

ID: 433022
Cookbook: browseurl.jbs
Time: 06:46:02
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut 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: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
Static File Info 42
No static file info 42
Network Behavior 42
Network Port Distribution 42
TCP Packets 43
UDP Packets 43
DNS Queries 43
DNS Answers 44
HTTP Request Dependency Graph 50
HTTP Packets 50
HTTPS Packets 51
Code Manipulations 58
Statistics 58
Behavior 58
System Behavior 58
Analysis Process: chrome.exe PID: 1736 Parent PID: 4852 58
General 58
File Activities 58
Registry Activities 58
Analysis Process: chrome.exe PID: 5584 Parent PID: 1736 58
General 58
File Activities 58
Registry Activities 59
Analysis Process: chrome.exe PID: 7080 Parent PID: 1736 59
General 59
Analysis Process: chrome.exe PID: 2792 Parent PID: 1736 59
General 59
File Activities 59
Registry Activities 59
Analysis Process: chrome.exe PID: 8148 Parent PID: 1736 59
General 59
File Activities 60
Registry Activities 60
Analysis Process: AcroRd32.exe PID: 5724 Parent PID: 1736 60

Copyright Joe Security LLC 2021

General 60
File Activities 60
File Created 60
Registry Activities 60
Key Created 60
Key Value Created 60
Analysis Process: AcroRd32.exe PID: 7576 Parent PID: 5724 60
General 60
File Activities 60
Registry Activities 61
Analysis Process: RdrCEF.exe PID: 7304 Parent PID: 5724 61
General 61
File Activities 61
File Read 61
Analysis Process: RdrCEF.exe PID: 2220 Parent PID: 7304 61
General 61
Analysis Process: RdrCEF.exe PID: 5124 Parent PID: 7304 61
General 61
Analysis Process: RdrCEF.exe PID: 4012 Parent PID: 7304 62
General 62
Analysis Process: RdrCEF.exe PID: 6140 Parent PID: 7304 62
General 62
Disassembly 63
Code Analysis 63

Copyright Joe Security LLC 2021

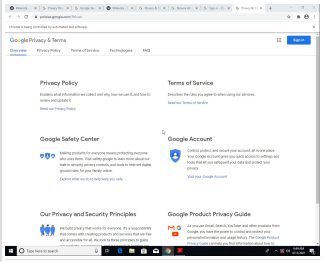
Analysis Report http://app.milanote.com/1LQWMe1tFoG…

Overview

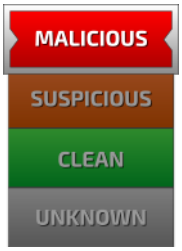
General Information

Sample URL:	http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut
Analysis ID:	433022
Infos:	

Most interesting Screenshot:



Detection

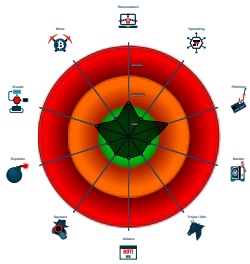


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Contains functionality to access load…
- Drops files with a non-matching file e…
- Found iframes
- Unusual large HTML page

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 1736 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5584 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7080 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2792 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6740 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 8148 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=quarantine.mojom.Quarantine --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3156 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - AcroRd32.exe (PID: 5724 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Downloads\google_terms_of_service_en_eu.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - AcroRd32.exe (PID: 7576 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Downloads\google_terms_of_service_en_eu.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
    - RdrCEF.exe (PID: 7304 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 2220 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1688,10530306713486204241,2167271992676285589,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=16344355117710085358 --mojo-platform-channel-handle=1708 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 5124 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=1688,10530306713486204241,2167271992676285589,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17060473708032021879 --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=17060473708032021879 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 4012 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=1688,10530306713486204241,2167271992676285589,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2108192486941613496 --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=2108192486941613496 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - RdrCEF.exe (PID: 6140 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=1688,10530306713486204241,2167271992676285589,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11960134190916244897 --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=11960134190916244897 --renderer-client-id=5 --mojo-platform-channel-handle=1776 --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:

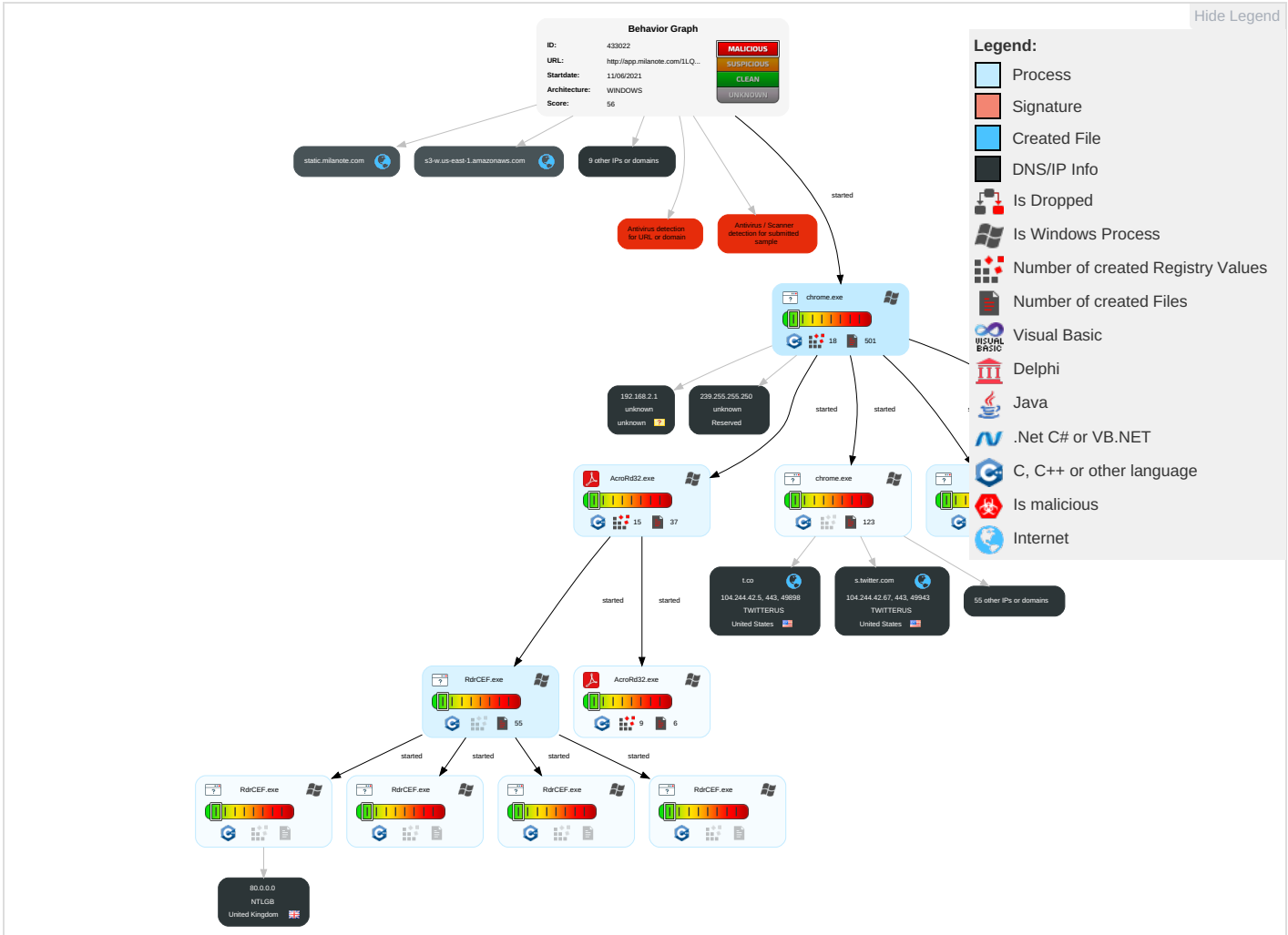
Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

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
Spearphishing Link 1	Windows Management Instrumentation	Path Interception	Process Injection 2	Masquerading 1 3	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Drive-by Compromise 1	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

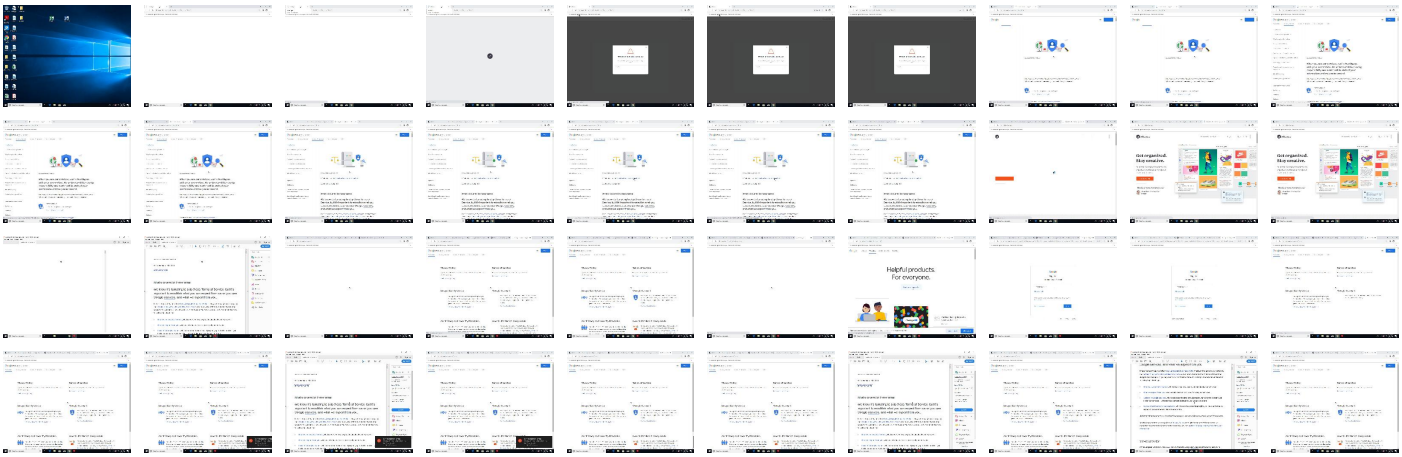
Behavior Graph

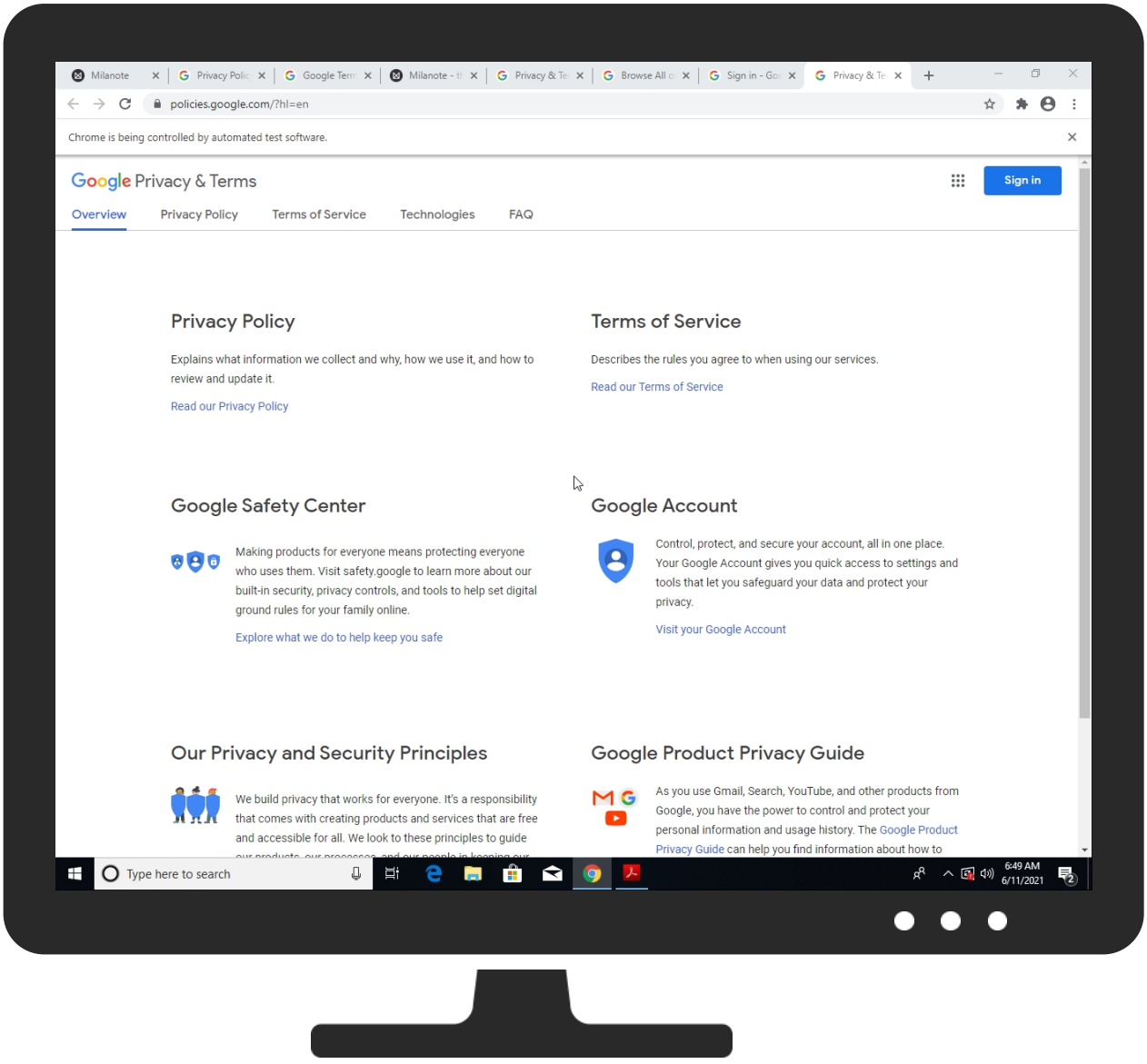


Screenshots

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://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut	0%	Avira URL Cloud	safe	
http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
platform.twitter.map.fastly.net	0%	Virustotal		Browse
about.google	0%	Virustotal		Browse
ghs-svc-https-sni.ghs-ssl.googlehosted.com	0%	Virustotal		Browse
dualstack.com.imgix.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://about.google/intl/en/products/	0%	URL Reputation	safe	
http://https://about.google/intl/en/products/	0%	URL Reputation	safe	
http://https://about.google/intl/en/products/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/Clas	0%	Avira URL Cloud	safe	
http://https://about.google/sn	0%	Avira URL Cloud	safe	
http://https://milanote.comh	0%	Avira URL Cloud	safe	
http://ocsp.rootg2.amazontrust.com08	0%	URL Reputation	safe	
http://ocsp.rootg2.amazontrust.com08	0%	URL Reputation	safe	
http://ocsp.rootg2.amazontrust.com08	0%	URL Reputation	safe	
http://https://about.google/intl/en/products/Browse	0%	Avira URL Cloud	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/k	0%	Avira URL Cloud	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://crl.sca1b.amazontrust.com/sca1b.crl0	0%	URL Reputation	safe	
http://crl.sca1b.amazontrust.com/sca1b.crl0	0%	URL Reputation	safe	
http://crl.sca1b.amazontrust.com/sca1b.crl0	0%	URL Reputation	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://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://ocsp.sca1b.amazontrust.com06	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://https://about.google/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	URL Reputation	safe	
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	URL Reputation	safe	
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/m&c	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/.3/1	0%	Avira URL Cloud	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/favicon.ico$	0%	Avira URL Cloud	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/?	0%	Avira URL Cloud	safe	
http://https://safety.google/)	0%	Avira URL Cloud	safe	
http://o.ss2.us/0	0%	URL Reputation	safe	
http://o.ss2.us/0	0%	URL Reputation	safe	
http://o.ss2.us/0	0%	URL Reputation	safe	
http://https://about.google/s	0%	Avira URL Cloud	safe	
http://https://about.google/l	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/O	0%	Avira URL Cloud	safe	
http://crt.rootg2.amazontrust.com/rootg2.cer0=	0%	URL Reputation	safe	
http://crt.rootg2.amazontrust.com/rootg2.cer0=	0%	URL Reputation	safe	
http://crt.rootg2.amazontrust.com/rootg2.cer0=	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://https://about.google/intl/en_IE/how-our-business-works)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
i.ytimg.com	172.217.18.86	true	false		high
milanote.prismic.io	52.55.94.115	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false	• 0%, Virustotal, Browse	unknown
about.google	216.239.32.29	true	false	• 0%, Virustotal, Browse	unknown
milanote.com	13.224.99.118	true	false		high
scontent.xx.fbcdn.net	157.240.27.27	true	false		high
t.co	104.244.42.5	true	false		high
script.hotjar.com	13.224.99.26	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
photos-ugc.l.googleusercontent.com	216.58.214.225	true	false		high
ghs-svc-https-sni.ghs-ssl.googlehosted.com	142.250.180.243	true	false	• 0%, Virustotal, Browse	unknown
nexus-websocket-a.intercom.io	35.170.0.145	true	false		high
dualstack.com.imgix.map.fastly.net	151.101.114.208	true	false	• 0%, Virustotal, Browse	unknown
d37gvrvc0wt4s1.cloudfront.net	13.224.89.197	true	false		high
app.milanote.com	34.198.55.140	true	false		high
q.quora.com	18.215.205.165	true	false		high
js.intercomcdn.com	13.224.99.75	true	false		high
static-cdn.hotjar.com	13.224.99.122	true	false		high
quora.map.fastly.net	151.101.1.2	true	false		unknown
www.google.de	172.217.18.67	true	false		high
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
stats.l.doubleclick.net	142.251.5.155	true	false		high

