.-....`P.q.....Q...https://www.brennergrill.de/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2...a.....D`....D`....D`.....!....`....&...&....&..A.&.(S.....`.....L`n....Y.Rc.....L.....Qb..Q.....n.....Qb6Or(....s....Qb".g.....r.....R....Qbn.....o.....M...Qb.U.+....c.....Qb.....d.....QbV..\....I.....Qb..^.....p.....Qb.9.....f.....Qb6.o.....y.....Qb.$.....m.....Qb.U%.....h.....QbJ.u.....v.....Qb.p.8....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0349c3ce756ae780_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	399
Entropy (8bit):	6.14908234712588
Encrypted:	false
SSDEEP:	6:mVtVYZHf/VpEV74alBgD0sySBKFgegll+pGo4HHgj6AcnK6tBxTP7TQVxWs06bk+:gtE/I7Zc78n4HHjp7RsWs0b4HHr
MD5:	0E6CD769C322B0E954018D05B8E494A3
SHA1:	49528A37EDE9C0CC5018D27D96C36E0249E83E7A
SHA-256:	51E877FC511C5CA52ADA846343CAC2688CA4197CB8B7BAF843C1091BEEFBFE69
SHA-512:	12A2DF45A9028E92340C83B1284D9AB87731760D0DDDEA67D80553106B2FD7EE7AFD958354B4E9E92F8C58A8BD8C2CBABE59943C4D1B67CD4ECD471958020DB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!BY....._keyhttps://maps.googleapis.com/maps/api/js?key=AIzaSyDUxnfOO7dcYC8B01tCsfRMmVrLqXpecWA&language=de&ver=3.2.1 .https://brennergrill.de/6V..&$/...../.....[_J..w..X.DO.....U.}.....i..A..Eo.....o.....A..Eo.....6V..&$/.....45EDF17C261EF72CD6272C98F9A95B2287FE67CECE48114362A478A56CCC5E08[_J..w..X.DO.....U.}.....i..A..Eo.....zL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\076da36ef9bbc6ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	994
Entropy (8bit):	5.6924657108650685
Encrypted:	false
SSDEEP:	24:fSVZ4fJM1eJmX0t9DRXZOVZ4fJY6c0Hv6eePeZB:syJ/JsSLuyJY6pe2ZB
MD5:	6E88605548B161E72EB5734DD847DA39
SHA1:	3B35B39839AC4EA203221C5AC3E842883BD644C7
SHA-256:	B499DD0314BFD315F169BB3E41AC1717EEAABC463BE0D9B4B156271ED77D3C8B
SHA-512:	4260F2A02C24DCB64A155444967204EC1202EECDE74A691D8EAE6F8C1F19C7568220CABFE5D48AEBBF12ACD251B3750A1320014243BC50CEEDCF5C153502430
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....._keyhttps://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_d013db1583b49aa8be6336b53dd83504.js?ver=5.7.2 .https://brennergrill.de/..&$/.....P..h....+!..NS....=..?tp..D..A..Eo.....OM'.....A..Eo.....&$/.....'.c.....O....@....z.....(S.H..`H.....L`.....Q.@.....jQuery....Qc.....document..QcZa.T....ready....(S.....Ia....b....@..l,.....9.....(....d.....d.....IE.@.-.....P.....|...https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_d013db1583b49aa8be6336b53dd83504.js?ver=5.7.2a.....D`....D`....D`.....0...`....&...&.....D`....DI]d.....K`....DI .....&....&.]...&.(...&.....&.Y....&.....$Rc.....`.....Ib.....c.....@.....d.....P..h....+!..NS....=..?tp..D..A..Eo.....[Z.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07a86bad00df05dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4601
Entropy (8bit):	5.722573354625157
Encrypted:	false
SSDEEP:	96:Zlftg4xotRWwh8qaNch20mGYzzBIEb/dUah3LdE1H:/12t0cZae80mGczBjJUg3R0
MD5:	A6185BDD1C47550FB7C4BE6718541DC0
SHA1:	BAABC32F1853AB35F95DD04B3286445B0DA21947
SHA-256:	554B11B2D5068D3E93D00C8CDC022918E395734EB9EE6412E1FC0434F98CC70E
SHA-512:	0C791769EFE5798E759A98B858170748E75F20A75C912E76FE95E23F5D5AA66FF1A5FE54B24D6A1240BDF0616DD66F0E5A3B71E4F2A7EB7F2476C95830D3E104
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.4 .https://brennergrill.de/m...&$/...../.....Qr.....\S..cc....(J.bqH.....A..Eo.....CM.....A..Eo.....'.....O....P.....(S.0..`.....L`.....(S..`d....hL`0....PRc$.....&.....Qb.q.8....e.....Qb".g.....r.....Qbn....._.....Qb.%.....t.... Qf.2....__webpack_require__.d.....I`....DaP...:%...(S.....Iah.....a...!..@.-....pP.....c...https://www.brennergrill.de/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.4.a.....D`....D`@...D`.....t...`6...&...&....&....&.(S.....5.a.....Qb&.....t..a.....I.....d.....@.....D&.(S.....a.....a...Qb.....d..a-.....I..!..d.....I.....&.(S.....a.....Qb~E.....e..a...I..I..d.....I.....D&.(S.....a.....Qb>y.....u..a`.....I..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07d972fb7bfbe0c8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4620
Entropy (8bit):	5.7447080034518905
Encrypted:	false
SSDEEP:	96:fOfnKeCinVYcYaTUia20mGYzz8MEb/IBUat8LdE+X:fO/jmcYaTUK0mGcz8XQUo8RDX
MD5:	21C21D5A62FEEEE1C8E43B4251BC9F70
SHA1:	B9EA72912ED7101515A6BA1B9EE6F194074181D7
SHA-256:	40198D86F379A8FFBACA3F4013B6E974FD60C342262032E030B3DB1045FC5FEA
SHA-512:	A5A1DDC29D8810767EA49B379503835A156499A21C0F6E0885D78E132F9326F09AF6D5E411FA904D47877ED064971EA190AABD28F91004CD700EB43F7C4A87F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....+....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.4 .https://umstellungsverfahren-de-corona.com/m...&$/..... .."....;...[}s..m...R..*J.A..Eo.....z.,.....A..Eo.....'.....O....P.....(S.0..`.....L`....(S..`d....hL`0....PRc$.....&.....Qb...6....e.....Qb...:....r.....Qb.C}]...._.....Qbv.....t.... Qf..fv...__webpack_require__.d.....I`....DaP...:%...(S.....lah.....a...!..@.-....pP.....c...https://www.brennergrill.de/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.4.a.....D`....D`B...D`.....t...`6...&...&....&....&.(S.....5.a.....Qb.5.f.....t..a.....I.....d....@.....D&.(S.....a.....a...QbnrW.....d..a-.....I..!..d.....I.....&.(S.....a.....QbV.K9.....e..a....I...I..d.....I.....D&.(S.....a.....Qbz.....u.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10a8fa12917c9b73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.529715479899543
Encrypted:	false
SSDEEP:	6:mqU6tXYAnM7QApUv0XOWvtgi8W0I/MhK6t:f37MUApau5dQIk7
MD5:	635D160F5252287DB40341EFE70A51CD
SHA1:	87985A82EE297DAD179EC799A4C368A99841FAD8
SHA-256:	89C5280EC0E38F0AB9720023DC55032C119264F295F980F35615A438A62E42BA
SHA-512:	6CD61895FB7C87B9E1F62BB7A3487F4C0C3374D36FB88A3590BBDEC022664BBFBA688D6E8C1897B8326F641B5A95EE97E08EFADDC264D716CFC7BC1F1B2F69 5E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...`B1....._keyhttps://de.yoordi.app/main/mainf2bd57525d8d73dbcd66.js .https://yoordi.app/E..&$/.....#.....j.....^.....J....kw..@.....A..Eo.....9.6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16437ab375daa4de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13768
Entropy (8bit):	5.760510369658115
Encrypted:	false
SSDEEP:	192:hh207xHXm9/9JJ7g3evzL21ipL67gC/4FYcyBKBVIt6vtNTc5KqJfva/HixvsHY3:j2j3RfPh8ysjnkPvZtJ0
MD5:	103302FF954283015391F0FC8344D4A1
SHA1:	8481DF73DA679B892E5D4E349FCE5C2D2085F6C1
SHA-256:	116CD3F7B512B2D098F16BF2D19F1FAB531B987AF15313B651F318F69DD62EF0
SHA-512:	AA807736C6B87E9E49E887F8B27CEBBA36F2437EB24C03F75852562612FC5B9CD6D88106BC58023208550F52C71EB6C91DAB25CA0173DFDA60923D4B6E89E17
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....._keyhttps://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_a7ce780949735c20349e45ceae03a2b6.js?ver=3cdb22ea051a2fae380a7ecc49f25308 .https://umstellungsverfahren-de-corona.com/....&$/.....v.....I...\C.....%5.,.*,B9...;..`5..*.A..Eo.....o.....A..Eo.....'.....O.....3....o.....(S.\..`n.....L`.....(S...`.....LL`"....@Rc.....Qb...6....e.....M...Qbv.....t...b$.....I`....Da.....(S...`.....L`.....Qc..i.....exports..$..a.....S.C..Qb.A.\....I...H.....a.....Qb. .....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....I.`....Da@...8.....e..... P.....@....@.-.....P.....https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_a7ce780949735c20349e45ceae03a2b6.js?ver=3cdb22ea0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17251cebff9e9a12_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	181568
Entropy (8bit):	5.810262151571312
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17251cebff9e9a12_0	
SSDEEP:	3072:lDrHpVTB1HdG2XkQjhFFG0xU4ynNE5tgqHeTmUGynCoL:RrJVTXHPkQjhF0vn+tXmprnCoL
MD5:	73EA3B641B162CF8684703A9B9837D65
SHA1:	638E5EED839F4CADEF4B54FE817152FDE8EE55DD
SHA-256:	065C70D6F25D04925CCD8F517427E408A385A7AD97CE02A8CB4AE163902BAD37
SHA-512:	ED50841743C0713645B3B52DD66CEDF2A2688842B28BACA505C6C611E24BB42D9B03C1A1F397636BF45F636C04702934D47A53C8231464B44EEDA84822DB1082
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...0.0.....5921575FD8A2AB6A58592367299FD53F5D1DF68771F291F090388784E47B8D05.....'.....O0.....o][.....|.....(S.t..`.....$L`.....Qc.....window....Q.@..\|f....google....Qb.Mw.....maps.(S...`.....0L`.....8Rc..Qc.9.....modules...Qe.w.....loadScriptTime..a.....I`....Da....Z.....Q.....!..(S.....5.a.....a.....a.....Pd.....__gjsload__a.....I..A..@.-....xP.....i...https://maps.googleapis.com/maps/api/js?key=AIzaSyDUxnfOO7dcYC8B01tCsfRMmVrLqXpecWA&language=de&ver=3.2.1...a.....D`....D`....D`.....`....&...&....&....&...(S.D..`@.....L`.....Q.....Qbv..5....Load.....`.....L`X.....Xa...@.z.?...`.....(L`....F...`.....$L`.....`.....M`.....8Ql.N.H,...https://khms0.googleapis.com/kh?v=904&hl=de&.8Ql..M.,...https://khms1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17a08cd5603a5544_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1013
Entropy (8bit):	5.715343877084462
Encrypted:	false
SSDEEP:	24:LVVZ4fJ05YL7C/mi9DRXZOVZ4fJYes0Hv6eed7f:VyJeYL74FLuyJYeZed7f
MD5:	ABA2BB1ADBDFA886A8CF23AAB4A8BA38
SHA1:	5B27C588250D51D7E880BAF5DDF3F7A524F0C5D6
SHA-256:	9873CBEB98D2059895D750CFB5495E73259FA8C9DFB9899EB2A8637546BAB965
SHA-512:	B566034CCD3F5AC2F82C8676834DDD3C21D4A363682EFDDEAB500DA82D4C06AB7EB31F6DB7B1F3BD8748FD98AA3BEE54418EC5D9F8BE51E19BE1C4518A624C65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p..l...._keyhttps://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_d013db1583b49aa8be6336b53dd83504.js?ver=5.7.2 .https://umstellungsverfahren-de-corona.com/..&$/.....%.....AZ.xr...h...n.....R.B...2hH...+>.A..Eo.....&<.b.....A..Eo.....&$/.....'.c.....O....@...,y.m.....(S.H..`H.....L`.....Q.@.s.....jQuery....Qc*."4....document..Qc.(]/....ready....(S.....la....b....@..l,.....9.....(....d.....d.....IE.@.-.....P.....|...https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_d013db1583b49aa8be6336b53dd83504.js?ver=5.7.2a.....D`....D` ...D`.....0...`....&...&.....D`$...DI]d.....K`....Dl .....&....&.]...&.(...&.....&.Y....&.....$Rc.....`.....Ib.....c.....@.....d.....AZ.xr...h...n.....R.B...2hH...+>.A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\19814e80196efb9d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1418
Entropy (8bit):	5.706004939158955
Encrypted:	false
SSDEEP:	24:DnBCrWMB0di3l9hu+PgwBCre476bzUo+TgAonYkWY0+jkXTJnD:1CKMB0dCvhFCa43oelkWYSXTJnD
MD5:	8F12177AAA702A65D6C4A1E5A35A060C
SHA1:	053C55B03A3EC3D54B3549FD579367EFA760F67D
SHA-256:	3578F66FF58E0F34787E3DFB377BCB8938B6FFA64101573BFF775BEA339ACA4C
SHA-512:	54FD4FD05396A1EDA3F60CFF9403496FA86368869A67055B9C0A09E7BBCB6DBDEA4ECFFE16889A56DFA788D506939240D64CAC145B702A17C669AAA73482BFB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b.....q...._keyhttps://www.brennergrill.de/wp-includes/js/wp-embed.min.js?ver=5.7.2 .https://brennergrill.de/....&$/...../.....7-....[R.7..n...9.....A..Eo.....J.....A..Eo.....&$/.`.....'.....O... .....(S.<..`2....L`.....(S..`....0L`.....@Rc.....Qb.....d.....Qb.U.+....c.....Qb..Q.....n...b....$.....I`....DaX.....(S.....Ia.....Qb.%.....t.....@.-....PP.1.....D...https://www.brennergrill.de/wp-includes/js/wp-embed.min.js?ver=5.7.2a.....D`....D`,...D`.....`....&...&....&.(S.....5.a.....!....a.....a.....Qb..l....wp.....a..... QfZC@-....receiveEmbedMessage.a....H...l.....d.....@.....&....`....DI]d.....@.....Qe..r.....querySelector....Qe...a....addEventListener..1.....a..m...Q.`..B.....DOMContentLoaded..Qb...#....load..K`....D.Q.@.....%...%.....&..&.....&.(.....&.(.....&...&...&.(...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bb810769fd7ec7d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131944