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s.twitter.com	104.244.42.67	true	false		high
static.milanote.com	13.224.99.113	true	false		high
widget.intercom.io	13.224.99.109	true	false		high
cdn.amplitude.com	13.224.89.71	true	false		high
api-iam.intercom.io	99.83.219.81	true	false		high
d119wgbtegajwl.cloudfront.net	13.224.99.81	true	false		high
vars.hotjar.com	13.224.99.109	true	false		high
s3-w.us-east-1.amazonaws.com	52.217.92.196	true	false		high
googleads.g.doubleclick.net	142.250.180.226	true	false		high
api.amplitude.com	34.217.196.79	true	false		high
www.milanote.com	13.224.99.118	true	false		high
www.google.ch	172.217.20.3	true	false		high
googlehosted.l.googleusercontent.com	142.250.180.225	true	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
yt3.ggpht.com	unknown	unknown	false		high
a.quora.com	unknown	unknown	false		high
www.blog.google	unknown	unknown	false		high
static.cdn.prismic.io	unknown	unknown	false		high
huntr.in	unknown	unknown	false		unknown
lh3.googleusercontent.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
images.prismic.io	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
accounts.youtube.com	unknown	unknown	false		high
prismic-io.s3.amazonaws.com	unknown	unknown	false		high
www.youtube-nocookie.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut	false		high
http://https://vars.hotjar.com/box-25a418976ea02a6f393fbbe77cec94bb.html	false		high
http://https://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high
http://https://www.youtube-nocookie.com/embed/ZdEIZNg3epQ?rel=0&showinfo=0&theme=light&version=3&hl=en&cc_lang_pref=en&cc_load_policy=1	false		high
http://https://about.google/intl/en/products/	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://app.milanote.com/embed/auth-status	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.89.197	d37gvrvc0wt4s1.cloudfront.net	United States		16509	AMAZON-02US	false
31.13.92.36	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
13.224.99.118	milanote.com	United States		16509	AMAZON-02US	false
151.101.1.2	quora.map.fastly.net	United States		54113	FASTLYUS	false
13.224.99.113	static.milanote.com	United States		16509	AMAZON-02US	false
34.217.196.79	api.amplitude.com	United States		16509	AMAZON-02US	false
13.224.99.26	script.hotjar.com	United States		16509	AMAZON-02US	false
142.250.180.243	ghs-svc-https-sni.ghs-ssl.googlehosted.com	United States		15169	GOOGLEUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.114.208	dualstack.com.imgix.map.fastly.net	United States		54113	FASTLYUS	false
216.58.214.225	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.224.89.71	cdn.amplitude.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.217.92.196	s3-w.us-east-1.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.99.122	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
172.217.18.86	i.ytimg.com	United States		15169	GOOGLEUS	false
52.55.94.115	milanote.prismic.io	United States		14618	AMAZON-AESUS	false
13.224.99.75	js.intercomcdn.com	United States		16509	AMAZON-02US	false
142.250.180.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.180.226	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
35.170.0.145	nexus-websocket-a.intercom.io	United States		14618	AMAZON-AESUS	false
34.198.55.140	app.milanote.com	United States		14618	AMAZON-AESUS	false
13.224.99.81	d119wgbtegajwl.cloudfront.net	United States		16509	AMAZON-02US	false
18.215.205.165	q.quora.com	United States		14618	AMAZON-AESUS	false
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
104.244.42.67	s.twitter.com	United States		13414	TWITTERUS	false
142.251.5.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
13.224.99.109	widget.intercom.io	United States		16509	AMAZON-02US	false
99.83.219.81	api-iam.intercom.io	United States		16509	AMAZON-02US	false
104.244.42.5	t.co	United States		13414	TWITTERUS	false
172.217.20.3	www.google.ch	United States		15169	GOOGLEUS	false
157.240.27.27	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433022
Start date:	11.06.2021
Start time:	06:46:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut
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:	46
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:	mal56.win@76/421@47/36
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.google.com /intl/en/policies/privacy/ • Browse: https://www.google.com /intl/en/policies/terms/ • Browse: https://www.milanote.com/ • Browse: https://policies.google.com/ • Browse: https://www.google.ch/ intl/en/about/products • Browse: https://accounts.googl e.com/ServiceLogin?passive=120 9600&continue=https://poli cies.google.com/privacy?hl%3De n&followup=https://policie s.google.com/privacy?hl%3Den&a mp;hl=en&ec=GAZAoQQ • Browse: https://policies.google.com/?hl=en • Found PDF document • Find and activate links • Close Viewer • Browse: https://www.google.com /intl/en/policies/privacy/ • Browse: https://www.google.com /intl/en/policies/terms/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:46:49	API Interceptor	1x Sleep call for process: chrome.exe modified
06:47:35	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:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

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):	5.640523712918254
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QiKXtWmi7Z+P41TK6tdMen9YOFLvEWdM9QFGKXV2mi7Z+P41T0:vDRM9NpZiEnhDRM9rG2VZiE2
MD5:	BA6E9EA71304900BE8A60B3AEDBF0DE3
SHA1:	660BC618F7177DC088E8914DACE08F64B8D5590E
SHA-256:	C8FD9DDFCCD1C24E9A16DFDE6EB8D38288E4698C7E1B8AAB2CF562FCAFA61E4A
SHA-512:	918314B413409B35E52112CFD666702689529927DC8284AFB3BEDA0ED9EF41AA070E3C3FEC5BFC7159D62310F7F7233E5F35535B30A469307198DE286DF9B409
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....#/....."#.D.|Eb.0.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....Xw.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .X,...#/....."#.D..<c.0.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....6.....

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):	5.5837280488582675
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkalthH1jF8Be7Ywcr1TK6tNii9NqEYOFLvEkl9tw9kUF8Be7Ywc1:V9zeD9PQp9zoY9z9PQ1
MD5:	576332D2222B4B57585DD69BD8DF6A5D
SHA1:	CAA31FD746A9FD5E312CAEC491895F4BA7B6E98A
SHA-256:	F19B668E001D53190C8CA184B4A1DC6223D0CB9ED62030A81FB7430BBCA04F56
SHA-512:	C2771F4D83D96C9C5398984C25ED6D49EAA6B2C742DCC4A7AA1B349E9B3A19BBB5F02F602FF472FF84EBBF2E1A8DDAD31A466B9DAB99C94C3A633CD8A664D4FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...^..#/....."#.D..?a.0.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....t.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .....#/....."#.D.).b.0.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):	5.584828598479534
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFoEfVjvlUo6jWX5yeRVFAFjVFAFD4+vlUo6j:tB4v4Z9jSBWHB4v4MESB
MD5:	BC869EE65B6CD59526DF98E22EA330BB
SHA1:	FEB2C60BA4B2130C2F8FB4C314B9E940440B3175
SHA-256:	4908BD123D81E6216D871B8ACE037A33AA3FA492C6362DF62A8CD477EE16E09B
SHA-512:	C5C01184DE4BCF1C9646C7C4CBDCD84CA5B5AC3AD3A8B3B653B72C842913644D5914283C7C62926873E1EB948D2ACDEEEEE43657ADF1AB6DC28DE534DBB9AFB
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.YCb.0.A..hvD O.N.t@.....n.*..... ....A..Eo.....A..Eo.....E.....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.77c.0.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0.....

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):	5.666119911144176
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RstvX0iWulHyA1TK6tr:IbRkiDc1Wuss
MD5:	833F64A6346206F99148296C74966682
SHA1:	0CFFEEC0CF3766CBA4836768656C85A13E87CF02
SHA-256:	63451FDA96297C0374543F2B30004CE338F60BA26786A39D0879887924107A1F
SHA-512:	92C5AD73B58BB4A438FADC411CC4B01D95522F71B165BBFA3844B3BEB5E9515BC83E4EE584F7B8AA9799834EAB31BF3FBC8E10BCFCD1387763C97B0A166DAF5F
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 .....#/....."#.DT..b.0.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.525981564814881
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuM1XzGrRVyh9PT41TK6t3rt:pyixRu21DSRV41TEtr
MD5:	217DEAF7E246215ECA1A179E8DA6CA57
SHA1:	B39C1A8E4B0A4DE944555E1FB977ACC0EC4BA03F
SHA-256:	0468453B762C34ABEACDA98C529B2C3C549E52C58A7E70897B2EC7E40F5FBA30
SHA-512:	8CF05BD6D3758C179F9E53B0207D5E5CEFC6AE9BD31E2CB7E56932BD23364069209A2442BF716DF6F8B5B1BEF96729ECA1C5B15B5EB6B63CFA35A6818A62BEE6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .[p...#/....."#.D..7c.0.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....6^.].....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.547842448618613
Encrypted:	false
SSDEEP:	3:m+lifll08RzYOCGLvHkWBGKuKjXKoyNjXKLuV5sNndGvco2sZI8xeGvP5m1TK5kc:mvYOFLvEWdhwjQLHGvLZll6P41TK6t9
MD5:	F435E9B817FE3A53A5A6B96C0B7EADCC
SHA1:	15B296D628FF0057460204FE2D171FE2BEDD292D

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
SHA-256:	CE5CF8748D72D48CA1931606F97CFF2D7B057C62AE3FE9439C0E2D0D4FC07D64
SHA-512:	C7EEFF005B1209AF1A3A0BEB851D4BF9BD7561FE60E7F261442052E0353AE8BAAAE287B1AB9DDF41AB11BB16909173E3DC37850910DA738FDC4BB162D6B756B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ..i...#/....."#.D..c.0.A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....a.'.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.496597565668653
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQxPGKXXAkEAV6g1TK6tt:2RHRQCCqk91
MD5:	F6DD9D8C8F3B0B375238D2959A835D24
SHA1:	FCE123516E112642B4B62FDC4B40BE4B591B3BE4
SHA-256:	744370CF7A71943019FDD2B0F329D1FC56ABC7EE11C7967439D98AA48163095B
SHA-512:	D453858D872EC6B12329BEA41138D416A6BCD361224565BDA717FA6CDAE993117A35EF7AE6A583DF9C04DA6DE0ABFCFD036FE5120DC78708FF03E8D23B2DD8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .!v...#/....."#.D)&8c.0.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo.....F.....

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):	5.558612651778491
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLAGWMuR/41TK6tNOYOFLvECMLYT+tidGhMuR/41TK6tj:Z5MXWMuR/El5MpSIMuR/E
MD5:	F8833D88CB8A787B7AB1CF5A9FD5E6D2
SHA1:	88AD1CA37E77A75E1E08B776125A9B3E62957A2D
SHA-256:	F4EA0318348AAA8E278B81A5996B801FFB58FE1B1C2BF3FF5B39F07B604AB51A
SHA-512:	7ADA7038A3E8979A334D4506440052AAAA9FC3776EA8F5A40E234561BAEB3BF97C7914970BC86E28D7EB17B6352F59406AE2352FCE798B521F7522B7743FFB82
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...^..#/....."#.D.I?a.0.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....3q.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .....#/....."#.DSA.b.0.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....5c.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.510796495142273
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtudXoR+by0zBUKSAA1TK6tsF:pRc4R+be
MD5:	B7A3DE175DE5F312CF37DFE40B033502
SHA1:	B8FCD5DE9CD7E65141097F16FFC28ABA7AB0A19B
SHA-256:	65841ADF524019DA65A043112AC39D37CAC9F64BEEB7F14BEFCA39BB69146E5E
SHA-512:	ACF7DCC61AFD4C18829566C48703393D6368E11C69996EED884EB036BA2C1549D9551562CCAF77F1F362198C1EC7ABB9B443B8B67422297388AC75502892C5A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .Ih...#/....."#.D.&7c.0.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....;.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.5347251706904705
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFv6yeaMtUdyP41TK6t5+d4HXXYOFLvEjMSWFvkm3GotUdyPB:KkXxKMSCvOntUl+kXxKMSCv1GotUlbm
MD5:	29F736C7E22DCE80917DBFE37546AF21
SHA1:	5A588657BB3604513681BF40FEC62807DABF70EF
SHA-256:	E5099D97D739E5FAF50B002F4CFC7DFBE0293474930029C76B363F774450DD37
SHA-512:	2DDC8CDA2B017C0CBD846E58C2190E661596C834EA548E77B8B350F5782547FF5C90BCBFBBA50D818ABB454B6CAD92532B6E8F30A738EF0C307E3768EDF1C9 1E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .%.^..#/....."#.D.;?a.0.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....K.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js .....#/....."#.DG:.b.0.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):	5.555464830123351
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOLRJyyM+VY1TK6tqkl9YOFLvEWsfOLPTqBOyyM+VY1TK6t:5h6OL/kXh6OL/k
MD5:	B113E18033D4F961314F5935C51C9458
SHA1:	4951F142BAB2368F23614DF6807065FB74F35F85
SHA-256:	80C54E9A2CA008D81C944F264491AB9348EF2B46045BE0F92691007BFE97AAD7
SHA-512:	0B20E7AC418D188DD30BB2138A37C4EC20102E2F0B8A547F3179C761BAAE2FEBD359848ABBABE3A5D1FC09FB38FDFB2FDE4592FE10A7388D7E24C80E79B953 ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .!.p..#/....."#.D...a.0.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....z.".....0\r..m.....;.. .I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .)....#/....."#.DYm.c.0.A..q.O...j....._y..L^z...?..@N..A..Eo.....A..Eo.....[.R.....

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):	5.610594029789751
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFJTYwSeKaTLnWkRVFAFjVFAF08vwSeKaTLn:UB4v4JTYwzXLnWkB4v40mwzXLn
MD5:	88761450A77F85655896AC5B49ABB4A1
SHA1:	1540E9905601095DC7D29A861C09B090EB4EA856
SHA-256:	A5DD98C312706A0A33C9759DE242724F42F9F7B540CCE849E8E197837165E723
SHA-512:	922C50E4B109743D1DA0ABCE1FA7CA5FFB22ADA948134D70DC430448C7251D722A8DB53BEF8E9256BD071AF907286CC6AC22F5DF6D47891AF4EAFD2CF22FF FD
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 .:8...#/....."#.D..Pb.0.A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....[.....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 .?r...#/....."#.D..>c.0.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....".....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.47527960001831
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXufsvlt8Z11TK6tAH:BsR2Esecs9G3
MD5:	0F065F5CBAD096473652812C222915F8
SHA1:	BC7A3FA6511BA354B0E855CEFB4816117B9BC812
SHA-256:	C6CC622785E8840FBFE1867A7A3A16B937EB84A84D1C9A8644BAEBF1D6C33C71

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
SHA-512:	ABAAAE84BA68FC87FFC7CDF4AE5FDB26843773CD8CF5E5CB783CE88FB9C26422831E1860881A681F5A0665E8F8916A444A8D6D59887EED9F739F58EA98B4C9B2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .....#/....."#.D.w7c.0.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....b.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.597861892603335
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQmzB7OhKlvA1TK6tz:RbR16DBJk9
MD5:	59F0C6994FEA885A77D0DAD5A8F04EFE
SHA1:	F5C3D5E9DD56C733BF880EE81C61C52C6E0F7E6C
SHA-256:	9C33C38F0618D454E9BB47D468ECBA7359EE6911308392B05277FA3CBCB265FA
SHA-512:	02E68C317DEBA92413FB9A47459B2952AD39B43339A2185C4FB47E6E9DBD9B69E89CA9A269976823B5AE758D6EC3571D99A05AE8B2071C356DFC5D4BD99DCF2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .....#/....."#.D.].c.0.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....8.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.511864078987536
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu8cIfcSQdFt1TK6ti:B2geRHRQOIfL08
MD5:	6658EBD597B7E878BE915113BF4D3FD9
SHA1:	548D770006E923480E41EEDE88018BEF0478F87C
SHA-256:	F0022959C6C3C18D6EC405588D96FC7A47671B06BC9906309369A5B3CFC50466
SHA-512:	A4262EB3EF8EB5277A0C3495A57B36B84F851A6AE9E025A44B62C31F28E843ADBCD5E40A61A3BFA438EF2FC0E30D41D31DF5BAD9A7A17234BC5E4B880EDBD09D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .a....#/....."#.D.m7c.0.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A..Eo.....Ww.....

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):	5.576980638352593
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQHwXUEt1S/1TK6tR9zyEYOFLvEWdrIOQZut6t1S/1TK6t:WyeRlF9t1w/pyeRlquQt1w
MD5:	7465BFED73270157B769435E336E16E4
SHA1:	CD07686F60955AC966F097816982EA9C14901893
SHA-256:	5E9EF033A5A1C45F3574C771B329FED94E1B11C8FE8488531D6F6AB120172356
SHA-512:	B46679A14242605A7CF4E14B7D5663742B87B1B8F6D99725B727C851F5F156AD24805E7FDBE101BC641CCD8161C9CA991CBBF38DFE47D2B30D4A5E6076E6B0C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ...|..#/....."#.D"..a.0.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo....CF9.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .ll...#/....."#.Di..c.0.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo..... >.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Size (bytes):	218
Entropy (8bit):	5.520253121561402
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvBKX/Wd9kNqww6U+5m1TK5kt:mnYOFLvEWdhwyuTKXQ9IqwK+41TK6t
MD5:	2F7817B0BFFB6E10E5456841FA69A1EF
SHA1:	C259C2372DDA674E2B7068E59CDC3B60E0F4CCE8
SHA-256:	74523599FF30FAFD06E0E243CEAAB13E72D12BA4267BCF3A7446218D1EB8036D
SHA-512:	1325B3BD910D082ECDDBBF14E087294402416ADDD566947F8FDB984EEB2C9FF92350910F964696859464CC0AF69300915E7E382B2DBC22593175564D5560AF45
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .....#/....."#.D.:.c.0.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....AS.....

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):	5.5818375412269
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbumtoZfO441TK6tT1EYXYOFLvEWdrROk/RJbu9XgBfO44R:/RrROk/YfLEZ1NRrROk/iwfLEd
MD5:	A5F6E5E8B40C973FD8618F1CDCB500E2
SHA1:	0F79D3B7F720E9796E241EBEE337C90BAE129F51
SHA-256:	814FBD819D40074AD809F79D7D4A02484AD2803CC5E4DEB5882D87EA69DC6755
SHA-512:	F4BF54A9F5967E529EA7A4CDC379982D5BACC188C18F5710FFA1CA44C3FCC106B139A75CE4575DBF1AD315BFECC82746814CC3F8D13AFD42E6E786EC96754 A4
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 ...|..#/....."#.Dd".a.0.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 .|....#/....."#.DF..c.0.A..~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....A..Eo.....".9.....

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):	5.567662370724521
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXIfqyIPS1QPLr1TK6th+mDEYOFLvEWXIW9CbS1QPLr1TK6tk:xqTkoPSCPLndqT9CSCPLna
MD5:	E21CE3228B099D515C3B7E2DAAC6EC99
SHA1:	1260550E77B76C8C12F8A60ADD3F145D4CCAA867
SHA-256:	237F7E48B3837F69C268883DB4C2467E61EFEA745203E9D06095B91287CD2E7E
SHA-512:	E8A8C78573776C3A92A8DAE318158B6BDF32F8C8D2D4CF70147DCCC1F2B08AD2BCB976C7A994A8EE59A3FECC444797084DB263A78BAA68DF02518DB1029F1 FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...p..#/....."#.D._.a.0.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....05P.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .j....#/....."#.DUg.c.0.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....l3.....

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):	5.6051964205985785
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAupdXgOO+ZsEJ41TK6tR/252YOFLvEWdMAuYH+sEJ41TK6t2:zRM/2KZsDnjRMA+sD
MD5:	F2AAA5CDFFFAA99D3F3220DFA2C9A4EE
SHA1:	CF808399CA10B53E092FAF7A0FAED8212AB5A965
SHA-256:	510602270B10BEAE41C2B868B76557F0682BF38E6235B35D1E3C5B06E2954796
SHA-512:	10B7E699CF159F5B2E6AA76906CF9FC847A00AA6CED519F1862519E790D29A5843704BEAF7B323E06B9461D3C42705B1D6980B34BC789D58A26C4CA8E3C3B9F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .DH...#/....."#.D.+Cb.0.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....e#.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....#/....."#.D..7c.0.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....I.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.613247636362058
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuHXX0XESFong1TK6tceYilPYOFLvEWd8CAdAuWFVESFonE:6lJREUrFoM1lJR/V7FoM
MD5:	51710D9B2F686EF5C418A7D798F3822C
SHA1:	4E47C009B10B02715035461BE76E15A88FAB4671
SHA-256:	18013E60C488E420F0726777DB2E25C932B55886A18E63EAAB3B77D4B30321C4
SHA-512:	9B83EE47C486870299B246446A93A8A92D6BDE3423B4DEDD519C336585DC17E1B810CA9EBAF90228BD37C6F9443A5E5709645C63973B6A0282F966761427C506
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .....#/....."#.D,ECb.0.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....9.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .....#/....."#.D..7c.0.Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....**.d.....

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):	5.582925893947578
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuCvXR2e16wG1TK6t0Y8nYOFLvEWdrROk/Iu1BEKA2e16wH:F8hRrROk/Kwe2t8hRrROk/+ae28
MD5:	094DFE806604C6D6586CB2461D16D49B
SHA1:	2152D19023D6E092BC754987F39BCC325EC41869
SHA-256:	CB61DEC02DD72ED6234E2A10D2CA7BD97A277833AAA56B2AFD972992EEA1624D
SHA-512:	04AD79446D2F6C95F1A362C5BD2AC3BA4F648906FA42AADF4F933329694D08CFF8B8B5823FAD4B9F3BC4628F15FA2368BF2445F9F9D6EF51AE34870D5F830A2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...{..#/....."#.D...a.0.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....%._x.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .:....#/....."#.D..c.0.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....uD.....

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):	5.676894537503105
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQoAqPWV9/qrNJli1TK6tbLrnYOFLvEWdrIoJUQZqmrNJlin:ehRcvATVYrNJICBhRcArNJIC
MD5:	29BAA4D3C3E2715A190F77291C701634
SHA1:	E1B3B7F8303D6D7506C60A2B3D60E0DA194E0D74
SHA-256:	6C53AF5F0DD3EB5F25CD95F975A2B557BD32F853CF11AE8EE75BD6387DF5C17A
SHA-512:	158F32ED5B481499BF0179E9377C511F3EB3F97D89201536838A3625B2750000DB171BBA0AAD36ABD7CE8B6B154D83A4BE5E66B134D634FD1DD65D1C6AAEC8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ...|..#/....."#.D.>.a.0.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....v.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..K...#/....."#.D(..c.0.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....+*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Entropy (8bit):	5.5636904597966765
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuiBXTLzgm2d/1TK6tq2OEYOFLvEWdrIhubbL18Lzgm2d/1TK6t:0RQnRe8kRh/gRe
MD5:	1C8EE6400D39C53900B59F301C036FD5
SHA1:	2A1BAC4E8B52A5E0F08776BBE5CC1DA5D99E7940
SHA-256:	AA306C46810EA26C0DA4EE2891ABC6F1C3A68C01BCC965DB4F854EF4D2772885
SHA-512:	FDBA8FB71F7BB1BBCCD05DEC1F4307245411F00B9DFEA0856147C0DA08BE7CE843EC45BC76DAB2D5377BC7C675DE200296DDAD8913641ACE54ED134AB94E10F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .t.{..#/....."#.Du..a.0.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....;.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....#/....."#.D.u.c.0.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....^.C.....

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):	5.559470116636045
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1K5Us2kx56uvp1TK6teMAElVYOFLvEW1KA/XWas2kx56uvp1TK6I:6JJK+s9hJJKR9I
MD5:	6EC702F426D85089F10137CD8F7313E2
SHA1:	D135D03DC64FCC421FD5805A7818B1FEE02F01C6
SHA-256:	5DE55240F6EE26ACC50885C1F9B09A8DB72007E34AD9D1BEA7C8824E864D1297
SHA-512:	E44253485D0262BAF448AAAB871530F74E9B56E65D1CB7C5029C705BE4D74E9BC4BB2F9850C49D3BF4C8B98532A9A7FC2E63ED24E8A4F6B4A2F08C147F2A38EA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .J.b..#/....."#.DV.]a.0.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....1}p.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ..o...#/....."#.DsG.b.0.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....{hrB.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.615716655521178
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuKt2mhUDLYtmOZn1TK6t:xRBJCDcFZL
MD5:	4E27B80C5EEB8BCD4104124CF89BC0A4
SHA1:	BDCDEA9F459D2DED10C51E1FA78A5A913BC6FA6C
SHA-256:	C339540717107A003D2FFBF3835FBA7A36C45F660778F513C330DF5FB26CC797
SHA-512:	416CFAD5187C7973246F8DAC353D51A074ED62CE5C1071D2B22DE82E464ABF9577645294368AE84FC34E66F95E1E5DA7705CD4B4FBAC9CDB8720EF300F13B73
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .....#/....."#.D.7c.0.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....O.....

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):	5.609873926561388
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWla7zp7CfEVS2aVPu1TK6t+7sRPYOFLvEWla7zp7BqV7yaVPu1TK6e:BPHRgHcg4PH2VHce
MD5:	09A65E7FCA31C909CD98E8467716BFBB
SHA1:	C264420C0256DB5806CD4F9D2DF458C5CCBBA8B2
SHA-256:	E1E61E573A742585548AFEC1C0AFDFD0BDA67F85FE6221F7FCEE601700B35A81
SHA-512:	F1593EE48187EE5C800D66E5D5FAFCAFCC279905DF1A1C4174E4BD5378C7A9115025E2B229B3562B35D3B75404C1249C6D19EBD08C963A4341D547376DA43D4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...^..#/....."#.D..?a.0.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....s.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....#/....."#.DCs.b.0.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.56444097430725
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QofC7VciM3Y1TK6tf/l:bJRT9viVcr05/
MD5:	21D003C12F6B056F19876C09A40F9F2F
SHA1:	CDF11C59BD9DDABD22989CCF72C3A76D906D63E6
SHA-256:	5FEF35E19F562D903246E7EDB732141ABD5990EB62A0DD56ACDC1078186F6E7D
SHA-512:	330F20552C94616F439FD48F3025A9BBC540AD47826E4DFA67C630206B8724EBA1BC93722784AC51353384E286CE212C0F189576E17AE0AB3D1004F6975B67E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .Fg...#/....."#.D...c.0.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.534030262964498
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQjFajBRCh/41TK6t:XRc9DDi/E
MD5:	36568D4EFA3A000CA44F69018912E2F8
SHA1:	EB9D121B597B31CA6F8E5F67FDBA04427C7ABE00
SHA-256:	D54E0CFAE9CC346E4F98EB960D1153AE330B538C054CD28C00DAB20670772C86
SHA-512:	E0F4126D044C3A15A1D5B56755CD95C02B170BAB0BB3F82A54C38250BC09C9BF0869880111DA488767C80C3008ABA35EBAAD74902CB73846B322FAFDD70BE8 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..s...#/....."#.Du;Ac.0.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....xk.....

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):	5.539980048140547
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu4beUlIF4r1TK6t:bs6xRkim9LlF4n
MD5:	F72CD3410717F94993161F80855B21BA
SHA1:	2ACEFAEC980F10AC8609D32C8A13C3D6AC0848CC
SHA-256:	46398AA2C27D284F2CB8A897FC80691BADDFA78DA517717D457D66184ED81D35
SHA-512:	311165C3711349534A364DE59626699186181A4F94EF6245E75C61C47D1E4DDFA620669530E188B6703BE3FEB9B923D7D736F6194630E36982C444AA3433C4C5
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 .k....#/....."#.D..a.0.A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....l.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.487298077480504
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
SSDEEP:	6:mhYOFLvEWd/aFugzGltN1dT941TK6tXg:WRSzGdTT9Ea
MD5:	832DF3542F38CCE1A66795596A1B83EF
SHA1:	10DE7C62F8F359C9E5BA5BC7B2593549DC159AAB
SHA-256:	DBD0FEFD980BBA95C6B4FD11A7EB93CD09AE35D8DF53CB4B62BBB05A4575DEBB
SHA-512:	1AF8D4B8F097857709B1C4BCDF9BE966D64C7FA162952DD205757B77FFF3BDA83D65EFDD9298685B08BCD6B601A30F812FFF4461B6ED4EF04FA13CB35E5FDD7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..|...#/....."#.D.d7c.0.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.508167239234896
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQoA+tYZoBMqVd3G4K41TK6t:2DRuRfA+qyB9Vd2k
MD5:	B1D8ACCF3ADBB8551E76B8E638A231AC
SHA1:	ECBDA1BAEABB82B27B3E71E7377F521269FC752F
SHA-256:	548BBBB2C848A77B5BCEF0D495AFEF8B9CA1473650CAFE480AF66DDDDF9BD362
SHA-512:	91C0CB1C88BD8A2C44371C0AD2EB6B935D6326A06CB3BF1D2421B7F518B25EAFE1C68A2A8B7206990EE7BE515935BA4E66F26D86F275E813C23741B215A7077
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ..W...#/....."#.Dg.6c.0.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....%*u.....

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):	5.582092940521651
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9QwX4HOuA424r1TK6twkqYOFLvEWd8CAd9QjPIOuA424r1TKu:+RQpohrnmRQXrnd
MD5:	82733D7F6C6E982FB9836F996C0DF1D8
SHA1:	ABFAA6246C2129501FAF0BC6CE5F7D9BE22B761D
SHA-256:	E5543731384DFE5D30837399F55F7970E73E25C60681080BB725466851E0B010
SHA-512:	593639CFF4377EDFAE2AF808441CFDC9C9FF4CBAD812892231A75BF95D36CC0795D9B04FFCEF504521A9DC8972B266B3E05EE8636C9EE89D8AF3F8A3808221F6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..:...#/....."#.D.}Jb.0.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....H.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ../...#/....."#.D)x>c.0.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....o.g9.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.545158689539947
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAujAqm4jebyC8n1TK6tk:xhRThAQ+7Q+
MD5:	46AB8F914ADD12880CB8A9E3952C8CB2
SHA1:	F18BD2260F6BAEEE0BFD80456AE7A2D2496BF4CF
SHA-256:	BB9F04D3ADA899510AEB9A041DDF3185CE382B32EB00E08B3940CC11E1451E1C
SHA-512:	68175203B0A05D8E20F418BF557B8C9C7855C7749E370D8245CD9921624A0CE282465696DF9A6F5CADD585250A4D6BE4C6B76254D9B87EC3919459D4DBF34C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .,...#/....."#.D.&.c.0.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....D8[.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.612472219168067
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQ4qyPsLmB41TK6t89QZYOFLvEWdrROk/VQfXjbKsLmB41Tv:nRrROk/VnmqoRrROk/VyMmB
MD5:	6F095D8AE4249A79ADC8125315934298
SHA1:	8585DE7DA87346AAE4E06690D8D5224DBA5B592E
SHA-256:	D7A571A370931E72913A4921792EEBBC8081ED5B918967B18A3F6826164BFA0C
SHA-512:	46DBC16990E73EA6A01B510DABA011B7A0F8F83025C92D3A503CAFAC3574C6A2225D5F5F8C182F0BC5AE5405A0DC44C987EDDA66B0C27744E0AE2E194D6C2C2E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .ar}..#/....."#.D.M.a.0.A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .(P...#/....."#.D...c.0.A ./.ev.....N~..6.b.....$.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):	210
Entropy (8bit):	5.545317757070254
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuW+3Adm9741TK6t:qxRcB3Adu7E
MD5:	9BE4C56708F85C32C8E03F7BC3BA5604
SHA1:	AA1E9327F969F1F097FBE5909049F463E18BA118
SHA-256:	C9A8F3D532C6B6B83AF521FE5540419D303996966DB754E8644EE69307D5205D
SHA-512:	D0CB0514036E370CBBCB1F5D50CC670C375C98D238D1C4D13DF06A7A6201A10338EFC08D39E41F1F1890D13766128041C66F7C7461E563685D80F1C3E24B22E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .....#/....."#.D*X7c.0.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....G.F.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.512999090768522
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvBq99xp6shoq+Nem1TK5ktBll:mMOYOFLvEWdwAPVu694Jn1TK6tBll
MD5:	116053A8788025BD90156DD4CDC7DB3D
SHA1:	C947D0E06B59FC1820FCD3FAD946B01DE00C3F1E
SHA-256:	599979C90B7F05C1E84963619A7D4762BE8D1D1B1F57A264F1785CC62902FE76
SHA-512:	1D5A23F7DEFB16D09E0D56F850EE791D5CFD9B993642E794B02C36DF06F670F467AC07849FB9B01620470BBA67EEBBF074C152FD627F1F68709D32CBE099D7F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .z....#/....."#.D...c.0.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....e.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.605597178047743
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQhtyNdzhcsBXIh1TK6tji:mxRBJQkkDB0Ji
MD5:	21C87DD6E90B97EDED7C694B8832B07D
SHA1:	CC8F43820E28EC73450F2DB2A6F19C78F82B205A
SHA-256:	B1F43735F91AF5C1F0B45926EC9AB1C5FC07FF624CE478B9759A9EFDD0CC3FC3
SHA-512:	0CFC073F77E88C77A87AF080FE2E96BE6A167C3FF8D424F4F41965481733AC6C2003E80159327D5AC17346A034A549C140292A80CC35E6512C792CDAC4B60A1F

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ..x...#/....."#.Du.6c.0.A...k..`..N3.... ..d..$[....{.A..Eo.....A..Eo.....f.p.....