Entropy (8bit):	5.865190968201739
Encrypted:	false
SSDEEP:	3072:BXB8/wbwyU9/Nf8DISSMEE4BYkcUdVXJAC2UoB:78/wy6ikB
MD5:	49E734F534DF18D0CA4655E8891AB11B
SHA1:	0670669F4D23ED2B6AF0EA994E74044E00FF1CA7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1bb810769fd7ec7d_0	
SHA-256:	1FA4894B58478FE5D60CAECF0682111C521FFE568B639C889C8C963A82B4573A
SHA-512:	B0C97A453AEE0907A4630730CE819E0E3C515746E06E4E1A577369D9A8BB2884B260E77A7446013FCFA7F4CE72184687EFC9E229EF81EC88F81C1267447166F6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....69E1AF263C19F1D4EEF7955481F11FF46529ADF40C9BCF9BC53E634FCADD54DD.....'.zd....O,.....[.....`.....<.....(S.M...`N.....L`.....QbFT.&....self.(Q...3[.....webpackChunkelementor_pro.....Qb.....push...`.....`.....TMs&.....4...,.....H...P.....@...T...d...>...p...t.....v.....Z.....a.....`.....L`.....`.....Mc....l/.....f.....b.....C`|...C`.)..C`. ..C`(...C`:G..C`F&..C`B=..C`....C`|I..C`.&..C`.J..C``...C`x@..C`....C`,...C`....C`.(..C`I...C`\:..C`.'..C`n...C`.'..C`$%..C`T9..C`....C`."..C`^3..C`FI..C`....C`\|...C`....C`b...C`.1..C`,(..C`.E..C`z...C`.B..C`.L..C`.7..C`I/..C`*H..C`.I..C`.<..C`.*..C`....C`.9..C`....C`.>..C`r7..C`.!..C`.E..C`.$..C`.1..C`....C`.9..C`.K..C`.H..C`....C`.)..C`.K..C`~&..C`DG..C`.*..C`V...C`....C`....C`.!..C`....C`.E..C`Z...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fb406827feb5c5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33478
Entropy (8bit):	5.852034509144224
Encrypted:	false
SSDEEP:	768:wrSRydXz128MB6N7Twzky4GP9dYf/3dVPT1WjAtL5/p:w+RydXzI8MBqn49PHYf1RT1rR5B
MD5:	A5060BEE41C62D21245F69C410D6DB5A
SHA1:	64AFE7E8ED4140C0EBEE212B409EDB69B1B46E5C
SHA-256:	AB482112C904CC70A8728ED8DF6EF617385CD5275727258EE522488A62747E69
SHA-512:	D82999522091BF7C8DAC254A59AD12661B79D33FF970517339F0FA7A5C4BBAEF768412918374F06515E0A10F5540FB69D70CA7A97CC05BD7F80B7894204F9E83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/js/preloaded-modules.min.js?ver=3.2.4 .https://umstellungsverfahren-de-corona.com/....&$/.....k....I.;....;.t..oj.....Q..Z....A..Eo.....".....A..Eo.....'.....O.....HO}.....(S.a...`z.....L`d.....Qb..t....self.$Q...O.....webpackChunkelementor.....Qb.k.p....push.....`.....L`.....`.....8Ml.....j.....a.....`.....L`.....`.....Md....t...f...D.....y...b.....C`|...C`.)..C`(...C`:G..C`.>..C`F&..C`B=..C`....C`|I..C`.J..C`....C`I...C`\:..C`.'..C`n...C`$%..C`T9..C`^3..C`|...C`....C`.1..C`.E..C`z...C`.B..C`.L..C`.7..C`,B..C`jH..C`.L..C`.=..C`4...C`....C`.I..C`^...C`....C`.)..C`t...C`p...C`f...C`....C`.%..C`. ..C`.!..C`.0..C`.....(S.4.` .....L`.....Q.@..i.....exports...K`....Dg.... .....&.]...-.....(Rc.....&....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\219e600b74ace8a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9185
Entropy (8bit):	5.527636904649585
Encrypted:	false
SSDEEP:	96:qXkuO2GW+XZUHz/ZHz+98pVlSXGisKS7u/PzXBBc/0L+8Z+gHHx3+DrRPkdBqiVm:qXkuO2GWcZUHz9+Qy20xSsL+c1nIA1fE
MD5:	EA99E84825E217C8F8E3CF9DE98BE73D
SHA1:	727BC107424F87E022E3DA5D9A1A170A195B830F
SHA-256:	B1CCCCD9EB72F60CCF02C205AF37FEF3191004618F26D11E2F1618333547DB7D
SHA-512:	64D39709D9F11666D17EB72AB252C548EF55B3083C8DBBE0A5C505316CE3D9A021135A184C1204C0112DD83C6F0345B1BB47A5AF2EFD65F57C76A9705BDA21E
Malicious:	false
Reputation:	low
Preview:	0\r..m..... ...._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2 .https://umstellungsverfahren-de-corona.com/4...&$/.....Gh8Aul..V..Y..j..2.d.$$...C..PH.A..Eo.....y.....A..Eo.....'../....O.... "....[g.....(S.T..``.....L`.....(S.U..`b.....L`V....@Rc.....Q.@..1k....Waypoint..Qd">J:....keyCounter....Qd"..O....allWaypointsb.....I`....Da....,...(S.....Ia*.....!...!..@.-....tP.....h...https://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2a.....D`....D`H...D`.....`....&...&..a.&..1.&.(S.....5.a.....a.....Qd.`.7....queueTriggera....P...I.....d.....@.....&.(S.....a.....!...Pc.....triggerat.....I..!..d.....@.....&.(S.....a.....Pc.....destroya.....I..d.....@.....&.(S.....a.....Pc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22fa42cd9c404f19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	61768
Entropy (8bit):	5.752940533725166
Encrypted:	false
SSDEEP:	768:owkdOaMpH8AdIc5ga3JiBMhQaHMse6k+ep3jqjCuOQYg8MV4Sxh9st:3kOanAdga3QBMrX++c3jaCuOQYzmst
MD5:	E85B955D483454AE1AC90F6BB04D5760
SHA1:	986321763DC9028FEB2A38DD7B828A084212726C
SHA-256:	4E9DA0BA51D0B09FDC972FE4B4E600B3E96105AA440F471B7A77A005DA9668B6
SHA-512:	2452E07DAA4EB9F758E47ACE998AE985C410DF5E326425A1048674F702841B21E99A88E1591A486E8F14DA8C9914B30EA7EB1DDB7475C8491E78F4E81FF2B93A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22fa42cd9c404f19_0	
Preview:	0\r..m.....Hv....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6 .https://brennergrill.de/r...&$/.....e0..... .2p.;.4....?.....-.b%.C..r....A..Eo.....S.....A..Eo.....'.....O....`.....,".....(S.<..`4....L`.....(S.x. `..... L`.....Q.@.j.G....exports...Q.@~.....module....Q.@."U]....define....Qb..~.....amd...QbFT.&....self..Q.@>.U{....Swiper....K`....Dx.....s.....s.....&.\..&.-...%..3...s. .....&.(.....&.]....%.....&.\..&.-...%.....(Rc.....I`....Da....<.....e.....`...p...@... ..@.-....pP.....b...https://www.brennergrill.de/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6..a.....D`....D`....D`.....E....`....&...&....&.(S...-".`.D.....L`.....y.Rc.....T.....Qb.q.8....e.....Qb.%.....t.....S...Qb6Or(....s.....M..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\249f3c9265a5c7c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13749