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):	5.577396761216874
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQYeUc3Me/1TK6tRz/EsPYOFLvEWdrROk/RJUQZrQntgsq:3RrROk/s3cHZRrROk/sq82sMc
MD5:	1C0ECA0C541F49BDB352FD8FB26017DE
SHA1:	8AB698A5B271A5FD78907849CDD793366C7C2662
SHA-256:	CC6B30593302387BEC72CBB07A9BE595F9678A64D057142DBA22DF3DBFD51CB9
SHA-512:	FA9D2737A43B8F24FEBE9185BAA0AB7D11FD8962F24A337A01A40A0F4DE0F5C6BBF4E40C9E60D8C3B73AF560FCC7300AD6FB0C2306E5C33823C9AADB5C0FDA43
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 ..t}..#/....."#.D...a.0.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 .uR...#/....."#.D.I.c.0.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....{.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.180682911276209
Encrypted:	false
SSDEEP:	48:h1zZ4+dsp6zkxyW5qOYGCVJpfxlYqYFlrzvsapM1l0tJVNB4L5YMimmmM5Uhw:hX4p6z2yQ1YGCVJpfxlFIIrzvsapM1l8
MD5:	8B3862202582C723C3ECCAF572D0209F
SHA1:	C16CB730E0934F6D77E89412FFD5633DF401405E
SHA-256:	1D3F3AA80D6BE174E2588019B0F80791E9B81DF26CBD0BAE1DE0A9A3C2BAEF4C
SHA-512:	1706EE3CC332EC764A4B04A77E50DAF4347D8FFC9DB73C4DE063127CD0A9E95FAE7068D5D061F56D49F43C50615ECBC814C5F4172A19A1C9632AF38F208538
Malicious:	false
Reputation:	low
Preview:	....h...oy retne....'.....'.....:.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S.....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.....AJ.8oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.197805336110884
Encrypted:	false
SSDEEP:	6:mwXIY34q2PWXp+N2nKuAl9OmbnIFUtpDXIsH3JZmwPDXIJDkwOWXp+N2nKuAl9Oe:TJ34vaHAahFUtpDHH3J/PDKD5fHAaSJ
MD5:	42866DA7DFE7DE5CD35774F970B42740
SHA1:	1B7248DE1EAD2059E4436E9DD78634DC3619F7F5
SHA-256:	43E7DA2BAAA1A98DD4104B8403C739E8664E4B5DD7C4181EB7A51D819721F61F
SHA-512:	0CEA0E4D073ED38BAFE6846DDE66B1899D0BFF1B33A0E3BF4E2B5C5F617EC5EF969F6CE2E43F93C232476C36335C9473383183FEB886099FC23A1AB70CE6CDDC
Malicious:	false
Reputation:	low
Preview:	2021/06/11-06:47:50.015 1e64 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/06/11-06:47:50.017 1e64 Recovering log #3.2021/06/11-06:47:50.018 1e64 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
File Type:	data
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.00795231738728784 5
Encrypted:	false
SSDEEP:	24:TGEXiXKGEXiXJ88hMXiXN8hMXiXTg8hMXiXTg8hMXiXT:TGEiaGEiCsMi9sMiDgsMiDgsMiD
MD5:	B6D6D8092327194522BEE7EC4E9D29B0
SHA1:	248DA8ED1A94F29906C944B56FF9ECEAD7342542
SHA-256:	E2172C50F08FC62BD25EE7D9CE092A9F4BDCD3143D81E38E522A917FF7D6E86F
SHA-512:	573EBD8EE4A387576183D8232B1343E5CB51C4145068E90C144E84E10CD111A673567139E087FA7CE85FE276AD0F3CFF0A3CB2E60EB403735F2AA00520A848D3
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210611134743Z-588.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:	modified
Size (bytes):	65110
Entropy (8bit):	1.8689592807141013
Encrypted:	false
SSDEEP:	384:+rfpU+C/wKgqZIKKr7O+eaWBvu8weKJmad7:+ryR/wK1ZIKKr7O+eaWBvu8YJms7
MD5:	795CD0FEC8D4D3A3022D4735C09ED842
SHA1:	3150B466966646E728702FF028A0BC147781AE2C
SHA-256:	2BA757D1082F1713408AEBA4F07D262DB96C756F237F42AF5C877CB43AA8D63E
SHA-512:	2C1A8418EEF4DD586C391A2633BE6CC431D70096CE9DD527587C51C38A8BC6763CFDE773424D7EE958D155875D0C35DF9DBE0D1871DEF27AE40393D114FF7D 9
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):	3.3890016892194255
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQ+hOhFVCsL49IVXEBodRBkRq+hOhAVCs749IVXEBodRBklq+hi:iGedRBKredRByGedRBGOedRB8t
MD5:	1A2FFD95112511B245FE9AA9122CB4AD
SHA1:	12C2D1F2C0FF01F8FEEA5E850A54B1D1211B869F
SHA-256:	28C890520BF4541C5447CB66AEF3715B21BFA6962EF488EC07304E6480FED993
SHA-512:	CC330C97E8AE4F0ED13D99FC84A455A02444B8FBB7E0EFDFC8DC2E449C24375B66FB61F233F1E608BC4073E3115CCE8BB6590D56539B455005BCB6F309DB99 C
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:	dropped
Size (bytes):	34928
Entropy (8bit):	3.2012336263882184
Encrypted:	false
SSDEEP:	96:d7OhFVCPG949IVXEBodRBk0+hOhFVCszLR49IVXEBodRBkxq+hOhAVCsvd49IVXj:daiedRB2ELGedRByxCedRBqO+yedRBg

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
MD5:	CB6AB7085ED933E1A41580DE35DF29DA
SHA1:	CFC0D0EC4579EAE356D6C15BE8E409B78583766B
SHA-256:	79F3864C6B30E02AFF55F6A67F1305660852CF73DD88876374C4348FD6B536B2
SHA-512:	9C5959615BA8EC81B59D51A9082EF3A5F59C877F00038ADBF070AD1679294273C65AB8BA86CF1C411D827577E93455F86958F525D787F636E16B5AD48E10E423
Malicious:	false
Reputation:	low
Preview:	....X.. .h...y..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2A7611428D62805A3E4E5BC4103D82E4_93980168F338F037DAF9798B595DCB15	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.189009108896334
Encrypted:	false
SSDEEP:	12:JY0FXX5FZT5+7DqWmpfhN/qtGedVKZfu4+Rw:JY0Fn3ZTg7+1pphqtGedVKZ2o
MD5:	6A98C2BFFD658D9523DB244580930E06
SHA1:	8B01A7A27F58130D0AB0AFF7AF6627BBA3E82223
SHA-256:	5CDB3906A0182C40B4543FFADFE31A65ADAF0EAE9B709604AD71C35BC89F2883
SHA-512:	B71223E8DFA53DCC67F455D801F66ABA2821A4FB60093CE2449D15CAE08836A228094EA458AA9AADAB5A9EC4DF7DF1B57A246F57B565694CE19DDA902B8F09F1
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210610003349Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+.....y..]"g.....PX....20210610003349Z....20210617003349Z0...*.H.....;.....*'.V.i.H...#.e...&.9^.81.....p'].L<....?...=.../J.{P.5L....&..~|.n].x....P6.j...9.....I.V.H:..$H.T..+.&.#.U.....e....j..o..\|>K...hk...d.....~t.._W.....R..._4..vu..p.ou.4....-.$.....lj....z.C....J..4.^...w.....d.DT.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,....,qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y....,.5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2A7611428D62805A3E4E5BC4103D82E4_93980168F338F037DAF9798B595DCB15	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.8132510948463825
Encrypted:	false
SSDEEP:	12:O5PXDmxMiv8sF1JbqDkwJr0iraz5E7DmxMiv8sF1JbqDkwJr0irak:gzmxxvnFqYwJlVmxxvnFqYwJl5
MD5:	8A3053DA16243407DEEED97F20CAA988
SHA1:	3DF42681E68CC49CDAF55B32F96DEE6F0BF8AD54
SHA-256:	E93BF57297DB3CC1413A26A580B6C822FB96250D8AAAEACE278A468651A71630
SHA-512:	43A430D264E5D69342C216226A0B63BE8C004743CE4D7927E9B8B10F1912A1E71C788B1D9C4073ACF8C5BE5B28D47D77C5C5C03D9212C30C0C2BDA14D60A5ED
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2A7611428D62805A3E4E5BC4103D82E4_93980168F338F037DAF9798B595DCB15	
Reputation:	low
Preview:	p..... .....y+O:.^..(..... .....y.D.^..7.....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.c.X.e.R.E.A.X.S.J.n.9.o.i.S.9.o.%.2.B.L.U.F.g.%.3.D...".6.0.c.2.3.2.f.a.-.1.d.7."...p..... .....y+O:.^..(.....T.G.].....p.c.....p.c.. .....y.D.^..7.....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.c.X.e.R.E.A.X.S.J.n.9.o.i.S.9.o.%.2.B.L.U.F.g.%.3.D...".6.0.c.2.3.2.f.a.-.1.d.7."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.109576970393724
Encrypted:	false
SSDEEP:	6:kKCt56e8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:m568kPlE99SNxAhUe3OMx
MD5:	4036DDD1763DF305BB37A2861FA2FA48
SHA1:	46680B94D8AA713AF0B39C3EB2FF7940BBC44B04
SHA-256:	5333203E5B18721A21C899C66EC854423D5F8764EABE169853ACBDD6E460ECE0
SHA-512:	E035D193BCCFAAB919C0A1664150D6C2483638F22ADBD517E1F59E9683C75A710F71A25F89B58BFC0F494B13755703028BA66CA75AC9916F62631B19E1D0D9B7
Malicious:	false
Reputation:	low
Preview:	p..... .....m^:.^..(..... .....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\057327e6-7b60-45b8-92ee-1146262d4219.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):	164443
Entropy (8bit):	6.051049598187742
Encrypted:	false
SSDEEP:	3072:ZZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:ZZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	D48F4F493089A2C28EEF0D10459229E5
SHA1:	D8E38707D96C880F507B4BF2894C1959ADF30126
SHA-256:	1FF05AB8FEF9CBDA0B5E86AEEB0870F2D956CEFCEDD8FF9EF22CB529511FB0CA
SHA-512:	515AB39AB1BD7CB4783DD2C789131AE07EF1DA0D9F225CA030BED09DE9274FD030B448CF86EE9DA91AA916C5F940C64AA1360E4AEDAEEC44553E6CDD2F6C520
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\084df96b-f8b6-485b-b86c-e45c541fe328.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):	164022
Entropy (8bit):	6.049927729899139
Encrypted:	false
SSDEEP:	3072:QZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:QZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	887869480C9694863925C17672E9CA68
SHA1:	8AE3B02E62BA45DF0BA8BEA6CA28F52BD24EB45A
SHA-256:	6AA105670399F9629A6367236D523FCAC44709F3970614F8490B2FCEBFCB19B7
SHA-512:	1A69D423B77D6E021BF2825CF7EC9829F5C0A22C3749506263DAB0A4688F9B5AE56B8A9F38918BBFB660D26FA31072737FAC2B3A78EF230744AD1724CEDF5651
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\084df96b-f8b6-485b-b86c-e45c541fe328.tmp	
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016508895"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\12c5831d-f137-450d-aa73-79d1824bc549.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7516718190108365
Encrypted:	false
SSDEEP:	384:r/78MeRf6iNYvNkrVvAs3fsG3HCrGburpuQOx/S2yJrF4mxG9e8kA/OeScNx1slw:dGpJ223DseHSsuoH/aIKSEE9h
MD5:	DA83050F8FE900318B2B6E84300BA6B8
SHA1:	A206C0A0DDDF6458B675F0EB95C1D157D06DBD3E
SHA-256:	7F7B48E1769EFB01EBE321C23D201F592D36A0E4468FC205986C297C3A7F9A24
SHA-512:	6CCE2EF18A50AFEEC2116BD675D4B3A77AAEFB1E7A1590E318C44E0FBBB8368E0F66D135A59DC3275F04DCD9C93B1A72309BDFB7C59F2918E42981BDD02F8AC
Malicious:	false
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\131832d9-3f50-488e-b27e-97c0f3edb3a2.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):	172394
Entropy (8bit):	6.079452220734057
Encrypted:	false
SSDEEP:	3072:uRyZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:syZu7RElMjk71aQw7hbSmBaqfIlUOoSG
MD5:	969CFE2DDF67BF23A76D39712D3C9FA2
SHA1:	50E4C83719EC856D6C4DA72E35DE191FD956F3D5
SHA-256:	2BB34937FD17BDE677E0AA8372B18F85598606B80BAF8321FC079E800BC91B86
SHA-512:	832741E5BCFBDC017ADBB6FB2030482BA38960EAB61E5C83E7ECC0FA162A5E82110A0784CE30B8B493606A636DF4F3BD472B5EC3C3DE2B0E0733EAB512E68C7F
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\30023d21-433e-490d-a265-889b7ace06bc.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):	163918
Entropy (8bit):	6.049605787147607
Encrypted:	false
SSDEEP:	3072:YZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:YZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	80FB75E117150456CE50B0BEA9DF0BFD
SHA1:	672E358DAB0EB4EF1DC0554863DB16C22CCF71F7
SHA-256:	11B8FF314BDA2B0EEDE5BFE6C08FD1624A1F84F2227765BC645AD9CF0F284847
SHA-512:	D2F575B3A3CA7A4B8CB8007A9D33A1E9191AF3C478640DA736F154031F5C41282F22C330568E6A12CCFB6E5C80F4FC911A33D88846E55374828A360A325AEFD1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\30023d21-433e-490d-a265-889b7ace06bc.tmp	
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016508895"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\37a1ba4e-6a15-47ea-af96-d2642b0fe719.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	164618
Entropy (8bit):	6.051455870667482
Encrypted:	false
SSDEEP:	3072:pZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:pZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	66BF8505F115716128BA92A4CEF0C8C5
SHA1:	AECD4667197B37BBA0AED5EC1D46D49B1EDF8931
SHA-256:	D75D525B43FB47092E52FDC14E503779A6D0B26B703E88A5482981ABD468D1C3
SHA-512:	6F3E6AAE6DE68F96943033A185933B8CFC1909507405B2216C2766E83243369C4EE2A5C9B9E142B9710B65985324B143B3436A1C9E7F51C922D2CF723333510B
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\39013288-18ce-441a-a991-2efc7bb56b5a.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):	164526
Entropy (8bit):	6.0512055713028206
Encrypted:	false
SSDEEP:	3072:iZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:iZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	8BB1ACD9C06B3AE0A1FB29203D157A2A
SHA1:	F48E6807DC396C3E01C1E4273EF0125F653EFC57
SHA-256:	E0AFC99FB1EEE9CD665A3A3DAEE539694AD75B8653E0A994AD8E447F3494621A
SHA-512:	1A9B587FD0754E0DC1100F26F30496FAB2C052E2D0EA1C8821AED8A8844D77CFCD8F2A4A053F89405D0958DF1D4305A6F70FB3B67773A66A8D2EA1BC9A756D C
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

C:\Users\user\AppData\Local\Google\Chrome\User Data\4f70a932-0cd8-411e-8749-16a28dfdca34.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):	164202
Entropy (8bit):	6.050367431090951
Encrypted:	false
SSDEEP:	3072:sZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:sZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	5C0728B2986DFBDDDD0167FE31EAADC2
SHA1:	F1D4E27CB81C7FA6B1A810DFB1B584A7DED36687
SHA-256:	F08BAEB2644DC975FA22C82AB5F3F25AF25A4ED432936F435A9A3842EDE050EB
SHA-512:	CBF0DCFF447AD170494D635C32393DD8CAA9F48A7BBDDFC3946370935E26553152478E5563393A9EAA848A1FB1767724D5C0C99C821BC6AB8189A713A7CDDF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\4f70a932-0cd8-411e-8749-16a28dfdca34.tmp	
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016508895"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\5636ad80-f1c2-4bcb-bed7-ff00e5a3a085.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):	172394
Entropy (8bit):	6.079455394892124
Encrypted:	false
SSDEEP:	3072:8AfZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:zfZu7RElMjk71aQw7hbSmBaqfIlUOoSG
MD5:	48231348522C5265FB6F5749AA4E4E7D
SHA1:	C6B5805743FD302AC7FDC0C9853A64CD6AAA1DEF
SHA-256:	9AB07591640842A76A9454D9B04F6881E16C85AD57E1632A215FD0FDD611B44F
SHA-512:	653964929C2E184CC1203F8CD8F0B6E76442691DAF5444DC6024CD0E96A8CBE39AAC8FDAA11EC6AB43A34FD691EE499D94A7C91F83AEFB199BDDE3019E2E07B
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016508895"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\628b729e-1e57-496b-b110-7eb62a70e130.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	109592
Entropy (8bit):	3.7508698878412825
Encrypted:	false
SSDEEP:	384:q/Z48MeRfBX/Vi0VJ7YvNkrVvAs3fsG3Ha9rGMTurpJIbRk9xuHfCyXG0S2yJrF4:c5KGpJ853DseHcouPBkSoaIKOEE9n
MD5:	B781E9E5A1862299C3804DA53685FA08
SHA1:	3DB81F4FA57813067493B628FEA20AB5B2B98BF5
SHA-256:	7DF8154D4B2C02B874519CEF347471C59D84D0000D98745BA17C36C7A76A7771
SHA-512:	0F5084FC4680809FB4771F3C6CBE9B7EE2B1C5756EC1CD1F619DBFF6217AF3D7EF21E6A99D63017DB5D43AD5BDCF92AFF7B0AC7090440AC0E50BA29CF1827F8E
Malicious:	false
Reputation:	low
Preview:	.....*...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\7898a0d8-0aa4-4079-816b-1bc1264ea849.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):	172394
Entropy (8bit):	6.079455238502055
Encrypted:	false
SSDEEP:	3072:8OHZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:FHZu7RElMjk71aQw7hbSmBaqfIlUOoSG
MD5:	30F40745B3FC70EC91D1A520C870C3BB
SHA1:	0BAF516B1DBEF4D839283591DFFD77525C86F482
SHA-256:	196826CDECD5957CF5C6B367A3B48B57AE1B5277101A5B490943253D892CBD1C
SHA-512:	183311EBE761B9EBCA34FB5ECB8894496380227020E219FEAD91A1B591F3B8EF739F9E758686115DB7D70967888E4FCA412AEA5C4ED9825BD860FF2B02DEC95A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7898a0d8-0aa4-4079-816b-1bc1264ea849.tmp	
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016508895"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\7c66d3d3-98f8-4501-be84-616c3693140b.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):	172394
Entropy (8bit):	6.079452406269432
Encrypted:	false
SSDEEP:	3072:uWnZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:LnZu7RElMjk71aQw7hbSmBaqfIlUOoSG
MD5:	D0DAEE5E74DAD4C4BB5A9E1AEC24C5D4
SHA1:	7FBCF38628074C1C5CD3866D4E45296156399B02
SHA-256:	FC6FF28D5CFB353A8D019E15B179BC8B8C7578AB2AF7F8E4E4F6ADAEF6C9B525
SHA-512:	2C068CD549E873474892EAB7F28DCFFA74C52B6982D564C4D2108956CD5308101E6CAA05B314E61942A3E3AFEB1F8AAB82AF667126B3C93C660037E2A63A0CF
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\9601271c-2737-406f-b8fe-69221627bafb.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):	164443
Entropy (8bit):	6.051049598187742
Encrypted:	false
SSDEEP:	3072:ZZu7FCTczElMjKrUc1qTQ38o07heQvKedeKO6FcbXafIB0u1GOJmA3iuRk:ZZu7RElMjk71aQw7hbSmBaqfIlUOoSit
MD5:	D48F4F493089A2C28EEF0D10459229E5
SHA1:	D8E38707D96C880F507B4BF2894C1959ADF30126
SHA-256:	1FF05AB8FEF9CBDA0B5E86AEEB0870F2D956CEFCEDD8FF9EF22CB529511FB0CA
SHA-512:	515AB39AB1BD7CB4783DD2C789131AE07EF1DA0D9F225CA030BED09DE9274FD030B448CF86EE9DA91AA916C5F940C64AA1360E4AEDAEEC44553E6CDD2F6C520
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"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.623419208503116e+12,"network":1.62338681e+12,"ticks":92510731.0,"uncertainty":4636720.0}},"origin_trials":{"disabled_features":["SecurePaymentConfirmation"]},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"1324

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

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):	3477
Entropy (8bit):	5.53198019710749
Encrypted:	false
SSDEEP:	48:jhxy9QhTlx9Qh92092flx9Qh92092blu9Qh920922lN9V9Q792f92WZ:jOC1ph5phkph2Zdge
MD5:	CB336572CD6D12C43ADDEB276BCE5442
SHA1:	A4CCB4725E0CE2813ADBD2EB4037363E91CC7D51
SHA-256:	17F7C31D10493BFB0C7B969A0FC6B82776EAA11FE46EBE9BAEF13B5BB62C07BF
SHA-512:	77AE70A2276320CB773932E0C41509FE4C46FA64E80107E3E0A66AF902B2E41D75816EC7251F4EA17815F4A4775A740A599C3D804E1F3B3A714AD7DB4A047106
Malicious:	false
Reputation:	low
Preview:	...C.....-download,45db250b-5f3e-4c07-be10-e9d098a3b36f.....$45db250b-5f3e-4c07-be10-e9d098a3b36f.....F"...^https://www.gstatic.com/policies/terms/pdf/20200331/ba461e2f/google_terms_of_service_en_eu.pdf..https://policies.google.com/..'"https://policies.google.com/terms?hl=en*'https://policies.google.com/terms?hl=en0.B.J.Thu, 30 Apr 2020 13:45:00 GMTP...Z.application/pdfb.application/pdfj.....r.....x.....6.N.....-download,45db250b-5f3e-4c07-be10-e9d098a3b36f.....$45db250b-5f3e-4c07-be10-e9d098a3b36f.....F"...^https://www.gstatic.com/policies/terms/pdf/20200331/ba461e2f/google_terms_of_service_en_eu.pdf..https://policies.google.com/..'"https://policies.google.com/terms?hl=en*'https://policies.google.com/terms?hl=en0.B.J.Thu, 30 Apr 2020 13:45:00 GMTP...Z.application/pdfb.application/pdfj.....E...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.D.o.w.n.l.o.a.d.s.\.g.o.o.g.l.e._.t.e.r.m.s._.o.f._.s.e.r.v.i.c.e._

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\08660547-ae2d-41b5-8cca-76c690c43a15.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):	6488
Entropy (8bit):	5.190275409403284
Encrypted:	false
SSDEEP:	96:nCCi5k2Rl/UbcVWkokHVJCBRLL8Gkr1hbOTQVo2wn:nCC92RBUbcgqV4BZ9kr2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\08660547-ae2d-41b5-8cca-76c690c43a15.tmp	
MD5:	9E3D2661EBDA71AC7149B8FC17C99EDF
SHA1:	C2DB871C37B740B0D2E53DFC31B3E7C0E0369CE8
SHA-256:	A8A9DBFB57BD4F430D6DB2B7962B499AFC7670AB9899AFBDE671749FC27E841D
SHA-512:	212ADD893338152959D11849237EBA6488F1C4904F682FBC14186D90D62D63888FB4F09ED941F3680ED6F985FFF5AB9FE47FF05926573D2EFD52784EBE2DD6FA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267892805746794","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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\27b4f4c6-e1f1-43cc-b943-e29a4a44b9d8.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484808458443","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484808814952","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13270484808814954","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r8---sn-n02xgoxufvg3-2gbl.gvt1.com"},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"isolation":[],"server":"https://widget.intercom.io","supports_spdy":true},{"isolation":[],"server":"https://js.intercomcdn.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484854685411","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://yt3.ggpht.com","support

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\30aec1f8-da1d-4efc-87ad-fc090c01ef30.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):	6488
Entropy (8bit):	5.190511688671704
Encrypted:	false
SSDEEP:	96:nCCg5k2Rl/UbcVWrokHVJCBRLL8Gkr1hbOTQVo2wn:nCCj2RBUbcg9V4BZ9kr2
MD5:	C20E7ABA8B6ADE221E8A660E13423C6A
SHA1:	9FF346B1D2FC15AC6A789583C3319B874D8FBB15
SHA-256:	7B153B970B1FE35BECFE098F4274C0EBDF0440D95756165252F98A2468A99648
SHA-512:	7EA4C2D8E78380176C847859414B26C7913ED804BA8B50677A0C5ACF0A989461E8015098DF4BF14F9C6D77C0F074C502CC3F7828D6FE62D1C67B399E3D3C259
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267892805746794","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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\667cb09d-2cb4-45fc-b893-1d9fc2f29de2.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1639199240.401067,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623419240.401071},{"expiry":1654955294.448062,"host":"KVivTTKTVC3D7/hfpnbDFfPAgoVJQnjFfXBq+8P8zk8=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623419294.448065},{"expiry":1634305815.493934,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419415.493939},{"expiry":1654955293.652343,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419293.652347},{"expiry":1654955274.476398,"host":"NlMbAACeZ6GFqgYKbWFINnSsfFM9gCcHh+OP80Q98ts=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419274.476402},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\709c1a40-9c21-4bc5-83b9-b938db09eeb1.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):	5615
Entropy (8bit):	5.0032150712600565
Encrypted:	false
SSDEEP:	96:nCCBGX2pcVWwokHVJCKL8Gkr1vbOTQVo2wn:nCC+2pcgOV4K9krA
MD5:	CA1F4983F30869E11E39F5545C672D7C
SHA1:	9450F674DD0D4A9BB99C8F95B6AF38774B424E0B
SHA-256:	07BBCB9EFAEE63F2A87E68AD61C44797AC42568DD3D110DCCBBEA18C5DC05FCC
SHA-512:	2FAB53E0E399E5478234D000F9ED38E8637CF42BF8B1DD7AF9637EC050F6F8045A11B2BC41937F8CE8F3D087361AB7D2540F1823EB59B9AB53FD57A68A423C5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267892805746794","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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\7996e859-ff70-4d06-93db-cf6e11fc61e3.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1639199240.401067,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1623419240.401071},{"expiry":1634305640.8103,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419240.810304},{"expiry":1654955244.299763,"host":"NlMbAACeZ6GFqgYKbWFINnSsfFM9gCcHh+OP80Q98ts=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419244.299769},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1654955209.604612,"host":"RNsljhzQrppvtsaSJ2jzGCoQt5mAXe0MwslIjeUIK20=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1623419209.604617},{"expiry":1639187242.292649,"host":"XhfjKX/pWqI06hPmREKl/daJ2dWwZsvlSNAmuiMtJxQ=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\841e9eee-c78e-4b76-8b11-5210d95b5483.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):	6462
Entropy (8bit):	5.188771750353409
Encrypted:	false
SSDEEP:	96:nCCgsmk2Rl/UbcVWKokHVJCBRLL8Gkr1vbOTQVo2wn:nCCg+2RBUbcgAV4BZ9krA
MD5:	1DCE5CDC0BC53B4B05C69B894DF1DA87
SHA1:	E1F19272EDDF12C2C94DE7872067E92452DC5077
SHA-256:	9C5584714FC0B9EED61B6704D4648D23B0182C659027392CCD90455802400664
SHA-512:	8662BF25D7F8F66B638C5C2BE14C181F6DC98208A9B4331B750CE02F914B12EB2E6C17A1CD835C1740148B7A5EEF085F7443644088D9D3D19231EBE7033FD067
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13267892805746794","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","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\917d73ee-0b68-4044-bf2b-597c40e30e3a.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484808458443","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484808814952","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13270484808814954","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r8---sn-n02xgoxufvg3-2gbl.gvt1.com"},{"isolation":[],"server":"https://cdnjs.cloudflare.com","supports_spdy":true},{"isolation":[],"server":"https://widget.intercom.io","supports_spdy":true},{"isolation":[],"server":"https://js.intercomcdn.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13270484854685411","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://yt3.ggpht.com","support