Entropy (8bit):	5.75787026074542
Encrypted:	false
SSDEEP:	192:nf4HXv/7JJpg0e2yipL6741/4FYeyBKBVvIt6AtwdLmoqnJIRafHN3xSsH0uJcg2:nslr9AL4uKoqsOdTvqw8
MD5:	5E3343B7E08E6886F5AA7AD9A0B382CB
SHA1:	355F4CCC6091C0493FE1336C7E4CCE84B46E89CB
SHA-256:	55D61652811D5C24521145AF4CB0CADDB04B3E59533C9EFBCD5AEBCDD3D7866F
SHA-512:	FF657BBE0B3A6BE4CAB418BEC885361A376EF83BCEA1E6762FD0ACF96F5CA39170B3F7AF5D68311BF1F4DFF6C3FE25DBE1B37D187D81F010D4E71E78FBB93C56
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.K>...._keyhttps://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_a7ce780949735c20349e45ceae03a2b6.js?ver=3cdb22ea051a2fae380a7ecc49f25308 .https://brennergrill.de/....&$/...../.....@...ws.l.....SS..t.5.h..G.Go-..A..Eo.....<..n.....A..Eo.....'.....O.....3...v.....(S.\..`n.....L`.....(S...`.....LL`"....@Rc.....Qb.q.8....e.....M...Qb.%.....t...b$.....I`....Da.....(S...`.....L`.....Qc.j.G....exports..$..a.....S.C..QbV..\....I...H.....a.....Qb.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....I.`....Da@...8.....e..... P.....@....@.-.....P.....https://www.brennergrill.de/wp-content/cache/autoptimize/js/autoptimize_single_a7ce780949735c20349e45ceae03a2b6.js?ver=3cdb22ea051a2fae380a7ecc49f2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\250341cfbf7035da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33758
Entropy (8bit):	5.567189626906524
Encrypted:	false
SSDEEP:	384:GCVGf/nPLoWKBVTeUtdFgGeRUUnRzuTEtcR2o6F4YQmh1fwPuo:7soWKBVZdOnRUwzV2GF4IVo
MD5:	B08251DED47818EA0A667EEE342DF74C
SHA1:	171948BB3121E0089AE810532EE7E7B910AFE25A
SHA-256:	5CD050AE3BC223016B6C23F11340872351CA8CF914766EF529F73A06E2233970
SHA-512:	C869696E2C10655E7B4ABFDA7E5F83BF8953586660D35DD542D3F8C43E2CD372D91CCAE0CF861EC99C8FEFE7897FDDC86B2D9E8EE1FE1E9700BB1B6B4FA8E245
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....e....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/4/intl/de_ALL/onion.js .https://brennergrill.de/..&$/.....c4.....P.....O..Q....0.PH..R$)..." .K..A..Eo.....&.....A..Eo.....'..c....O....0...UYKa.....D.....x.....(S.H..`H.....L`.....Q.@.....google....QbB..#....maps. .Qd29Q....__gjsload__...Qc...?....onion....(S.%..`.....L`.....1.Rc.....Qbn....._.....Qb2.Qm....MG....Qbn..3....uBa...QbR.....vBa...Qb.....OG....QbR^.....w Ba...QbR)xn....xBa...QbR.Ln....$G....Qb.7U^....aH....Qb..l....bH....Qb>PgC....yBa...Qb.....cH....Qb..X.....zBa...Qb..I?....ABa...Qb.....BBa...Qb..?.....CBa...Qb.P.O....DBa... Qb.\'.....EBa...Qb.....GBa...Qb.....HBa...Qb6.....KBa...Qb.0F%....eH....Qb"7.....MBa...Qbb.@D....OBa...Qb..L.....RBa...Qb.....NBa...Qb.'.....PBa...Qb...f....SBa...Qb.e..... .QBa...Qb.....TBa...Qb".D.....fH....Qb.`....hH....Qb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27280eea6a4e74a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	32527
Entropy (8bit):	5.737723252635494
Encrypted:	false
SSDEEP:	384:qzSbQSLSERbexw7e8NS74wYkpVDmLZh1Ra5ORn3YQ0RA90U5r2FI481+0O82:uSbQGixOelTYkpVDMDzzV0O90U5PA82
MD5:	2B9216C4437B894B96162C7CA6674B52
SHA1:	25B2FB5692297F57D667B224B6758C98774052D2
SHA-256:	C23786F6AD78E990AA23F7802415253B75CC0A64EA6BD18F8B3510D6ADF8BAEF
SHA-512:	6ADF6E735694DF931EB0D137308064C0BB4B83A44A6F898D4638917397A29B3348EB7DA1618ECDC28CA942A53F9ECAB97F84DDF888BE243E3ADF4598E96A056
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27280eea6a4e74a6_0	
Preview:	0\r..m.....g....._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/4/intl/de_ALL/marker.js .https://brennergrill.de/+...&$/.....3.....b'N.-.l.....8..2....^.....A..Eo.....Wq.'.....A..Eo.....'.6.....O....`}...nv.....(S.H..`H.....L`.....Q.@.....google....QbB..#....maps..Qd29Q....__gjsload__...Qc^..C....marker...(S....`.....=.L`.....).Rc.....Qbn....._.....Qb...*....Nza...Qb>t.....Oza...Qb.....UF....Qb.2\.....VF....Qb>.....Pza...Qb.Y^7....Qza...QbZ.p.....Rza...QbrjGe....YF....Qb.\.....ZF....Qb.S.z....Sza...Qb...c....Tza...Qb."......$F....Qb.....aG....Qb...&....bG....Qb.w*.....Uza...Qb.....cG....Qb.....Wza...Qb.....fG....Qb....Vza...QbV.....Xza...Qbz.....Zza...Qbf.....mG....Qb.~o.....gG....Qb.Z/3....dAa...Qb..u.....hAa...Qb..SJ....$za...Qb.B.....iG....QbnKE]....kG....Qb.p.....bAa...Qb..\....eAa...Qb.....jG....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27dcf1f8d1e442d2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	90224
Entropy (8bit):	5.924761657502779
Encrypted:	false
SSDEEP:	1536:9mB7a46AbpXEhwnrEEU4+kK2gv8R4I5MeHeSC1f25UN90OkGtLXu0+Uo/P:0IAhEWrEa48qVSo+cltzu0bQP
MD5:	A5EABB208F50951490A02ED57F1E4BE5
SHA1:	F786A870F2C10604610BACCABD4DCA6077A80B41
SHA-256:	FE36E1C6D39C8BBBA5FA6A012B629813B637EF777988DA3F9BB421DBCB2E1C23
SHA-512:	D966433482DF64ABC0AA8DEAA4AD0BD89F11375D20EE7A805A14F3B079881B68412584E5CC8DAC9CEC2FCA24E46E6DB10319C20B58E1A30E6BB837DB0F8F6421
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....<....E90E65336E5828A7B03AAA57D836DB29874B7811BEE6D6BF8A1DA9735F2A0C9A.....'.....O ... _....m.....H.....(S.H..`H.....L`.....Q.@..|f....google....Qb.Mw.....maps..Qd.X.....__gjsload__...Qb6 .)....map..(S.....`.$.....L`.....E.Rc.....F.....Qb.C}]...._.....Qb..U.....hs....Qb6.<=....Cia...Qb..N.....is....Qb.c.^....js....QbZ..J....Dia...Qb...r....ks....Qb~..e....Eia...Qb~.....Fia...Qb.....ls....Qb.lN.....Gia...Qb>,.7....Hia...Qb."..k....Iia...Qb.;.....Jia...Qb..*L....Kia...Qb.Z.3....Lia...Qb~.....Mia...Qb.....Nia...Qbzq.....ms....Qb.@.3....Oia...QbN.....ns....QbR.IR....Pia...Qb.n.....os....Qb.d.]....Qia...Qb..m.....Sia...QbF..z....Tia...QbZ..u....Uia...Qbr.....Via...QbB.....Wia...Qb.....ps....Qb.g.^....qs....QbZ@.....Xia...Qb.>.....rs....Qb.....ss....Qb.....ts....Qb.....Yia...Qb...Z....Zia...Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\28a9f1935422018f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	413
Entropy (8bit):	5.943219357351551
Encrypted:	false
SSDEEP:	6:mWhXYGLJvAscGyQ+wyo3UIadTsOJeVAiuY/gjdSrAZ8tlhK6tU9KV68SjerBRESb:RewxUPThJAA3YydSrNr2V+iSrg
MD5:	A1B51B574425CB6B137DC4BD73282DE5
SHA1:	FD2E850B87DA72E771EF87B6B36FA2EB81A3CEB1
SHA-256:	2FD7EB0041CBF17BE1ECFD3D85DCA2DC95D262707022F7F653C0E8CD415D1D4A
SHA-512:	A6B4CE808C1EF2AF42EBC035356DEEF6B5815FE6393361404E4C1F5FD835AE967651649F15729BD6A0EE16A79A8577E84C4DD09C97B78EEB8C8FA956AF74D5D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor/assets/js/frontend-modules.min.js?ver=3.2.4 .https://umstellungsverfahren-de-corona.com/B...&$/...../.^4Bp...C..[.-.!Zl..4..0...OC.A..Eo.....A..Eo.....B...&$/.....FE6AFCDA876AD9430108DA1A165E101AD1A1712A9C37DC495B446D6267FF285B./.^4Bp...C..[.-.!Zl..4..0...OC.A..Eo.....I...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2abc212c37dc300f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92744
Entropy (8bit):	5.997365883708711
Encrypted:	false
SSDEEP:	1536:wf9wgpwj9+PxFIf9g4+FwjSBURn6vdrcDTMdKtV52e6Rofc:wigajkPIK1oiKtDv4Yc
MD5:	9D663BDE54356A1AC39309C1E81FD468
SHA1:	AC2FB8C7C1DE9D7EA49FED849028BE3AC858EA3B
SHA-256:	361E51EB8896C959B2A3A41EA536BD53286F6F4C2790A31F427A2C7BA6F4DDDE
SHA-512:	78756BFCF5EA92E3BCFACA96A7030D832322C01EFB24C59022CDABA3BAAC716C5234CFB7F16F543CC2880D1CA333FB2D5085FA679D378BA1E787A3B464C9ECA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2abc212c37dc300f_0	
Preview:	0\r..m.....@.....O.....5741CAA7818DAC039DB41321073172497B1C3EDAFEA76919DF10620B49A698C5.....'..j....O ....h.....o..... ... . (.....`.....(S.H..`H.....L`.....Q.@..|f....google....Qb.Mw.....maps..Qd.X.....__gjsload__...Qcv.....controls.(S.....`.;.....L`.....Rcx..... ....Qb.C}]...._.....Qbz.>?....zra...Qb.....nC....Qbv7.;....Ara...Qb>=.O....oC....Qb6.....pC....Qb^.....qC....Qb..v.....rC....Qb.....Bra...Qb.l.]....sC....Qbj.[*....Cra...Qbr..... tC....Qb^z._.....uC....Qb.>.G....Dra...Qb.....Era...Qb..c.....Fra...QbN.u.....Gra...Qb...2....vC....Qb&.....Ira...Qb.m|....wC....Qb.=.>....xC.....Qb./.....yC....Qb..G.....AC....Qb6.... ..Jra...Qb.....Kra...Qb..mh....Lra...Qb.....Mra...Qb.e\....BC....Qb.HQ&....CC....Qb..U....DC....QbN..@....EC....QbRCe.....Nra...Qb..`....Ora...Qb^h.....FC....QbV.....GC... .Qb2O.....HC....Qb...2....Rra...Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d21c84a287c79fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14745
Entropy (8bit):	5.862217774116188
Encrypted:	false
SSDEEP:	192:Pj5uuIGxpGaZcRA9Ka11pWLTVMA3wRPzjclHOTNV12Jyy6c4JcnLTT9+E5:bTtxph8EK5rwhX0Xf9r5
MD5:	E995A8A0CFBC4F6CEF8F2DD200B0D3B3
SHA1:	D5CAAD7289FAAE70BF1AFD614EAE099ACD7A72B7
SHA-256:	A434961F29D472D7464D099EC8432779B7D55F31808A1C83CCF3D6BC0B9D4D07
SHA-512:	C4865FA61A901F686FA1E7CE6E7264563AED861503016A3CD71C3712BBF958C16E04F11F510A6BE91123510BC24CD7FD271DBB1E044C5F4BD5543E49CD640D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...._keyhttps://www.bayerischerhof.de/typo3temp/assets/compressed/merged-5f325d6ffd932be1d9fc5cd1aa5e2539-a22122de4f2c59e4661cc38f6e348caf.js?1624546793 .https://umstellungsverfahren-de-corona.com/...&$/.....c..... ...I.U.Q@0.2._...h...&B.....A..Eo.....$.4@.....A..Eo.....'.=,....O..... 7..;.$h.....(S.d..`.....0L`.....Qc.....window.....a>.....Qd.....asyncLoading...a.....Qc..R.....enabled.G..Qc...%....autoA11y...a.....G..Qc..... baseUrl..(QhF..A....https://ka-p.fontawesome.com..Qd..-0....baseUrlKit...(Qh.....https://kit.fontawesome.com.. Qf2&F.....detectConflictsUntilF..Qd2.`.....iconUploads.. ..a.....Qb..,.....id..`.`....Qcr^.:.....license...Qb&.....pro...Qc>.....method....Qb..4.....css...Qc.U.....minify.....a.....G..Q.@R.\.....token.....Q.P.....50c4862801....Qd..R ....uploadsUrl...0Qj*,..#...https://kit-uploads.fontawesome.com...Qe.[I...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31c7ca0604ee4197_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	121784
Entropy (8bit):	5.616506053760636
Encrypted:	false
SSDEEP:	1536:LCYpjvpGxJzW9gh2v7BqOQZikd+eoe4Rf861P6grp5i3qpW:LCYpbpGbzWTqOdEPi8aE
MD5:	3AB53649FF71F9A423002F4DD4BFEEF9
SHA1:	569ECAC611A9CFC614109CAD71F89C4CD6167096
SHA-256:	62411CDC5EC3735C7632B99039109C5544A3048F94D7035E5ABB3EFC43B75F6D
SHA-512:	642B6EDE0F7B1EB96F4A437825750F34B045A939F6B3B3F3F03EA9E1F8DB36FC3BE5BC61E102A3AEA4D48022681FA5494073476F0074BBE220E968513F4A8F60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....69D9FE25BBFC22512B1C423CDE1ACA08CF49AE00E8E26CCD56C79D69679DEF35.....'.i.....O(...H...Y`Z~.....`..... .....@.....(S.....`V.....L`.....QbFT.&....self.$Q..V..R....webpackChunkelementor.....Qb.....push.....`.....L`.....` .....Ma.....a.....`.....L`.....`.....Mb.....2..D....Y...b.....hI..C`.'..C`.A..C`.9..C`....C`....C`....C`.@..C`J...C`. ..C`.*..C`.@..C`....C`&I..C`....C`(E..C`N...C`....C`.F..C`.B..C`X 4..C`N!..C`.9..C`F>..C`....C`....C`VL..C`.5..C`.I..C`.#..C`Z...C`.M..C`(7..C`.F..C`....C`h7..C`2B..C`>...C`.;..C`....C`.&..C`....C`.4..C`.J..C`.H..C`$...C`.9..C`.-..C`...C`....C`. ...C`zA..C`.;..C`.:..C`.H..C`";..C`x@..C`....C`....C`>!..C`....C`.8..C`*I..C`.4..C`P...C`....C`....C`....C`....C`....C`....C`,...C`6...C`....C`....C`&>..C`....C``-..C`r"..C`....C`~)..C`,G..C`.(..C `....C`.6..C`....C`.D..C`2*