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):	5.197630102504709
Encrypted:	false
SSDEEP:	6:mwpuZFIq2PWXp+N23iKKdK9RXXTZIFUtpDUZZmwPDUzkwOWXp+N23iKKdK9RXX5d:hva5Kk7XT2FUtpwZ/Pwz5f5Kk7XVJ
MD5:	A7E3C77F8BB967D1527F1ED1497B6CA1
SHA1:	25CE6910878EA4283A775CFE2FD6BD36C6BF6EF9
SHA-256:	98A7DCC624827D992C7EA25F5BD9571A06A1A312F5288FB8F36DA9CA56AA495C
SHA-512:	6769574ED0F550649E18D29F72411DDAE1611A372CB597902D727CA62AB599C34CD723C5A8692AE06A08AC1E308259BE9D55F9C6DA23C0CCA06F89F35EEEDB8
Malicious:	false
Reputation:	low
Preview:	2021/06/11-06:47:03.767 1a34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/06/11-06:47:03.770 1a34 Recovering log #3.2021/06/11-06:47:03.770 1a34 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/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):	5.18961850388218
Encrypted:	false
SSDEEP:	6:mwdECIq2PWXp+N23iKKdKyDZIFUtpDtyZmwPDt+kwOWXp+N23iKKdKyJLJ:BECIva5Kk02FUtpI/PQ5f5KkWJ
MD5:	F8CBEBF8C62178C8477545C61867A638
SHA1:	57489A49D276BFFE83ACE80FF81315847495185A
SHA-256:	B062A9B4B7CBE08A6D542761E3682885C1ED6A668D09E0E9BE9AF92CC1120E56
SHA-512:	BB387B1C2FF4C9EB9F69AB44CAA3A25E793A41548606DCCA580568CA804ACD8EC987C3562D3DF22782F6518AD08A2594AC2EB57E918341BA1330042FF62D452C
Malicious:	false
Reputation:	low
Preview:	2021/06/11-06:47:03.762 1a34 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/06/11-06:47:03.763 1a34 Recovering log #3.2021/06/11-06:47:03.763 1a34 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0301da6c6587c074_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.904417314542393
Encrypted:	false
SSDEEP:	6:m0YvEdCN8uVvUCllfHaquK9alfM2NZXmAo1lOdgUWQLhw+ucy5AykeUgmnK6t:6Em80vbSquPlfMMZXAmKUq+uBT1UDp
MD5:	95D1D8EDF5F4E6F9C327E52D84D919D1
SHA1:	0C3A608DAE410E049D48093FAC19715A2A52C5E8
SHA-256:	F9616FCEF98EFB39AC0B17F7D514665205A4392C072596A2DE331E4E19839460
SHA-512:	4E54F2B34C3C70A7BD6F44692EBA3C6DB036FC16941758F02C0ECF24020DBB64F31BF906D767B1395144A5CDC7919F37EEA26DBB10F2113AB88011FAB00CEA84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....MO...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en.NllmGE6QfHM.O/am=B0BRhgUFAGEAAOAAAAAAAAAAAEZBQCEwxnP4/d=0/excm=glif_initial_css/ed=1/rs=ABkqax2gLjwWvE8Sd0sESu2pQy8eXlp6Vw/m=sy72,wg1P6b .https://accounts.google.com/M.*..#/.....HV.....Z...3...qnd..<.*.....{..A...A..Eo.....o.X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\033041f4d52a27a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\033041f4d52a27a8_0	
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.577151854783296
Encrypted:	false
SSDEEP:	3:m+lUgtl6v8RzYzYXXAJn43H9PWVNRBLKk9flHC9D5gJn9ZC2vRmfK/llpK5kt:msqEYMHAJn8tsNLLa9Nkn9ZCvfahK6t
MD5:	461BABDD301BDD0459B947A5CC67556D
SHA1:	FFB830956430450246E9CEFF5E97DA8EDCE44884
SHA-256:	AD57DBF4AF2C6C64684035F7115F342915BB5B6B904FAB80164311195D06528F
SHA-512:	4C4C4B803974E168F0B3B99A070A10964CD2D742B707C84E027C99F1CD07E1BEF02B0504DBEAD429C132175096C3761B00DD4E4675828539D71062AB80B32A42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://script.hotjar.com/modules.12f7375208c548a9407a.js .https://milanote.com/W#...#/.....I.\p0V...A...x+.2...[..K.2.|..A..Eo.....Y.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0407b3ae67cd00bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.540738124666517
Encrypted:	false
SSDEEP:	6:mU6EYk+ALUK7Wc7YmLc9Y1cghgv5c2kdMFkH4DK6t:t6U+ALUK7Wc7YmLpYcDdMki
MD5:	930C41CD30616836FEFD3C153E368453
SHA1:	20C41471E1C0B33AD16F02DF4EB120560A6F49A7
SHA-256:	1E7F259F6BA0A2B564DE6BE8A097BDB01EDF0595123C9A28031FEE897A248302
SHA-512:	4C684D3FAAC908BBB5B037F58EDAE6482A4F3F42FC23F5C61E0C658D5E804DAB333A237DC590203FE8EA4D497783A1A5114A1EA24FB3EADD082BE93575579C C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://static.milanote.com/vendor-40b8ab6b3936-modern.js .https://milanote.com/,<...#/.....o.....Qi.q...h?y...Y.?.=/.LW...x...G.A..Eo.....v .|?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0447ea93db317085_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.4525920048140675
Encrypted:	false
SSDEEP:	3:m+lkF+8RzYkwLYR8XfQV4JnLLK0ZTelHCEl72Hja+4d0KwYZMmthtlpK5kt:mNYk+zfQVGLLJBMqHjPWnNK6t
MD5:	DA06181FC550992C1ED09CBDC9B009C7
SHA1:	A9CB496A1665D78E817C305A34652481C23F0A12
SHA-256:	FEF5FD1F665F1D5B2DEE6D94C370A9FD3645B671CC99D23B1D05B2231B634A2C
SHA-512:	D6B1F383938778FE054DAA146AA511FEF59DDDB6244574DC98D41684F401A328F5354C09A1CE3E4E4AE6CFC8F55A8F73345EE4E20AC2A29FD83538387A4B57F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.... .8...._keyhttps://static.hotjar.com/c/hotjar-565550.js?sv=5 .https://milanote.com/=.|..#/.....P.....t.l."mFY. .dw.....`).....N..A..Eo.....Ql.2.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0688fad751c19b35_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.635054300075892
Encrypted:	false
SSDEEP:	6:mKsEYGLKdXNQKjsELq0G+AUn6q/xVOfAzrSK6t:p0hNQKjsELq/Cn6GLOfwg
MD5:	7D207CD6A487723E1240BEAB7F2D5C93
SHA1:	0A8CCA9E05FF9CA771C2CC7A6D85DA78C9514D71
SHA-256:	03866D13311CB39E940E4559BBA5D79707EDBA40AD80E9E2421E78F42D18276A
SHA-512:	C5E4E3C888D047ADB3C291E2DEF56D1723C79CE1764965275813D6C3616C5719EF8426DEB7097F6C886ADC753345974C6A034FD76975C0F0EC3E53CB7CC0EE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0688fad751c19b35_0	
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://www.gstatic.com/recaptcha/releases/CdDdhZfPbLLrfYLBdThNS0-Y/recaptcha__en.js .https://milanote.com/@3...#/.....)p.....a.rl$ ..7.....@.ODT..R.V..W...A..Eo.....jJ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\09bc3e1afcfb1edc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	433
Entropy (8bit):	5.850721132019261
Encrypted:	false
SSDEEP:	6:mdfDVYGLKdGMwjM71/XER3M75VMQmkpUSXscTkbNQYSyZZkvimuKaYMwPtt4DHbD:Sro9wwhy8fcIs/pFZZkvi7Kp9y
MD5:	CD3889251A26C274A92F2CA420E28592
SHA1:	98089346EA7F33E5321B35074ECE07C2908DE323
SHA-256:	2EF5C2E04D72FA05C2E2675BE302803A3A7D321BECD42037CB946D9A91C03A3B
SHA-512:	1619C39B73BC02822FE216B4449457E3B00AA6C0CBAFB967C3B0230167EC5F72D1EB6EF4532A82CCB6FBAF6B94771CD7CFE87CF2CACD056272E81C2404A64C B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....-...x....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en.ROaJ9ynLGFI.es5.O/ck=boq-identity.IdentityPoliciesUi.920uE yzD5CA.L.B1.O/am=FDAg/d=1/exm=_b,_tp/excm=_b,_tp,termshomeview/ed=1/wt=2/rs=AOaEmlHsweInmKcI_ympQaYZkeJ1kYHUVw/m=byfTOb,lsjVmc,LEikZe .https ://google.com/.....#/.....Ysr.m.J<c.....S..j.~.4GB!..9.y.A..Eo.....E.y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bd7a193caaa1084_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	357
Entropy (8bit):	5.80135769933985
Encrypted:	false
SSDEEP:	6:mr/VYGLKdGMwjM71/s9cxbOacQGD65SqUcur6E371UCVjrbrRK6t:Qo9wwh/s9cx9cV+5SqUNZPbH
MD5:	490FE1208BA4A424064324841644FEE1
SHA1:	4CC64F65751BB152DE1B4E84829D4DD1CA9A5913
SHA-256:	82344905EC2B9BD742C2D9C0AC315E0E7AD20C60D4B57E1774581D805DB9EC6B
SHA-512:	FCF24197436162A52C8951B108F3F47C9A8FBB6A2C919F22A5FC86A8B7C86F3B5BC2E112A203EB61686039F0086D35882DFF8A78CB9858908860D20BCFB526A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....9....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en_US.pWi_f_o0gHU.es5.O/am=FDAg/d=1/excm=_b,_tp,ho meview/ed=1/dg=0/wt=2/rs=AOaEmlGoetiJLF1PxJAGy4eEXb19nk7wZg/m=_b,_tp .https://google.com/C*}..#/.....V-.....5u(.O.+...9...%..?.e+..}c...P.A..Eo.....A$W..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1154c6710157da27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.4413970336123
Encrypted:	false
SSDEEP:	3:m+loGxlzA8RzYrSLLiMIwJJSp2KZlJmflHCMj//vqrMjWxkh6qUm4E/lpK5kt:mWj9YGL+MIwJJGZ6AG/JjWc/jbK6t
MD5:	70CDB26ACD241464B677AE21DA28CA4D
SHA1:	E723268CDE2DCC633ED9F64640B8099D44474873
SHA-256:	BC78A12D932B11AB7522C0E5DB5A4A14A6B3A15B2EDB92B879DD433971CC6B44
SHA-512:	44CB4562A2CA4470F9D808B4A6FC354C706A0781401C6C8FC0994646FD8AE41F08AFA4E3D3C97C77C483D75E4FF1F2CEC19A4F9A0EACB213461F3240DD94EA 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...6..N...._keyhttps://www.google-analytics.com/analytics.js .https://about.google/l....#/.....)D.....3k...w[..).`P_s..Y...`W.....A..Eo.....xMH.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12fc5b60660b3e84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1031