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\366bad7cddd89322_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	387
Entropy (8bit):	5.701680999100277
Encrypted:	false
SSDEEP:	6:mOMEYArn845BJzy2cA0n845BJzy2cCNpUv0X7gWg2IgLYPE8hK6t:LVHfzfclfzfcCNpauJYX
MD5:	A70F31735C8805422CAF941FDA0086B7
SHA1:	77AABB3612BDC56738C3900F2D855F4456B76660
SHA-256:	8395586B7FFC0B773057E11A9B6324A1F3B403FBE168D208DADC914E700A63A0
SHA-512:	FD55ADDBD3ABD8A17392196352EC59853FCCD03E8CB8B1DB1765DD6095F148ACACE6C9399CCB4DDD8DBAF58F05D0CC72818AC7D59A13AE084D93C6C4773 907
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://de.yoordi.app/vendors~CARD10~CARD2~CARD3~CARD4~CARD5~CARD6~CARD_1~DEMO~DINEIN~HOME~PICKUP~PREVI EW~TAKEAWAY/vendors~CARD10~CARD2~CARD3~CARD4~CARD5~CARD6~CARD_1~DEMO~DINEIN~HOME~PICKUP~PREVIEW~TAKEAWAYf2bd57 525d8d73dbcd66.js .https://yoordi.app/r..&$/.....b.....+<.~.Mx.ID<.L..x=.A.....A..Eo.....&+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\366bad7cddd89322_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3793e761c16ab2b3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1430
Entropy (8bit):	5.61013311556078
Encrypted:	false
SSDEEP:	24:fGm5YpsdP91ayqR4F7O6SmaPEI+2+Z4cefom7P9mZ:/YpsJ38RCid8IP+IoAAZ
MD5:	DB3ACB67E25EF6EAB064C42BDDFE9A59
SHA1:	3D4053B326EB29A0693CFECF2952752E35639CC4
SHA-256:	D786D13EF46080F28B0C482CABF9DA1CE70C367DC2341AED4999A419022E4F98
SHA-512:	5EB0F27BB694F8A979351363C251792ECCEE0B4CBA5DD75443FE978F27993A4583C74DFE46D5B5AEB0C8F8D95CE2298E78AD67AED7DC05909A596EEBA76AE1 3F
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=3.2.2 .https://umstellungsverfahren-de-corona.com/...&$/.....-..4-0..B.._.P*W!.K.?.....O....A..Eo.....{6.....A..Eo.....&$/.0.....'.....O.....Q+.....(S.4..`$.....L`.....(S.P.`\. ...$L`.....8Rc.....Q.@.c|....Sticky..a$.....l`....Da....r3...(S.....a ...z.....$. ...$.'....',...,....-.....+.....d.....d.....d..... .....!..@.-....\|P.....m...https://www.brennergrill.de/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=3.2.2...a.....D`....D`D...D`.....`>...&...&....&..Q.. D&.(S.....Pd.....$.fn.sticky.a.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\385b76f9136a9938_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	49231
Entropy (8bit):	5.350647348312567
Encrypted:	false
SSDEEP:	1536:o0bOkNyIfMUqm2+5a5R4XjOXgo+LfydfEW:o0bOkNTfMUr2+5a5eXjOXozyWW
MD5:	8C08A1FD81760B8BE6AC6D3F413F3883
SHA1:	249148BE0ABF02926088C641D82C6447AD9AD6B7
SHA-256:	F9F96C1306EA57BB3396165B5DE73625E48A5CDBD5A3C2006DA14E4D32370845
SHA-512:	4C48DFE2F2B2453D96E97F520513D611F75C9BE8F80196918E737E1E0734A3A6DD5DBDE8C085362EE69E385D536E3400DCEB0A6CB40B62EF9F5BDB0354BD9B 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....._keyhttps://maps.googleapis.com/maps/vt?pb=!1m4!1m3!1i15!2i17435!3i11370!1m4!1m3!1i15!2i17435!3i11371!1m4!1m3!1i15!2i17435!3i11372!1m4!1m3!1i15!2i17436!3i11370!1m4!1m3!1i15!2i17436!3i11371!1m4!1m3!1i15!2i17437!3i11370!1m4!1m3!1i15!2i17437!3i11371!1m4!1m3!1i15!2i17438!3i11370!1m4!1m3!1i15!2i17438!3i11371!1m4!1m3!1i15!2i17439!3i11370!1m4!1m3!1i15!2i17439!3i11371!1m4!1m3!1i15!2i17436!3i11372!1m4!1m3!1i15!2i17437!3i11372!1m4!1m3!1i15!2i17438!3i11372!1m4!1m3!1i15!2i17439!3i11372!1m4!1m3!1i15!2i17440!3i11370!1m4!1m3!1i15!2i17440!3i11371!1m4!1m3!1i15!2i17440!3i11372!2m3!1e0!2sm!3i561286316!3m12!2sde!3sUS!5e18!12m4!1e68!2m2!1sset!2sRoadmap!12m3!1e37!2m1!1ssmartmaps!4e3!12m1!5b1&callback=_xdc_._qeincr&key=AIzaSyDUxnfOO7dcYC8B01tCsfRMmVrLqXpecWA&token=68738 .https://brennergrill.de/...&$/.....\5.....<b....[.....D.0.....,M.....A..Eo.....A..Eo.....'.....O.....#x... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\394a7c63c56154a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5846
Entropy (8bit):	5.889496844588535
Encrypted:	false
SSDEEP:	96:dFwGrparaaTqUF98T2gB5GS4Ryrw6MyftgjCcWMpEtxe2lqsazozwP:/pQTqUFnTSs6w6Myfuj1jWtxe2lqFzoY
MD5:	A129E416A3128848F8467F31D9BF970A
SHA1:	D1D4213C6D71000407888CB1E0C232B4A04D4CCA
SHA-256:	18B53AE9A79BF56E38A3CCA58A6CBBCCB81C7F17A601534E5924DDDEBE540089
SHA-512:	574B0BBD336C262F7AAA3D6A0A97010165F9510A22054B518760BC7363D721AC698DAAB370BE3EC99C706429B3071F6A516B2D4CF52F18BE3E04EDD8BE2EA42 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\394a7c63c56154a9_0	
Preview:	0\r..m....._keyhttps://www.brennergrill.de/wp-content/themes/astra/assets/js/minified/style.min.js?ver=3.4.0 .https://umstellungsverfahren-de-corona.com/...&$/.....>.....l.3.63.e.....]...._...6}U.)....A..Eo.....A..Eo.....'..(....O.... ....(.....L.....(S.h..`.....<L`.....L`.....QeR.....astraGetParents...QdV..h....getParents....Qe.vk.....astraToggleClass..Qd.7.....toggleClass.. Qf..*.....astraTriggerEvent....(S.....a.....d.....E.@.-....lP.....]...https://www.brennergrill.de/wp-content/themes/astra/assets/js/minified/style.min.js?ver=3.4.0...a.....D`....D`,...D`.....`<...&...&....D&.(S.....a.....E....d.....&.(S.....q.a....%....E.d.....&.(S.....a:.....E.d.....&.(S.X..`l.....L`.....(S...Ia.....Qb...6....e...E.d.....Qc.....window....QdZ.....CustomEvent...Q.@b.7.....Event...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b2d43f2be68fc53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	90224