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12fc5b60660b3e84_0	
Entropy (8bit):	6.049251867263613
Encrypted:	false
SSDEEP:	24:Yww/EmtX4KuLMZkCP+T9WAobrN95pjrf+29H:YN/EmF4RCPa9RobrNpX59H
MD5:	83B328625F4611D4794B8B3E48AB1F9A
SHA1:	14606C20E67D0E8A3CBAD9E6573E7F89DDF7443A
SHA-256:	85CEE6783213F3189B43D507A00C17C5D740EC770F7E98845E64D1B213208684
SHA-512:	9B9C315334ECDE63BDB54CB558121A513B6EE4D9DF23239C4D139CB71F0F80DFE628A4D9BE5799457C7F0D28C26E885D76D397CBE0EF6A14A8BDF67DF169A(89
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]V....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en.ROaJ9ynLGFI.es5.O/ck=boq-identity.IdentityPoliciesUi.920u EyzD5CA.L.B1.O/am=FDAg/d=1/exm=A4UTCb,A7fCU,BVgquf,BqFhcd,CBlRxf,COQbmf,EFQ78c,FqLSBc,HDvRde,HLo3Ef,IZT63,IavLJc,JNoxi,Jis5wf,KG2eXe,KUM7Z,L 1AAkb,LEikZe,MdUzUe,MpJwZc,NpD4ec,NwH0H,O1Gjze,O6y8ed,O8k1Cd,OmgaI,PQaYAf,PrPYRd,QIhFr,RMhBfe,Ru0Pgb,SF3gsd,SdcwHb,SpsfSb,U0aPgd,U UJqVe,Uas9Hd,UgAtXe,Ulmmrd,V3dDOb,VXdfxd,VwDzFe,XVMNvd,Y2UGcc,YLQSd,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,b7FMof,blwjVc,byfTOb,duFQFc,e5qFLc,fKUV 3e,gychg,hTAg0b,hc6Ubd,iTsyac,iWP1Yb,krBSJd,lPKSwe,lfpdyf,lsjVmc,lwddkf,n73qwf,o02Jie,p8L0ob,pB6Zqd,pjICDe,pw70Gc,r2V6Pd,rHjpXd,s39S4,tfTN8c,uiNkee,w9 hDv,wmlPKb,ws9Tlc,x60fie,xQtZb,xUdipf,xiqEse,yDVVkb,yJVP7e,zbML3c/excm=_b,_tp,privacyhomeview/ed=1/wt=2/rs=AOaEmlHsweInmKcI_ympQaYZkeJ1kYHUV w/m=Wt6vjf,_latency,FCpbqb,WhJNk .https://google.com/.B...#/.....].DtlB..j+..F..>..~hs]mM....A..Eo...../.Wa.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17dc95475a6002b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.522310891268122
Encrypted:	false
SSDEEP:	6:mY+lyEYk+ALqwIPG6+mLJqgklXBUQk5NCDlRK6t:F+lb+ALqwIPx+mLDsRUQwNMr
MD5:	2E969607E001114D4FC4E811413354E5
SHA1:	C1D5403D466BF373D1B09BB5FC363D208BACFFD9
SHA-256:	A9DD986AF758C2334B6BC9C0A4C81CEC63254121CC2FA9D1CE5F6D2F07A238AB
SHA-512:	D3125145F6EA6078F70FD036201BA92F6CBF38B7488161305680084ED821C7831934EF69592F1D2BCA99EEA7887A8A7F88D90A7355198E6CEA519E94AEBBE540
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....y....._keyhttps://static.milanote.com/icons-light-small-cf8ec91f5bc3-modern.js .https://milanote.com/....#/.....q.....k.O..s.6..5...}..;.(bK0.:.....A..Eo.....b .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b74565d095aa82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.512268525723466
Encrypted:	false
SSDEEP:	6:m4XYk+AL0P7v2/LmLjyakl/CGgYQHlZK6t:hz+ALK4LmLYtDOT
MD5:	45A90D06EE1F591DAC0AE6EB56B751A0
SHA1:	C25BF667D7261CAA4910423912A3EF15DCE1E3FB
SHA-256:	93A743A6FD6DA6D7C25D068C0F8562E39C34C868F0A8F75D26B014E385853A0D
SHA-512:	FA1E7C3958B0ED9A71CDEBA9968B9DBAE9BAB876D781E6BBF101E3874AF73893E5263B68E380080EF50EDD690B6D47C451CDE1F58D5213880B5C1113F6E4C1 D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...sl)....._keyhttps://static.milanote.com/workspace-1981a238f450-modern.js .https://milanote.com/....#/.....lq.....}[.F.h.S;+..+..w~..!.gj.SHq.c.A..Eo..... .o.l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d9307e50ef6b7b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.4064417696612646
Encrypted:	false
SSDEEP:	6:maYGLKdZgRbLe8INdZgdpA1/vd4F8nK6t:mjybLlIN8ALp
MD5:	A24CCFB1FB644C3009DBF101CD3BDEE9
SHA1:	0DB7C78FE60848DF27DDAD0D9EEBF375AC4B7518
SHA-256:	AB995C26EE525FEBE88C6BE9F49B7871884C21AF874566D86095505DC2C49FCA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d9307e50ef6b7b0_0	
SHA-512:	6700042E9512593979D3775160AED2CA8897CF0D154DEA11F5D6B5CF45BCE93157BCB0512F74C2C43C5BDC3665881C1CD69E9810D2992CECE35FA9AA6EE5E4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t...P_k%...._keyhttps://www.gstatic.com/brandstudio/kato/cookie_choice_component/cookie_consent_bar.v3.js .https://about.google/.....#/.....J@.....ex.{T.;4.a[..Tt.NzpL..q.@..8...A..Eo.....|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fc81d98e0bca5b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	435
Entropy (8bit):	5.886414151887081
Encrypted:	false
SSDEEP:	6:mbYGLKdGMwjM71/XER3M75VMQmkpUSXs7ImIbNQYSyZZkvimuBxG+A+0QCk4ThK+:79wwhy8fcIsU5pFZZkvi7HndgkI7
MD5:	A979AC3194352E612C06E444BB5BA7D1
SHA1:	0F90CA44FCF177E506BF15F83F39F24FB6DDB8ED
SHA-256:	9D5321DF17DD404F74D6687E859B0D860DFFC0855D203E8E7D874D32444A4D48
SHA-512:	C20A988540089B173208ED0C51748B6D7C855BA5DC9005E32F42510082A2DF982E173F751D35E17BB4A186A6A2D4DF236BE9D8BA25353DD5AB65778CB973185
Malicious:	false
Reputation:	low
Preview:	0\r..m...../...I....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en.ROaJ9ynLGFI.es5.O/ck=boq-identity.IdentityPoliciesUi.920uEyzD5CA.L.B1.O/am=FDAg/d=1/exm=_b,_tp/excm=_b,_tp,privacyhomeview/ed=1/wt=2/rs=AOaEmlHsweInmKcI_ympQaYZkeJ1kYHUVw/m=byfTOb,lsjVmc,LEikZe .https://google.com/..h..#/.....J.....@....%....H.....i.....k...y.A..Eo.....e^.A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fde12061b590deb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	950
Entropy (8bit):	6.092787213167129
Encrypted:	false
SSDEEP:	24:iww/dpLTt7pdJQzibQVKJfpzobhp3m+A75G:iN/dpdzJQhVKw/A9G
MD5:	EA94A317A218F836F400117F780ED7FC
SHA1:	102CDF90B736BD1DADEF0AAC3E8C0801FC65A192
SHA-256:	B24D8B7C9A31F2D6B6DBC9DBF6E725582F97B77C14954950FE200555D10745F8
SHA-512:	99CA2683A1296486ACBF1EF2A8B5475229E215C7CE3D668240A52D83A5DE3CC30BE16CD857DA012A7C876E28D7813CE3BF62CF94F24A317BC2B3A6444258836
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2.....j....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.IdentityPoliciesUi.en.ROaJ9ynLGFI.es5.O/ck=boq-identity.IdentityPoliciesUi.920uEyzD5CA.L.B1.O/am=FDAg/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,termshomeview/ed=1/wt=2/rs=AOaEmlHsweInmKcI_ympQaYZkeJ1kYHUVw/m=n73qwf,ws9Tlc,IZT63,e5qFLc,UUJqVe,O1Gjze,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,r2V6Pd,p8L0ob,O6y8ed,NpD4ec,PrPYRd,MpJwZc,O8k1Cd,NwH0H,OmgaI,HLo3Ef,x60fie,xiqEse,hTAg0b,XVMNvd,L1AAkb,KUM7Z,lfpdyf,duFQFc,s39S4,Jis5wf,lwddkf,gychg,w9hDv,RMhBfe,Y2UGcc,SdcwHb,aW3pY,YLQSd,PQaYAf,iWP1Yb,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,Ru0Pgb,CBlRxf,EGlAz,xQtZb,lPKSwe,MdUzUe,QIhFr,JNoxi,b7FMof,rHjpXd,yDVVkb,pB6Zqd,SF3gsd,iTsyac,hc6Ubd,KG2eXe,SpsfSb,tfTN8c,o02Jie,VwDzFe,zbML3c,HDvRde,Uas9Hd,BVgquf,yJVP7e,A7fCU,UgAtXe,pjICDe .https://google.com/k....#/.....(.^..b.(.*Z;.....z..(...%...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d644143157c1488_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.440475773405396
Encrypted:	false
SSDEEP:	3:m+lBiFls8RzY9iRbwBLKRQflHCMlxcRtvdZwk9Wm1wt/lpK5kt:mTl9Y9i9aL8QAMlxcLlOSSbK6t
MD5:	6B1D00D997903368EDF1B502909738F0
SHA1:	16F05156FD714D6B019DE9B9E49DE53B7E612C64
SHA-256:	24A4D96F547F4FF6E5A125CD17449E2CC36A79FA3EF61F9804FDF6A85E25B03B
SHA-512:	20BC7955A4982E6EF7C7B78ABF97A18A3816FC5BA79596B6CDCEC429756FCA26D156209710361F357B41B97D43B1902344C1070D3562AAD80C5F78679A3C0C0E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....9...M....._keyhttps://a.quora.com/qevents.js .https://milanote.com/.Wz..#/.....U...\,.....->.x..V.....+....^E.A..Eo.....j.).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30f34755fdaaef11_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30f34755fdaaef11_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.390159112876164
Encrypted:	false
SSDEEP:	3:m+lMpXIv8RzYP2FycyGeULSQFvD0MDMKY9flHCAtwMw8SbrnAt79kRmbt/pK5kt:mAEYexMv9AAwMwRbrnAtuAphK6t
MD5:	54CA7ACC0C1D5C96BE00B1C10A1EAD31
SHA1:	7483C7666D3BF1F10A833F0D4B33929DE6F451FF
SHA-256:	C31DBB081738BB4844CF30C24BDB5F586BA8A25E9792E484D5F5998E78C12D94
SHA-512:	B40150262676341BFC3DA37600007A544A7E7A3B094D779B6FC12B0DDFAA0A5AFFD4D0BD4C1D5860870B178B46B755BA3101BAD9B5F5F65560323972A27D5CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....d.H...._keyhttps://code.jquery.com/jquery-2.1.1.min.js .https://prismic.io/.z...#/.....j).....R.8.S..*.L.....F.t.G.s..A..Eo.....k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31f82312ae6d6e09_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.5784462266550365
Encrypted:	false
SSDEEP:	6:mgAYGLUxwz1lT2buGgkyvyjtQpNupN6EYtRK6t:NUP6buGgGtQSpoEO
MD5:	588A747F85FD9CDC7DFF23D635BC4E0C
SHA1:	13C9286798A99DB85B98497D4BD7B97391AD99AC
SHA-256:	A50248D70AC31CBB0AF3AFDDE3333F65633E6EB44C754982CC66AE754FC82B42
SHA-512:	3123358BCD1C3793840A991F55A7DCF26B81FEFD998C26B77DBAAC36C092248EBBAA50BB8E708A3463D178B86F0F77512DA99F8EDC7189E5CD79FFE0EFEB4A4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w.....i?...._keyhttps://www.youtube-nocookie.com/s/player/a0094ae9/player_ias.vflset/en_US/remote.js .https://youtube-nocookie.com/+.}..#/..... ....2eIVJ8..[4..|.....<..._..~..A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33e5517cffb503cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.4008763801187465
Encrypted:	false
SSDEEP:	6:m+/XYAWQf257aL+6AqktlIS90fbd/N0DK6t:Xde5mL+6KQ9SF01
MD5:	1BC2FBB567FB4C773602F9BAAEF4CCE8
SHA1:	7510BF74B67189D5BFB782DF8E995DB38B7EAE16
SHA-256:	8E984DCE9DDC14CE4F559D731293EB08D69043B42753D6BB9B2C490E73F8FE0A
SHA-512:	4BD82B8BE3E6F9482E9627059E4A1F87EE30F07290D76236BF58CD6C04A2AEF74781C6FD7AD8163ABDF412F41F35683DE313E8CF696987872F12A295CA4A7572
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....y....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://milanote.com/p7z..#/.....q....y.>.mm.....H.....S.).....J.A..Eo.....A..Eo..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 06:46:48.127780914 CEST	192.168.2.3	8.8.8.8	0x63de	Standard query (0)	app.milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.042967081 CEST	192.168.2.3	8.8.8.8	0x3655	Standard query (0)	static.milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.378298044 CEST	192.168.2.3	8.8.8.8	0xfa20	Standard query (0)	cdn.amplitude.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.380489111 CEST	192.168.2.3	8.8.8.8	0x6e4a	Standard query (0)	d37gvrvc0wt4s1.cloudfront.net	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.494024038 CEST	192.168.2.3	8.8.8.8	0xb104	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.900798082 CEST	192.168.2.3	8.8.8.8	0x2f20	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.169523001 CEST	192.168.2.3	8.8.8.8	0x21eb	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.354871988 CEST	192.168.2.3	8.8.8.8	0xda67	Standard query (0)	api.amplitude.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:52.787848949 CEST	192.168.2.3	8.8.8.8	0xced8	Standard query (0)	widget.intercom.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.046638966 CEST	192.168.2.3	8.8.8.8	0x4d47	Standard query (0)	js.intercomcdn.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.505266905 CEST	192.168.2.3	8.8.8.8	0x7b3	Standard query (0)	api-iam.intercom.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.988547087 CEST	192.168.2.3	8.8.8.8	0xf9	Standard query (0)	app.milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.679225922 CEST	192.168.2.3	8.8.8.8	0xd897	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:58.503895998 CEST	192.168.2.3	8.8.8.8	0x38e	Standard query (0)	www.youtube-nocookie.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:03.991609097 CEST	192.168.2.3	8.8.8.8	0xfdf4	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.797753096 CEST	192.168.2.3	8.8.8.8	0x868c	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.816591978 CEST	192.168.2.3	8.8.8.8	0xbc1e	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.003602028 CEST	192.168.2.3	8.8.8.8	0xbaf9	Standard query (0)	www.milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.591267109 CEST	192.168.2.3	8.8.8.8	0x4d87	Standard query (0)	milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.053494930 CEST	192.168.2.3	8.8.8.8	0xc505	Standard query (0)	static.cdn.prismic.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.282696962 CEST	192.168.2.3	8.8.8.8	0xf3a3	Standard query (0)	images.prismic.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.496668100 CEST	192.168.2.3	8.8.8.8	0x36e1	Standard query (0)	prismic-io.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.159651995 CEST	192.168.2.3	8.8.8.8	0xe9d8	Standard query (0)	milanote.prismic.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.861295938 CEST	192.168.2.3	8.8.8.8	0x94c3	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.877372980 CEST	192.168.2.3	8.8.8.8	0x3ac6	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.878796101 CEST	192.168.2.3	8.8.8.8	0xca51	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.879273891 CEST	192.168.2.3	8.8.8.8	0x1aa1	Standard query (0)	a.quora.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.201819897 CEST	192.168.2.3	8.8.8.8	0xfc24	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.364461899 CEST	192.168.2.3	8.8.8.8	0x6269	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.365668058 CEST	192.168.2.3	8.8.8.8	0x6760	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 06:47:21.378587961 CEST	192.168.2.3	8.8.8.8	0x4dfb	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.379345894 CEST	192.168.2.3	8.8.8.8	0x3052	Standard query (0)	huntr.in	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.379465103 CEST	192.168.2.3	8.8.8.8	0x774	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.456474066 CEST	192.168.2.3	8.8.8.8	0x6857	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:22.276413918 CEST	192.168.2.3	8.8.8.8	0x73fc	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:22.983962059 CEST	192.168.2.3	8.8.8.8	0x5d15	Standard query (0)	milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.159774065 CEST	192.168.2.3	8.8.8.8	0x273c	Standard query (0)	images.prismic.io	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.209733009 CEST	192.168.2.3	8.8.8.8	0x373e	Standard query (0)	prismic-io.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.292843103 CEST	192.168.2.3	8.8.8.8	0x150f	Standard query (0)	static.milanote.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.729952097 CEST	192.168.2.3	8.8.8.8	0x4e1c	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:26.751982927 CEST	192.168.2.3	8.8.8.8	0x53bd	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:42.467888117 CEST	192.168.2.3	8.8.8.8	0x31cb	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:43.002856016 CEST	192.168.2.3	8.8.8.8	0x47a7	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:43.983493090 CEST	192.168.2.3	8.8.8.8	0x8012	Standard query (0)	www.blog.google	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:45.565413952 CEST	192.168.2.3	8.8.8.8	0xc459	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:48.953238010 CEST	192.168.2.3	8.8.8.8	0x6cb	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Jun 11, 2021 06:49:45.647181988 CEST	192.168.2.3	8.8.8.8	0x7d43	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:46:48.187241077 CEST	8.8.8.8	192.168.2.3	0x63de	No error (0)	app.milanote.com		34.198.55.140	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:48.187241077 CEST	8.8.8.8	192.168.2.3	0x63de	No error (0)	app.milanote.com		3.213.84.19	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:48.187241077 CEST	8.8.8.8	192.168.2.3	0x63de	No error (0)	app.milanote.com		54.235.149.247	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:48.187241077 CEST	8.8.8.8	192.168.2.3	0x63de	No error (0)	app.milanote.com		35.172.55.187	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.104676962 CEST	8.8.8.8	192.168.2.3	0x3655	No error (0)	static.milanote.com		13.224.99.113	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.104676962 CEST	8.8.8.8	192.168.2.3	0x3655	No error (0)	static.milanote.com		13.224.99.31	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.104676962 CEST	8.8.8.8	192.168.2.3	0x3655	No error (0)	static.milanote.com		13.224.99.123	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.104676962 CEST	8.8.8.8	192.168.2.3	0x3655	No error (0)	static.milanote.com		13.224.99.128	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.442064047 CEST	8.8.8.8	192.168.2.3	0xfa20	No error (0)	cdn.amplitude.com		13.224.89.71	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.442064047 CEST	8.8.8.8	192.168.2.3	0xfa20	No error (0)	cdn.amplitude.com		13.224.89.35	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.442064047 CEST	8.8.8.8	192.168.2.3	0xfa20	No error (0)	cdn.amplitude.com		13.224.89.45	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.442064047 CEST	8.8.8.8	192.168.2.3	0xfa20	No error (0)	cdn.amplitude.com		13.224.89.109	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:46:49.449139118 CEST	8.8.8.8	192.168.2.3	0x6e4a	No error (0)	d37gvrvc0wt4s1.cloudfront.net		13.224.89.197	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.449139118 CEST	8.8.8.8	192.168.2.3	0x6e4a	No error (0)	d37gvrvc0wt4s1.cloudfront.net		13.224.89.80	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.449139118 CEST	8.8.8.8	192.168.2.3	0x6e4a	No error (0)	d37gvrvc0wt4s1.cloudfront.net		13.224.89.22	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:49.449139118 CEST	8.8.8.8	192.168.2.3	0x6e4a	No error (0)	d37gvrvc0wt4s1.cloudfront.net		13.224.89.79	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.559787989 CEST	8.8.8.8	192.168.2.3	0xb104	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.559787989 CEST	8.8.8.8	192.168.2.3	0xb104	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.953305006 CEST	8.8.8.8	192.168.2.3	0x2f20	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:46:50.953305006 CEST	8.8.8.8	192.168.2.3	0x2f20	No error (0)	stats.l.doubleclick.net		142.251.5.155	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.953305006 CEST	8.8.8.8	192.168.2.3	0x2f20	No error (0)	stats.l.doubleclick.net		142.251.5.157	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.953305006 CEST	8.8.8.8	192.168.2.3	0x2f20	No error (0)	stats.l.doubleclick.net		142.251.5.154	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:50.953305006 CEST	8.8.8.8	192.168.2.3	0x2f20	No error (0)	stats.l.doubleclick.net		142.251.5.156	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.236717939 CEST	8.8.8.8	192.168.2.3	0x21eb	No error (0)	www.google.de		172.217.18.67	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		34.217.196.79	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		52.27.22.245	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		44.235.41.194	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		34.208.141.66	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		35.83.183.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		52.25.178.156	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		35.163.112.20	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:51.405421019 CEST	8.8.8.8	192.168.2.3	0xda67	No error (0)	api.amplitude.com		34.213.101.166	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:52.849708080 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	widget.intercom.io		13.224.99.109	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:52.849708080 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	widget.intercom.io		13.224.99.107	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:52.849708080 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	widget.intercom.io		13.224.99.10	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:52.849708080 CEST	8.8.8.8	192.168.2.3	0xced8	No error (0)	widget.intercom.io		13.224.99.33	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.115277052 CEST	8.8.8.8	192.168.2.3	0x4d47	No error (0)	js.intercomcdn.com		13.224.99.75	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.115277052 CEST	8.8.8.8	192.168.2.3	0x4d47	No error (0)	js.intercomcdn.com		13.224.99.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:46:53.115277052 CEST	8.8.8.8	192.168.2.3	0x4d47	No error (0)	js.intercomcdn.com		13.224.99.60	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.115277052 CEST	8.8.8.8	192.168.2.3	0x4d47	No error (0)	js.intercomcdn.com		13.224.99.116	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.557910919 CEST	8.8.8.8	192.168.2.3	0x7b3	No error (0)	api-iam.intercom.io		99.83.219.81	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:53.557910919 CEST	8.8.8.8	192.168.2.3	0x7b3	No error (0)	api-iam.intercom.io		75.2.88.188	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.047326088 CEST	8.8.8.8	192.168.2.3	0xf9	No error (0)	app.milanote.com		35.172.55.187	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.047326088 CEST	8.8.8.8	192.168.2.3	0xf9	No error (0)	app.milanote.com		34.198.55.140	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.047326088 CEST	8.8.8.8	192.168.2.3	0xf9	No error (0)	app.milanote.com		3.213.84.19	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.047326088 CEST	8.8.8.8	192.168.2.3	0xf9	No error (0)	app.milanote.com		54.235.149.247	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.729440928 CEST	8.8.8.8	192.168.2.3	0xd897	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.729440928 CEST	8.8.8.8	192.168.2.3	0xd897	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:54.729440928 CEST	8.8.8.8	192.168.2.3	0xd897	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Jun 11, 2021 06:46:58.573512077 CEST	8.8.8.8	192.168.2.3	0x38e	No error (0)	www.youtube-nocookie.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:04.074322939 CEST	8.8.8.8	192.168.2.3	0xfdf4	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:04.074322939 CEST	8.8.8.8	192.168.2.3	0xfdf4	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.859097958 CEST	8.8.8.8	192.168.2.3	0x868c	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:04.859097958 CEST	8.8.8.8	192.168.2.3	0x868c	No error (0)	photos-ugc.l.googleusercontent.com		216.58.214.225	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		172.217.18.86	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		172.217.19.118	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		172.217.20.22	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		142.250.180.214	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		142.250.180.246	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		142.250.201.214	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		216.58.214.214	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:04.884509087 CEST	8.8.8.8	192.168.2.3	0xbc1e	No error (0)	i.ytimg.com		172.217.16.118	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.068936110 CEST	8.8.8.8	192.168.2.3	0xbaf9	No error (0)	www.milanote.com		13.224.99.118	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.068936110 CEST	8.8.8.8	192.168.2.3	0xbaf9	No error (0)	www.milanote.com		13.224.99.122	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:47:18.068936110 CEST	8.8.8.8	192.168.2.3	0xbaf9	No error (0)	www.milanote.com		13.224.99.97	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.068936110 CEST	8.8.8.8	192.168.2.3	0xbaf9	No error (0)	www.milanote.com		13.224.99.67	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.653554916 CEST	8.8.8.8	192.168.2.3	0x4d87	No error (0)	milanote.com		13.224.99.118	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.653554916 CEST	8.8.8.8	192.168.2.3	0x4d87	No error (0)	milanote.com		13.224.99.67	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.653554916 CEST	8.8.8.8	192.168.2.3	0x4d87	No error (0)	milanote.com		13.224.99.97	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:18.653554916 CEST	8.8.8.8	192.168.2.3	0x4d87	No error (0)	milanote.com		13.224.99.122	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.128293991 CEST	8.8.8.8	192.168.2.3	0xc505	No error (0)	static.cdn.prismic.io	d119wgbtegajwl.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:19.128293991 CEST	8.8.8.8	192.168.2.3	0xc505	No error (0)	d119wgbtegajwl.cloudfront.net		13.224.99.81	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.128293991 CEST	8.8.8.8	192.168.2.3	0xc505	No error (0)	d119wgbtegajwl.cloudfront.net		13.224.99.125	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.128293991 CEST	8.8.8.8	192.168.2.3	0xc505	No error (0)	d119wgbtegajwl.cloudfront.net		13.224.99.95	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.128293991 CEST	8.8.8.8	192.168.2.3	0xc505	No error (0)	d119wgbtegajwl.cloudfront.net		13.224.99.36	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.345940113 CEST	8.8.8.8	192.168.2.3	0xf3a3	No error (0)	images.prismic.io	prismic-io.imgix.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:19.345940113 CEST	8.8.8.8	192.168.2.3	0xf3a3	No error (0)	prismic-io.imgix.net	dualstack.com.imgix.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:19.345940113 CEST	8.8.8.8	192.168.2.3	0xf3a3	No error (0)	dualstack.com.imgix.map.fastly.net		151.101.114.208	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:19.558634043 CEST	8.8.8.8	192.168.2.3	0x36e1	No error (0)	prismic-io.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:19.558634043 CEST	8.8.8.8	192.168.2.3	0x36e1	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:19.558634043 CEST	8.8.8.8	192.168.2.3	0x36e1	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.92.196	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.335217953 CEST	8.8.8.8	192.168.2.3	0xe9d8	No error (0)	milanote.prismic.io		52.55.94.115	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.335217953 CEST	8.8.8.8	192.168.2.3	0xe9d8	No error (0)	milanote.prismic.io		34.238.91.71	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.335217953 CEST	8.8.8.8	192.168.2.3	0xe9d8	No error (0)	milanote.prismic.io		18.234.4.250	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.914630890 CEST	8.8.8.8	192.168.2.3	0x94c3	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:20.914630890 CEST	8.8.8.8	192.168.2.3	0x94c3	No error (0)	scontent.xx.fbcdn.net		157.240.27.27	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.932070971 CEST	8.8.8.8	192.168.2.3	0xca51	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:20.932070971 CEST	8.8.8.8	192.168.2.3	0xca51	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.939637899 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:20.939637899 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	static-cdn.hotjar.com		13.224.99.122	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:47:20.939637899 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	static-cdn .hotjar.com		13.224.99.100	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.939637899 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	static-cdn .hotjar.com		13.224.99.50	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.939637899 CEST	8.8.8.8	192.168.2.3	0x3ac6	No error (0)	static-cdn .hotjar.com		13.224.99.58	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.940926075 CEST	8.8.8.8	192.168.2.3	0x1aa1	No error (0)	a.quora.com	quora.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:20.940926075 CEST	8.8.8.8	192.168.2.3	0x1aa1	No error (0)	quora.map. fastly.net		151.101.1.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.940926075 CEST	8.8.8.8	192.168.2.3	0x1aa1	No error (0)	quora.map. fastly.net		151.101.65.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.940926075 CEST	8.8.8.8	192.168.2.3	0x1aa1	No error (0)	quora.map. fastly.net		151.101.129.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:20.940926075 CEST	8.8.8.8	192.168.2.3	0x1aa1	No error (0)	quora.map. fastly.net		151.101.193.2	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		18.215.205.165	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		18.205.51.212	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		3.224.194.150	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.252149105 CEST	8.8.8.8	192.168.2.3	0xfc24	No error (0)	q.quora.com		52.71.230.189	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.426170111 CEST	8.8.8.8	192.168.2.3	0x6269	No error (0)	script.hotjar.com		13.224.99.26	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.426170111 CEST	8.8.8.8	192.168.2.3	0x6269	No error (0)	script.hotjar.com		13.224.99.44	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.426170111 CEST	8.8.8.8	192.168.2.3	0x6269	No error (0)	script.hotjar.com		13.224.99.33	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.426170111 CEST	8.8.8.8	192.168.2.3	0x6269	No error (0)	script.hotjar.com		13.224.99.19	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.429456949 CEST	8.8.8.8	192.168.2.3	0x6760	No error (0)	www.facebo ok.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:21.429456949 CEST	8.8.8.8	192.168.2.3	0x6760	No error (0)	star-mini. c10r.faceb ook.com		31.13.92.36	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.429490089 CEST	8.8.8.8	192.168.2.3	0x774	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.429490089 CEST	8.8.8.8	192.168.2.3	0x774	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.429490089 CEST	8.8.8.8	192.168.2.3	0x774	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.429490089 CEST	8.8.8.8	192.168.2.3	0x774	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.443212032 CEST	8.8.8.8	192.168.2.3	0x4dfb	No error (0)	vars.hotjar.com		13.224.99.109	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.443212032 CEST	8.8.8.8	192.168.2.3	0x4dfb	No error (0)	vars.hotjar.com		13.224.99.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:47:21.443212032 CEST	8.8.8.8	192.168.2.3	0x4dfb	No error (0)	vars.hotjar.com		13.224.99.12	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.443212032 CEST	8.8.8.8	192.168.2.3	0x4dfb	No error (0)	vars.hotjar.com		13.224.99.33	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:21.523417950 CEST	8.8.8.8	192.168.2.3	0x6857	No error (0)	googleads.g.doubleclick.net		142.250.180.226	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:22.344520092 CEST	8.8.8.8	192.168.2.3	0x73fc	No error (0)	www.google.ch		172.217.20.3	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.043716908 CEST	8.8.8.8	192.168.2.3	0x5d15	No error (0)	milanote.com		13.224.99.118	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.043716908 CEST	8.8.8.8	192.168.2.3	0x5d15	No error (0)	milanote.com		13.224.99.67	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.043716908 CEST	8.8.8.8	192.168.2.3	0x5d15	No error (0)	milanote.com		13.224.99.97	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.043716908 CEST	8.8.8.8	192.168.2.3	0x5d15	No error (0)	milanote.com		13.224.99.122	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:23.223622084 CEST	8.8.8.8	192.168.2.3	0x273c	No error (0)	images.prismic.io	prismic-io.imgix.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:23.223622084 CEST	8.8.8.8	192.168.2.3	0x273c	No error (0)	prismic-io.imgix.net	dualstack.com.imgix.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:23.223622084 CEST	8.8.8.8	192.168.2.3	0x273c	No error (0)	dualstack.com.imgix.map.fastly.net		151.101.14.208	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.273344040 CEST	8.8.8.8	192.168.2.3	0x373e	No error (0)	prismic-io.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:25.273344040 CEST	8.8.8.8	192.168.2.3	0x373e	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:25.273344040 CEST	8.8.8.8	192.168.2.3	0x373e	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.128.129	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.351845026 CEST	8.8.8.8	192.168.2.3	0x150f	No error (0)	static.milanote.com		13.224.99.113	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.351845026 CEST	8.8.8.8	192.168.2.3	0x150f	No error (0)	static.milanote.com		13.224.99.31	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.351845026 CEST	8.8.8.8	192.168.2.3	0x150f	No error (0)	static.milanote.com		13.224.99.123	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.351845026 CEST	8.8.8.8	192.168.2.3	0x150f	No error (0)	static.milanote.com		13.224.99.128	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:25.783478022 CEST	8.8.8.8	192.168.2.3	0x4e1c	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:26.805588007 CEST	8.8.8.8	192.168.2.3	0x53bd	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:42.529597998 CEST	8.8.8.8	192.168.2.3	0x31cb	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 06:47:43.072618008 CEST	8.8.8.8	192.168.2.3	0x47a7	No error (0)	lh3.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:43.072618008 CEST	8.8.8.8	192.168.2.3	0x47a7	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:44.053847075 CEST	8.8.8.8	192.168.2.3	0x8012	No error (0)	www.blog.google	ghs-svc-https-sni.ghs-ssl.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:44.053847075 CEST	8.8.8.8	192.168.2.3	0x8012	No error (0)	ghs-svc-https-sni.ghs-ssl.googlehosted.com		142.250.180.243	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:45.628099918 CEST	8.8.8.8	192.168.2.3	0xc459	No error (0)	lh3.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:47:45.628099918 CEST	8.8.8.8	192.168.2.3	0xc459	No error (0)	googlehosted.l.googleusercontent.com		142.250.180.225	A (IP address)	IN (0x0001)
Jun 11, 2021 06:47:49.020220041 CEST	8.8.8.8	192.168.2.3	0x6cb	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:49:45.697752953 CEST	8.8.8.8	192.168.2.3	0x7d43	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 06:49:45.697752953 CEST	8.8.8.8	192.168.2.3	0x7d43	No error (0)	stats.l.doubleclick.net		142.251.5.155	A (IP address)	IN (0x0001)
Jun 11, 2021 06:49:45.697752953 CEST	8.8.8.8	192.168.2.3	0x7d43	No error (0)	stats.l.doubleclick.net		142.251.5.157	A (IP address)	IN (0x0001)
Jun 11, 2021 06:49:45.697752953 CEST	8.8.8.8	192.168.2.3	0x7d43	No error (0)	stats.l.doubleclick.net		142.251.5.154	A (IP address)	IN (0x0001)
Jun 11, 2021 06:49:45.697752953 CEST	8.8.8.8	192.168.2.3	0x7d43	No error (0)	stats.l.doubleclick.net		142.251.5.156	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- app.milanote.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	34.198.55.140	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 06:46:48.325531960 CEST	1273	OUT	GET /1LQWMe1tFoGL1X?p=oGL1dCkr1ut HTTP/1.1 Host: app.milanote.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Jun 11, 2021 06:46:48.457814932 CEST	1278	IN	HTTP/1.1 301 Moved Permanently Server: awselb/2.0 Date: Fri, 11 Jun 2021 04:46:48 GMT Content-Type: text/html Content-Length: 134 Connection: keep-alive Location: https://app.milanote.com:443/1LQWMe1tFoGL1X?p=oGL1dCkr1ut Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently </body></html>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:46:48.777647018 CEST	34.198.55.140	443	192.168.2.3	49714	CN=*.milanote.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 06 01:00:00 CET 2021	Sat Feb 05 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:46:51.830620050 CEST	34.217.196.79	443	192.168.2.3	49741	CN=*.amplitude.com CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Feb 18 01:00:00 CET 2020	Mon Feb 14 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:46:52.019783974 CEST	34.217.196.79	443	192.168.2.3	49742	CN=*.amplitude.com CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Feb 18 01:00:00 CET 2020	Mon Feb 14 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 06:46:53.062501907 CEST	34.198.55.140	443	192.168.2.3	49746	CN=*.milanote.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jan 06 01:00:00 CET 2021	Sat Feb 05 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:46:53.783795118 CEST	99.83.219.81	443	192.168.2.3	49757	CN=*.intercom.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Apr 15 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sun May 15 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:46:55.012260914 CEST	35.170.0.145	443	192.168.2.3	49762	CN=*.intercom.io, O="Intercom, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 11 01:00:00 CET 2019 Fri Mar 08 13:00:00 CET 2013	Wed Feb 09 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jun 11, 2021 06:47:19.438442945 CEST	151.101.114.208	443	192.168.2.3	49873	CN=*.cartrawler.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 02:11:23 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 02:11:22 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 11, 2021 06:47:19.497364044 CEST	151.101.114.208	443	192.168.2.3	49874	CN=*.cartrawler.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 02:11:23 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 02:11:22 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:47:19.871097088 CEST	52.217.92.196	443	192.168.2.3	49879	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 11 01:00:00 CET 2021	Sat Feb 12 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jun 11, 2021 06:47:20.652374983 CEST	52.55.94.115	443	192.168.2.3	49886	CN=*.prismic.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Oct 23 02:00:00 CEST 2020	Tue Nov 23 00:59:59 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:47:20.693017960 CEST	52.55.94.115	443	192.168.2.3	49887	CN=*.prismic.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Oct 23 02:00:00 CEST 2020	Tue Nov 23 00:59:59 CET 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
							Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
							Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
							Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:47:21.035257101 CEST	199.232.136.157	443	192.168.2.3	49893	CN=ads-twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Aug 14 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Aug 19 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jun 11, 2021 06:47:21.556982040 CEST	104.244.42.5	443	192.168.2.3	49898	CN=t.co, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jun 11, 2021 06:47:21.576001883 CEST	18.215.205.165	443	192.168.2.3	49894	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 30 18:12:07 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 28 18:12:07 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 11, 2021 06:47:21.948587894 CEST	18.215.205.165	443	192.168.2.3	49895	CN=*.quora.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 30 18:12:07 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 28 18:12:07 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 11, 2021 06:47:23.179801941 CEST	13.224.99.118	443	192.168.2.3	49909	CN=*.milanote.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Mar 13 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Apr 12 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:47:25.457695961 CEST	13.224.99.113	443	192.168.2.3	49924	CN=*.milanote.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Mar 13 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Apr 12 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 06:47:26.030586004 CEST	52.55.94.115	443	192.168.2.3	49928	CN=*.prismic.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Oct 23 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Nov 23 00:59:59 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 06:47:26.893471003 CEST	104.244.42.67	443	192.168.2.3	49943	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jun 11, 2021 06:47:45.778718948 CEST	142.250.180.225	443	192.168.2.3	49996	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jun 11, 2021 06:47:45.781620979 CEST	142.250.180.225	443	192.168.2.3	49997	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon May 17 04:58:56 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 09 04:58:55 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 1736 Parent PID: 4852