Entropy (8bit):	5.923636473237861
Encrypted:	false
SSDEEP:	1536:WQDveaNTO8gctfOsw3K9iEktSy2m3c5fP1teAGQCF32siOFcULXv5fF/O:9vvOYfOJK9i/cdoQwGZUzv5fdO
MD5:	C869044A017FBDB47D4AE78BE1CFD07C
SHA1:	CF6A73C5C910C28D11DF175776A19BDD57256817
SHA-256:	F51738F2C3881BF517DEC98A1AA0CD2EE0ED6CC40FA92703EA080F2859BECFEF
SHA-512:	13EAFB79B8DEC211CD375A6C3737C556B5143284454B4733FBDD5657B8488AAAAFA0B4E060F8E24417054A3C57EDAFB848E4C6EE7743FEDE51EA96AFCA916F40
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....?....21A48FAFA458BF8F7AFD6BCA3B6543F9C33CD7A82DB8EE6E9A67FB7056E537C3.....'.....O ... _....j.....H.....(S.H..`H.....L`.....Q.@.....google....QbB..#....maps..Qd29Q.....__gjsload__....QbbEj....map..(S.....`.$.....L`.....E.Rc.....F.....Qbn....._.....Qb6..g....hs....Qb...Z....Cia...Qbb.j\....is....Qb.....js....Qb.9A....Dia...Qb..p.....ks....Qbv.3.....Eia...Qb.0.....Fia...Qb.~....ls....Qbz.Y.....Gia...Qb.m).....Hia...Qb...V....Iia...Qb.....Jia...Qb..m.....Kia...Qbrpn.....Lia...Qb.IV.....Mia...Qb*J2.....Nia...Qb.hh.....ms....Qb.....Oia...Qb.v.....ns....Qb.....Pia...Qb~h.d....os....Qb.....Qia...QbF.1.....Sia...Qb.-?.....Tia...Qbz.....Uia...Qb..uZ....Via...Qb..n.....Wia...Qb..d.....ps....Qb...!....qs....Qb.V.t....Xia...Qb.5.V....rs....Qb6.p.....ss....Qb.....ts....Qb.R.....Yia...Qb...t....Zia...Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f6a4243f664d955_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	383
Entropy (8bit):	5.940640879649927
Encrypted:	false
SSDEEP:	6:mgHEYZHfY7ttTUNJeVAiuYAgdKg0RM4DnK6tdiubtjiXASg0RM4F+:NJ/cTUNJAA3YRsRMKpLi2tjiXNHRM4+
MD5:	16E86A9133AD5E0BD180DCDF1CFD7A8E
SHA1:	FE1CE13897FADAFF9F66DA16DFEC51EB1859551E
SHA-256:	6B50F41A2C71EA8ECAF27E5ADEF17C2262253C1E8E949F60206AC563A5F8F901
SHA-512:	2F40F39DF9C118C77C2C4AB43F1A0D65BD7AE48C96ECAC0DF94E949FA4B90F2274CA6F10F1D6FFBF3231A419D8E53BE8DFA06EBC6312ECDC8B82B07393CEECE4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....1'p...._keyhttps://maps.googleapis.com/maps-api-v3/api/js/45/4/intl/de_ALL/map.js .https://umstellungsverfahren-de-corona.com/....&$/.....tQ..0...U,....PD..._.....G(...A..Eo.....Q.<.....A..Eo.....&$/.._..E90E65336E5828A7B03AAA57D836DB29874B7811BEE6D6BF8A1DA9735F2A0C9A.tQ..0...U,....PD..._.....G(...A..Eo.....8.L.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 25, 2021 07:18:43.450268030 CEST	192.168.2.4	8.8.8.8	0x944c	Standard query (0)	sparkasse.umstellungsverfahren-de-corona.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:46.654604912 CEST	192.168.2.4	8.8.8.8	0x3f61	Standard query (0)	www.brennergrill.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:51.339891911 CEST	192.168.2.4	8.8.8.8	0x2573	Standard query (0)	www.brennergrill.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:52.683693886 CEST	192.168.2.4	8.8.8.8	0x3c16	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:03.972412109 CEST	192.168.2.4	8.8.8.8	0xf95c	Standard query (0)	www.bayerischerhof.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:04.591463089 CEST	192.168.2.4	8.8.8.8	0x2cac	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:05.008204937 CEST	192.168.2.4	8.8.8.8	0x7f89	Standard query (0)	ka-p.fontawesome.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:05.483951092 CEST	192.168.2.4	8.8.8.8	0xc49f	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:05.758694887 CEST	192.168.2.4	8.8.8.8	0xbb57	Standard query (0)	consent.cookiebot.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:06.375962973 CEST	192.168.2.4	8.8.8.8	0x84f2	Standard query (0)	consentcdn.cookiebot.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:09.313419104 CEST	192.168.2.4	8.8.8.8	0x8cbb	Standard query (0)	www.bayerischerhof.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:09.968041897 CEST	192.168.2.4	8.8.8.8	0x26ba	Standard query (0)	de.yoordi.app	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:12.908690929 CEST	192.168.2.4	8.8.8.8	0xb8d3	Standard query (0)	de.yoordi.app	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:18.082892895 CEST	192.168.2.4	8.8.8.8	0xb920	Standard query (0)	www.brennergrill.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:19.996962070 CEST	192.168.2.4	8.8.8.8	0x5d37	Standard query (0)	scontent-ham3-1.cdninstagram.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:22.757965088 CEST	192.168.2.4	8.8.8.8	0x1465	Standard query (0)	scontent-ham3-1.cdninstagram.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:24.403924942 CEST	192.168.2.4	8.8.8.8	0xf05f	Standard query (0)	www.brennerkitchen.de	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:26.280494928 CEST	192.168.2.4	8.8.8.8	0x8b37	Standard query (0)	sparkasse.umstellungsverfahren-de-corona.com	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:27.551275015 CEST	192.168.2.4	8.8.8.8	0x3ab7	Standard query (0)	www.brennerkitchen.de	A (IP address)	IN (0x0001)