General

Start time:	06:46:44
Start date:	11/06/2021
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 'http://app.milanote.com/1LQWMe1tFoGL1X?p=oGL1dCkr1ut'
Imagebase:	0x7ff77b960000
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: 5584 Parent PID: 1736

General

Start time:	06:46:46
Start date:	11/06/2021
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=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff77b960000
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: 7080 Parent PID: 1736

General

Start time:	06:47:06
Start date:	11/06/2021
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=audio.mojom.AudioService --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6728 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 2792 Parent PID: 1736

General

Start time:	06:47:07
Start date:	11/06/2021
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6740 /prefetch:8
Imagebase:	0x7ff77b960000
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: 8148 Parent PID: 1736

General

Start time:	06:47:17
Start date:	11/06/2021
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=1508,11621764212539941692,4938375941718598832,131072 --lang=en-US --service-sandbox-type=none --enable-audio-service-sandbox --mojo-platform-channel-handle=3156 /prefetch:8
Imagebase:	0x7ff77b960000

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: 5724 Parent PID: 1736

General

Start time:	06:47:19
Start date:	11/06/2021
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\google_terms_of_service_en_eu.pdf'
Imagebase:	0x810000
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

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: AcroRd32.exe PID: 7576 Parent PID: 5724

General

Start time:	06:47:22
Start date:	11/06/2021
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\google_terms_of_service_en_eu.pdf'
Imagebase:	0x810000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
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: 7304 Parent PID: 5724

General

Start time:	06:47:34
Start date:	11/06/2021
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:	0x8e0000
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: 2220 Parent PID: 7304

General

Start time:	06:47:40
Start date:	11/06/2021
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=1688,10530306713486204241,2167271992676285589,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=16344355117710085358 --mojo-platform-channel-handle=1708 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x8e0000
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: 5124 Parent PID: 7304

General

Start time:	06:47:42
Start date:	11/06/2021
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=1688,105303067134862 04241,216727199267628558 9,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=17060473708032021879 --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=17060473708032021879 --renderer-client-id=2 --mojo-platform-channel-handle=1732 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x8e0000
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: 4012 Parent PID: 7304

General

Start time:	06:47:45
Start date:	11/06/2021
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=1688,105303067134862 04241,216727199267628558 9,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=2108192486941613496 --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=2108192486941613496 --renderer-client-id=4 --mojo-platform-channel-handle=1848 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x8e0000
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: 6140 Parent PID: 7304

General

Start time:	06:47:47
Start date:	11/06/2021
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=1688,105303067134862 04241,216727199267628558 9,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=11960134190916244897 --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=11960134190916244897 --renderer-client-id=5 --mojo-platform-channel-handle=1776 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x8e0000
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

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021