DNS Answers

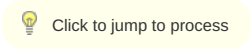
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 25, 2021 07:18:43.773874998 CEST	8.8.8.8	192.168.2.4	0x944c	No error (0)	sparkasse.umstellungsverfahren-de-corona.com		47.243.138.168	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:46.716581106 CEST	8.8.8.8	192.168.2.4	0x3f61	No error (0)	www.brennergrill.de		217.31.83.134	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:51.410331964 CEST	8.8.8.8	192.168.2.4	0x2573	No error (0)	www.brennergrill.de		217.31.83.134	A (IP address)	IN (0x0001)
Jun 25, 2021 07:18:52.760987997 CEST	8.8.8.8	192.168.2.4	0x3c16	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:18:52.760987997 CEST	8.8.8.8	192.168.2.4	0x3c16	No error (0)	googlehosted.l.googleusercontent.com		142.250.74.193	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:02.277205944 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:04.071110010 CEST	8.8.8.8	192.168.2.4	0xf95c	No error (0)	www.bayerischerhof.de		85.214.113.241	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 25, 2021 07:19:04.654092073 CEST	8.8.8.8	192.168.2.4	0x2cac	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:05.067486048 CEST	8.8.8.8	192.168.2.4	0x7f89	No error (0)	ka-p.fontawesome.com	ka-p.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:05.541913986 CEST	8.8.8.8	192.168.2.4	0xc49f	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:05.816431046 CEST	8.8.8.8	192.168.2.4	0xbb57	No error (0)	consent.cookiebot.com	consent.cookiebot.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:06.432454109 CEST	8.8.8.8	192.168.2.4	0x84f2	No error (0)	consentcdn.cookiebot.com	consentcdn.cookiebot.com-v1.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:09.385250092 CEST	8.8.8.8	192.168.2.4	0x8cbb	No error (0)	www.bayerischerhof.de		85.214.113.241	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:10.062943935 CEST	8.8.8.8	192.168.2.4	0x26ba	No error (0)	de.yoordi.app	yoordi-de.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:10.062943935 CEST	8.8.8.8	192.168.2.4	0x26ba	No error (0)	yoordi-de.azurewebsites.net	waws-prod-am2-381.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:10.062943935 CEST	8.8.8.8	192.168.2.4	0x26ba	No error (0)	waws-prod-am2-381.sip.azurewebsites.windows.net	waws-prod-am2-381-93f5.westeurope.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:12.962835073 CEST	8.8.8.8	192.168.2.4	0xb8d3	No error (0)	de.yoordi.app	yoordi-de.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:12.962835073 CEST	8.8.8.8	192.168.2.4	0xb8d3	No error (0)	yoordi-de.azurewebsites.net	waws-prod-am2-381.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:12.962835073 CEST	8.8.8.8	192.168.2.4	0xb8d3	No error (0)	waws-prod-am2-381.sip.azurewebsites.windows.net	waws-prod-am2-381-93f5.westeurope.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)
Jun 25, 2021 07:19:18.146239042 CEST	8.8.8.8	192.168.2.4	0xb920	No error (0)	www.brennergrill.de		217.31.83.134	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:20.086070061 CEST	8.8.8.8	192.168.2.4	0x5d37	No error (0)	scontent-ham3-1.cdninstagram.com		157.240.210.63	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:22.805607080 CEST	8.8.8.8	192.168.2.4	0x1465	No error (0)	scontent-ham3-1.cdninstagram.com		157.240.210.63	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:24.475507975 CEST	8.8.8.8	192.168.2.4	0xf05f	No error (0)	www.brennerkitchen.de		217.31.83.134	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:26.338207006 CEST	8.8.8.8	192.168.2.4	0x8b37	No error (0)	sparkasse.umstellungsverfahren-de-corona.com		47.243.138.168	A (IP address)	IN (0x0001)
Jun 25, 2021 07:19:27.619225979 CEST	8.8.8.8	192.168.2.4	0x3ab7	No error (0)	www.brennerkitchen.de		217.31.83.134	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5144 Parent PID: 4944

General

Start time:	07:18:39
Start date:	25/06/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://sparkasse.umstellungsverfahren-de-corona.com/ALC81OPACG'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6152 Parent PID: 5144

General

Start time:	07:18:41
Start date:	25/06/2021
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 --field-trial-handle=1564,12754223477804659990,14032383889391973514,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 7576 Parent PID: 5144

General

Start time:	07:19:39
Start date:	25/06/2021
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=quarantine.mojom.Quarantine --field-trial-handle=1564,12754223477804659990,14032383889391973514,131072 --lang=en-GB --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3624 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: AcroRd32.exe PID: 4176 Parent PID: 5144

General

Start time:	07:19:40
Start date:	25/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Downloads\PfifferlingeMittags.pdf'
Imagebase:	0xc70000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Moved

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 7764 Parent PID: 4176

General

Start time:	07:19:41
Start date:	25/06/2021
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' --type=renderer /prefetch:1 'C:\Users\user\Downloads\PfifferlingeMittags.pdf'
Imagebase:	0xc70000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A

Copyright Joe Security LLC 2021

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: RdrCEF.exe PID: 7776 Parent PID: 4176

General

Start time:	07:19:55
Start date:	25/06/2021
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:	0xa30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: RdrCEF.exe PID: 7880 Parent PID: 7776

General

Start time:	07:20:00
Start date:	25/06/2021
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' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,4124687374001318311,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=14220142155135163333 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=14220142155135163333 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xa30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 6864 Parent PID: 7776

Copyright Joe Security LLC 2021

General

Start time:	07:20:02
Start date:	25/06/2021
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' --type=gpu-process --field-trial-handle=1692,238294790207997486,412468737400131831 1,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences =KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAA EAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAA AAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAA AAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=9558252731115271562 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xa30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 6528 Parent PID: 7776

General

Start time:	07:20:07
Start date:	25/06/2021
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' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,4124687374001318311,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=15100887731048530030 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=15100887731048530030 --renderer-client-id=4 --mojo-platform-channel-handle=1824 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xa30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RdrCEF.exe PID: 4204 Parent PID: 7776

General

Start time:	07:20:09
Start date:	25/06/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1692,238294790207997486,4124687374001318311,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1029686541791480953 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1029686541791480953 --renderer-client-id=5 --mojo-platform-channel-handle=1984 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xa30000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021